UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR § 1.53(b))

Attorney Docket No.	067292-5005-US
First Inventor	Alen Capalik
Title	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
Electronically filed	June 17, 2011

APPLICATION ELEMENTS

See MPEP Chapter 600 concerning utility patent application contents.

Address to: **Commissioner for Patents**
P.O. Box 1450
Alexandria, VA 22313-1450

1. ☐ Fee Transmittal Form *(with duplicate for fee processing)*
2. ☒ Applicant claims Small Entity status, see 37 C.F.R. § 1.27
3. ☒ Specification [Total Pages 32]
4. ☒ Drawing(s) *(35 USC § 113)* [Total Sheets 17]
5. ☒ Oath or Declaration [Total Pages 2]
   a. ☒ Newly executed *(original or copy)*
   b. ☐ Copy from a prior application *(37 CFR § 1.63(d))*
   (for con/div with Box 18 completed)
   ☐ Deletion of Inventor(s)
   Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR §§ 1.63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet, see 37 C.F.R. § 1.76
7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program *(Appendix)*
8. ☐ Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. ☐ Specification Sequence Listing on
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ CD-ROM or CD-R (2 copies); or
      iii. ☐ Paper
   c. ☐ Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers *(cover sheet & document(s))*
10. ☐ 37 CFR § 3.73(b) Statement
    a. ☐ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement and PTO-1449
    a. ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☐ Return Receipt Postcard *(MPEP 503)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☐ Non-Publication Request under 35 U.S.C. § 122 (b)(2)(B)(i)
17. ☐ Other:

18. If a CONTINUING APPLICATION, *check appropriate box and supply the requisite information below and in a preliminary amendment or in an Application Data Sheet under 37 CFR 1.76:*

☐ This application is a ☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: filed

Prior application information: Examiner: Group Art Unit:

☐ This application is a ☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: filed , which is the National Stage of International Application No. PCT/US , filed .

Prior application information: Examiner: Group Art Unit:

☒ This application claims the benefit of Provisional Application No. 61/358,367, filed June 24, 2010 under 35 U.S.C. § 119(e).

☐ This application claims the benefit of Application No. , filed in under 35 U.S.C. § 119(a).

☒ All of the foregoing applications are incorporated by reference in this application in their entireties.

19. CORRESPONDENCE ADDRESS: Customer Number 24341

Signature		Date	June 17, 2011
Name (Print/Type)	Dion M. Bregman	Registration No. (Attorney/Agent)	45,645

System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application Serial No. 61/358, 367, entitled "System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model" filed on June 24, 2010, which is incorporated by reference herein.

[0002] This relates to U.S. Patent Application No. ____, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States" filed concurrently herewith, which claims priority to U.S. Provisional Application Serial No. 61/358,363 filed on June 24, 2010, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States," both of which are incorporated by reference herein.

[0003] This application relates to U.S. Patent Application No. 11/788,795, entitled "System and Method for Analyzing Unauthorized Intrusion into a Computer Network," filed on April 20, 2007, which is a continuation-in-part of U.S. Patent Application No. 11/488,743, entitled "Decoy Network Technology With Automatic Signature Generation for Intrusion Detection and Intrusion Prevention Systems," filed on July 17, 2006, both of which are incorporated herein by reference in their entireties.

TECHNICAL FIELD

[0004] This invention relates generally to systems and methods for protecting computer networks, including but not limited to systems and methods for analyzing malicious activities on a computer system in order to better protect the computer system from future malicious activity.

BACKGROUND

[0005] An increasing number of computers are connected to computer networks (e.g., the Internet). Networked computers provide a significant benefit of accessing and sharing data over the networks. However, these networked computers are also vulnerable to attacks, unwanted intrusions, and unauthorized access.

IPR2025-00069
CrowdStrike EX1002 Page 2

[0006] Certain existing network security systems have been developed to protect computers from attacks, unwanted intrusions, unauthorized access, and other malicious activities. Such network security systems typically include a firewall to prevent unauthorized access to the network or its computers. Exemplary network security systems also include intrusion detection systems (IDS) and intrusion prevention systems (IPS) that typically contain a library of malware fingerprints (e.g., fingerprints of malware payloads and other unauthorized activities). By using the malware fingerprints, the IDS or the IPS can detect attempts to access computer systems without authorization. When a connection is attempted to a network port, the IDS or IPS examines the low-level IP data packets and compares them to its library of fingerprints for a match. When a match is identified, the IDS or IPS provides notification of the match and/or prevents further access. Therefore, the malware fingerprints play a critical role in network security.

[0007] A critical threat to computer networks is the so-called zero-day attack that exploits security vulnerabilities previously unknown to software developers or system operators. Because the security vulnerabilities are unknown to the software developers or system operators, often the fingerprints of such zero-day attacks are unavailable for comparison. Until the fingerprints are identified, attacks exploiting the same security vulnerabilities continue without detection by the network security systems. However, identifying the fingerprints of malicious activities in the middle of numerous other non-malicious processes is not a trivial task.

[0008] Because network security systems depend on the malware fingerprints, there is a great need for efficient methods of identifying fingerprint data for previously unknown types of malicious and/or unauthorized activities.

SUMMARY

[0009] A number of embodiments that address the limitations and disadvantages described above are presented in more detail below. These embodiments provide computer-implemented methods and systems for generating fingerprint data for zero-day unauthorized activities.

[0010] As described in more detail below, some embodiments involve a computer-implemented method performed at a computer system having one or more processors and memory storing one or more programs for execution by the one or more processors. The method includes monitoring activity on the virtual machine. A

IPR2025-00069
CrowdStrike EX1002 Page 3

plurality of activities performed at a virtual machine is identified. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. The activity sources, activity targets, and associations are stored in the memory. A fingerprint indicative of the activity on the virtual machine is created from the stored activities. The fingerprint is transmitted to one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the fingerprint is transmitted to identify the attack on other affected systems.

[0011] In accordance with some embodiments, the system includes one or more processors, and memory. The memory stores a virtual machine, a virtual machine monitor supervising the virtual machine, and one or more programs. The virtual machine, the virtual machine monitor, and the one or more programs are configured for execution by the one or more processors. The one or more programs include instructions for monitoring activity on the virtual machine, and instructions for identifying a plurality of activities being performed at the virtual machine. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. The one or more programs furthermore include instructions for storing the activity sources, activity targets, and associations in the memory. The one or more programs also include instructions for creating a fingerprint indicative of the activity on the virtual machine from the stored activities. Finally, the one or more programs include instructions for transmitting the fingerprint to one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the one or more programs include instructions for displaying at least a subset of the activities (e.g., action sources, action targets, and actions).

[0012] In accordance with some embodiments, a computer readable storage medium stores one or more programs configured for execution by one or more processors of a computer. The one or more programs include instructions for performing the method described above.

[0013] These embodiments identify unauthorized activities by monitoring and identifying associations between activity sources and activity targets without using pre-determined fingerprints. The data collected by these embodiments can be used to generate fingerprint data in response to the zero-day attacks.

IPR2025-00069
CrowdStrike EX1002 Page 4

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] For a better understanding of the aforementioned aspects of the invention as well as additional aspects and embodiments thereof, reference should be made to the Description of Embodiments below, in conjunction with the following drawings in which like reference numerals refer to corresponding parts throughout the figures.

[0015] Figure 1 is a high-level block diagram illustrating an exemplary distributed computer system in accordance with some embodiments.

[0016] Figure 2 is a block diagram illustrating a decoy network device, in accordance with some embodiments.

[0017] Figures 3A-3D are exemplary network diagrams illustrating unauthorized activities on a network socket, in accordance with some embodiments.

[0018] Figures 4A-4D are exemplary network diagrams illustrating unauthorized activities on files in a computer system, in accordance with some embodiments.

[0019] Figure 4E is an exemplary network diagram illustrating unauthorized activities on a computer system, in accordance with some embodiments.

[0020] Figure 5A illustrates an exemplary data structure of unauthorized activity data, in accordance with some embodiments.

[0021] Figure 5B illustrates an exemplary data structure of fingerprint, in accordance with some embodiments.

[0022] Figure 5C illustrates another exemplary data structure of fingerprint, in accordance with some embodiments.

[0023] Figures 6A-6C are flowcharts representing a method of identifying unauthorized activities on a computer system, in accordance with some embodiments.

DESCRIPTION OF EMBODIMENTS

[0024] Embodiments of various systems and methods for identifying unauthorized activities are described below. Reference will be made to certain embodiments of the invention, examples of which are illustrated in the accompanying drawings. While the invention will be described in conjunction with the embodiments, it should be understood that these particular embodiments are not intended to limit the invention. Instead, the invention is intended to cover alternatives, modifications and equivalents that are within

IPR2025-00069
CrowdStrike EX1002 Page 5

the spirit and scope of the invention as defined by the appended claims. Moreover, in the following description, numerous specific details are set forth to provide a thorough understanding of the present invention. However, it will be apparent to one of ordinary skill in the art that the invention may be practiced without these particular details. In other instances, methods, procedures, components, and networks that are well-known to those of ordinary skill in the art are not described in detail to avoid obscuring aspects of the present invention.

[0025] Figure 1 illustrates an exemplary distributed computer system 100, according to some embodiments. The system 100 includes a decoy computer network 102, a communications network 148, and protected computer network 104. Various embodiments of the decoy computer network 102 and protected computer network 104 implement the unauthorized activity identifying methods described in this document.

[0026] In some embodiments, the systems on the decoy computer network 102 and the protected computer network 104 can be accessed by client computers 101. The client computers 101 can be any of a number of computing devices (e.g., Internet kiosk, personal digital assistant, cell phone, gaming device, desktop computer, laptop computer, handheld computer, or combinations thereof) used to enable the activities described below. The client computer(s) 101 is also referred to herein as client(s). The clients 101 are connected to the decoy network device 106 and the protected network device 136 (e.g., 136-1, 136-2, and 136-n) via the communications network 148.

[0027] The protected network devices 136-1 through 136-n are accessible from the network 148 by one or more authorized users using the clients 101 (e.g., the protected network devices can be servers providing services for webpages, emails, file downloading and sharing, web applications, etc.). Typically, the protected computer network 104 includes a firewall/router 198 to protect the protected network devices 136 and route network traffic to and from the protected network devices 136. Alternatively, the firewall/router 198 can protect both the decoy computer network 102 and the protected computer network 104, as illustrated in Figure 1.

[0028] In some embodiments, the protected computer network 104 also includes an IDS/IPS system 142 (intrusion detection and prevention system). The IDS/IPS system 142 includes, or has access to, a fingerprint library. The fingerprint library includes fingerprints of unauthorized activities. The IDS/IPS system 142 identifies

IPR2025-00069
CrowdStrike EX1002 Page 6

unauthorized activities based on the fingerprints stored in the fingerprint library, and provides notification to a user or a system administrator, and/or prevents unauthorized activities matching the stored fingerprints by modifying the protected network devices 136 and/or the firewall/router 198. Suitable IDS/IPS systems 142 include Cisco Systems' IPS 4200 Series, Juniper's IDP 200, and Enterasys' Dragon IDS Network Sensor.

[0029] As explained above, in some embodiments, the IDS/IPS system 142 is coupled to the firewall/router 198 such that the IDS/IPS system can reconfigure the firewall/router 198 to protect the protected network devices 136 in the protected computer network 104 from future attacks. In some embodiments, the IDS/IPS and the firewall are located in a single combined device.

[0030] The decoy computer network 102 includes one or more decoy network device(s) 106. The decoy network device 106 is a decoy system that is monitored to collect fingerprint data of unauthorized activities. In some embodiments, the decoy network device 106 is intentionally kept vulnerable to unauthorized or malicious activities (e.g., known security weaknesses may be intentionally left unfixed or other security components (e.g., firewalls) are intentionally not installed). In other embodiments, the decoy network device 106 includes security devices and software applications like other protected network devices (e.g., the decoy network device 106 may be protected by the firewall/router 198 and any other security measures included in the protected network devices 136). The purpose of the decoy network device 106 is to allow attackers to attack the decoy network device 106, so that the pattern of the attack can be monitored and analyzed to generate a fingerprint. This fingerprint of the attack can be used to prevent similar attacks on the decoy network device 106 and/or other computers (e.g., protected network devices 136).

[0031] Attackers can initiate attacker activities over the communications network(s) 148 on both the decoy computer network 102 and the protected computer network 104. Ideally, the firewall/router 198 or security software on the protected network devices 136 will protect the protected network devices 136 from at least some of the attacker activity(s), whereas the decoy network device 106 is typically exposed to the attacker activity(s) in order to attract the attacks.

IPR2025-00069
CrowdStrike EX1002 Page 7

[0032] Although Figure 1 illustrates the decoy computer network 102 and the protected computer network 104 as separate networks, in some embodiments, they are part of a same network. For example, in some embodiments, the protected computer network 104 includes the decoy computer network 102. In other embodiments, the decoy computer network 102 and the protected computer network 104 are the same network. Although the methods described herein are described with respect to monitoring the decoy network device 106, persons having ordinary skill in the art would recognize that similar methods may be used for monitoring one or more non-decoy systems, such as the protected network device 136.

[0033] Figure 2 is a block diagram illustrating the decoy network device 106 in accordance with some embodiments. The decoy network device 106 typically includes one or more processing units (CPUs) 202, one or more network or other communications interfaces 204, memory 206, and one or more communication buses 208 for interconnecting these components. In some embodiments, the communication buses 208 include circuitry (sometimes called a chipset) that interconnects and controls communications between system components. In some other embodiments, the decoy network device 106 includes a user interface (not shown) (e.g., a user interface having a display device, a keyboard, and a mouse or other pointing device), but when implemented as a server, the decoy network device 106 is more typically controlled from and accessed by various client systems (e.g., the client 101 in Figure 1; and more typically, a client connected through a secure private network).

[0034] The memory 206 of the decoy network device 106 includes high-speed random access memory, such as DRAM, SRAM, DDR RAM or other random access solid state memory devices; and may include non-volatile memory, such as one or more magnetic disk storage devices, optical disk storage devices, flash memory devices, or other non-volatile solid state storage devices. The memory 206 may optionally include one or more storage devices remotely located from the CPU(s) 202. The memory 206, or alternately the non-volatile memory device(s) within the memory 206, comprises a computer readable storage medium. The memory 206 or the computer readable storage medium of the memory 206 stores one or more of the following programs:

- the network communication module (or instructions) 212 that is used for connecting the decoy network device 106 to computer networks (e.g., communication network(s) 148, decoy computer network 102, and protected

IPR2025-00069
CrowdStrike EX1002 Page 8

computer network 104), and/or other computers (e.g., the client 101) via the one or more communications interfaces 204 and one or more communications networks 148, such as the Internet, a wireless network (e.g., Wi-Fi, WiMAX, 3G, 4G, etc.), any local area network (LAN), wide area network (WAN), metropolitan area network, or a combination of such networks;

- the host operating system 110 (also called Hypervisor OS) that includes procedures for handling various basic system services and for performing hardware dependent tasks;
- database server 128, which stores data (e.g., unauthorized activity data 502 and/or fingerprint 580);
- fingerprint generation engine 130, which generates the fingerprint data 580 from the unauthorized activity data 502); and
- visualization interface 132, which prepares data (e.g., the fingerprint or unauthorized activities on the computer system) for display (e.g., on a GUI of a client 101).

[0035] The fingerprint 580, as described below with reference to Figures 5B and 5C, include data indicative of unauthorized activities on the decoy network device 106. Such fingerprint 580 can be used (e.g., by the IDS/IPS system 142) to detect and prevent unauthorized activities on protected network devices 136.

[0036] In some embodiments, the host operating system (e.g., the host OS 110) includes one or more of the following:

- a virtual machine monitor 214 (also called a hypervisor);
- virtual machines 216, including virtual machine 1 (113-1) and (optional) virtual machine 2 (113-2); and
- normal hypervisor OS user processes (e.g., 114-1 and 114-2), such as administrative utilities, network tools (e.g., netcat and ifconfig), shell processes (e.g., ssh and bash), package management utilities (e.g., dpg and apt), drivers, filesystem utilities, and programming environments (e.g., python and lua).

[0037] The virtual machine monitor 214 includes a hypervisor kernel 116 that resides in physical memory and provides the basic services to the virtual machine monitor 214. In some embodiments, the hypervisor kernel 116 is a part of the hypervisor

IPR2025-00069
CrowdStrike EX1002 Page 9

operating system 110 (e.g., a kernel of the hypervisor operating system 110). In such embodiments, the hypervisor kernel 116 is a part of the operating system that activates the hardware directly or interfaces with another software layer that, in turn, drives the hardware.

[0038] The hypervisor kernel 116 includes a hypervisor virtual machine kernel module 118 that supports virtualization of a "guest" decoy operating system 112. The hypervisor kernel 116 also includes an introspection module 120 interposed between the virtual machine monitor 214 and decoy operating system(s) 112. The introspection module 120 performs introspection (e.g., monitoring) into the physical memory segments assigned to each of the virtualized decoy operating system 112.

[0039] Because no software is installed in the virtualized decoy operating system 112, it is more difficult for the virtualized decoy operating system 112 (or an attacker who has gained access to the virtualized decoy operating system 112) to detect that its memory is being monitored.

[0040] The introspection module is configured to examine the memory assigned to virtualized decoy operating systems 112 in order to acquire low-level data about the interaction between the decoy operating systems 112 and attack activity. The introspection module examines the memory of virtualized decoy operating systems 112 by means of three functional components: a code region selector 222, a trace instrumentor 224, and a trace analyzer 226. Regular expressions (also known as 'regex') are used throughout the process to identify, describe, and profile the contents of the memory segments of the virtualized decoy operating systems 112. The code selector 222 identifies regions of code in memory that are of interest for further introspection. Regions of interest may include, but are not limited to, system calls, the arguments of system calls, the returns of system calls, device and memory input-output, driver information, library calls, branching information, instruction pointer jumps, and raw network information. The instrumentor 224 copies the memory traces of interest identified by the code selector and then profiles them. The trace analyzer 226 takes the profiled traces and uses them to build a simulation of the states in the virtualized decoy operating system 112 over time. In this manner, the introspection module examines the contents of the memory segments of the virtualized decoy operating systems 112 in an instrumented context that generates and retrieves forensic data (or fingerprint). In some

IPR2025-00069
CrowdStrike EX1002 Page 10

embodiments, the trace analyzer 226 is located outside the introspection module 120 (e.g., in the fingerprint generation engine 130).

[0041] In some embodiments, the trace instrumentor 224 is configured to perform operations in accordance with one or more user-defined conditions. The one or more user-defined conditions may specify when one or more memory traces should be generated. Respective user-defined conditions may be rule-based or pattern-based, and may be based on system states or independent of system states. In some embodiments, the trace analyzer 226 is configured to perform operations in accordance with one or more user-defined conditions. The one or more user-defined conditions may specify what portions of the profiled traces to analyze. This allows the user to easily find traces of interest, without having to go through the entire set of traces.

[0042] In some embodiments, the introspection module 120 is configured to pause the execution of the virtualized decoy operating system 112, copy the content of memory at prescribed locations, and return execution control to the virtualized decoy operating system 112. In some embodiments, the introspection module 120 pauses the execution of the virtualized decoy operating system 112 for preventing malicious or undesired execution from occurring in the virtualized decoy operating system 112.

[0043] An attacker may be able to detect that the decoy operating system 112 is a virtualized operating system, based on the time it takes to perform standardized tasks. However, since the introspection module 120 runs completely outside the virtualized decoy operating system 112, it is difficult for an attacker accessing the decoy operating system 112 to determine whether the decoy operating system 112 is being monitored. In other words, the attacker may suspect that the virtual machine monitor 214 exists, but the attacker may not determine whether the virtual machine monitor 214 includes the introspection module 120. As explained above, the introspection module 120 monitors and introspects into the memory segments of the virtualized decoy operating systems 112. The introspection module 120 introspects and gathers information on any virtualized operating system supported by the hypervisor operating system 110.

[0044] The virtual machines 216 are one or more software applications emulating one or more physical machines (e.g., computer systems). In some embodiments, at least one virtual machine (e.g., the virtual machine 1 (113-1)) includes a decoy operating system 112-1, which in turn optionally includes one or more programs (e.g., 220-1 and

IPR2025-00069
CrowdStrike EX1002 Page 11

220-2). The virtualized decoy operating systems 112 access the physical memory assigned to them by the virtual machine monitor 214 (or the hypervisor kernel 116).

[0045] These virtualized operating systems 112 act as decoy operating systems to attract attacker activity. For example, the decoy operating system 112 can be one of WINDOWS, SUN MICROSYSTEMS, SOLARIS, or any version of LINUX known to persons skilled in the art, as well as any combination of the aforementioned. The decoy network device 106 may include any number of virtualized decoy operating systems 112 or any number of virtual machines 113.

[0046] Each of the above identified modules, components, and applications in Figure 2 corresponds to a set of instructions for performing one or more functions described herein. These modules (i.e., sets of instructions) need not be implemented as separate software programs, procedures or modules, and thus various subsets of these modules may be combined or otherwise re-arranged in various embodiments. In some embodiments, the memory 206 may store a subset of the modules and data structures identified above. Furthermore, the memory 206 may store additional modules and data structures not described above.

[0047] Notwithstanding the discrete blocks in Figures 1 and 2, these figures are intended to be a functional description of some embodiments rather than a structural description of functional elements in the embodiments. One of ordinary skill in the art will recognize that an actual implementation might have the functional elements grouped or split among various components. In practice, and as recognized by those of ordinary skill in the art, items shown separately could be combined and some items could be separated. For example, in some embodiments, the fingerprint generation engine 130 and the virtualized decoy OS 112 are part of or stored within the decoy network device 106. In other embodiments, the fingerprint generation engine 130 and the virtualized decoy OS 112 are implemented using separate computer systems. In some embodiments, the fingerprint generation engine 130 includes the database server 128. In some embodiments, the database server 128 is a remote database server located outside the decoy network device 106.

[0048] The actual number of servers used to implement the decoy network device 106 and how features are allocated among them will vary from one implementation to another, and may depend in part on the amount of data traffic that the system must handle

IPR2025-00069
CrowdStrike EX1002 Page 12

during peak usage periods as well as during average usage periods, and may also depend on the amount of data processed by the decoy network device 106. Moreover, one or more of the blocks in Figures 1 and 2 may be implemented on one or more servers designed to provide the described functionality. For example, the decoy network device 106 may be implemented on two distinct computing devices: a monitor device and an analyzer device. The monitor device includes the virtual machine monitor 214, the virtual machines 216, and processes and modules therein. The analyzer device includes the database server 128, the fingerprint generation engine 130, and optionally the visualization interface 132. In such configuration, the monitor device collects unauthorized activity data, and the analyzer device analyzes the unauthorized activity data to generate fingerprints.

[0049] When in use, attackers typically search for vulnerable computers connected to the shared communication network(s), and attempt to perform unauthorized activities on such vulnerable computers through the shared communication network(s).

[0050] Attacker activity may be directed at the decoy computer network 102 through one or more ports of each of the virtualized decoy operating system 112 that are left open as a gateway for the attacker activity. For example, the decoy network 102 can be configured to respond to connection attempts made at network addresses that do not exist on the protected network 104 (e.g., through a connection from the firewall/router 198 to the decoy network device 106 as illustrated in Figure 1). Connections to these non-existent network addresses are assumed to be unauthorized and routed to one of the decoy operating systems 112, since no production hardware (e.g., protected network device 136) exists on the protected network 104 at these addresses. In particular, the decoy operating systems 112 are not configured to provide any user service, and therefore, no ordinary (i.e., authorized and/or non-malicious) user would attempt to access to the virtual machine.

[0051] The decoy operating systems 112 (in the form of a virtualized operating system) may be configured to respond to any such non-existent network address. In a typical attack, the attacker activity scans for an open port, ostensibly in an attempt to make a network connection and then access one or more computing devices on the protected computer network 104. When the attacker activity scans for open ports at non-existent network addresses, however, the attacker is presented with a virtualized decoy operating system 112 instead.

IPR2025-00069
CrowdStrike EX1002 Page 13

[0052] When the attacker connects to a virtualized decoy operating system 112 through an open port, the attacker sees a fully-functional standard operating system fingerprint. Since the decoy network device 106 can be configured to present any operating system as a fully-functional virtualized decoy operating system 112, responses to connection requests from attacker activity are guaranteed to be authentic for the operating system running on that decoy. For example, an FTP port access request for WINDOWS may return a specific character sequence that differs from an FTP response for LINUX. Similarly, an FTP access request to a WINDOWS port may return a response "> ftp: connect: Connection refused." This character sequence may be slightly different from that generated by LINUX. Further, different versions of WINDOWS may respond with slightly different, version-specific character sequences. Since attackers often use these sequences to identify what type of operating system is at a particular network address and the version (or range of possible versions) for that operating system, the fact that virtualized decoy operating systems 112 generate authentic responses makes them realistic decoys and encourages intruders to attempt unauthorized access to them. The instigator of the attack is thus lured into accessing the decoy 112, which is overseen by the hypervisor operating system 110 running on the hardware-based, decoy network device 106. Attacker activity may then initiate previously unknown attacks for the observed operating system. When the attacker activity proceeds to interact with the decoy operating system 112, the attacker provides the decoy operating system 112 with the data used to obtain control of the decoy operating system 112. These data are recorded and analyzed by the introspection module without the knowledge of the attacker.

[0053] All scans by the attacker activity receive real-world operating system and service information, leading the instigator of the attack activity to believe that there is a potentially vulnerable system responding. The attacker is thus lured into communicating with the decoy network device 106 and its virtualized decoy operating systems 112 and services. Since the decoy network device 106 includes real hardware, the attacker is essentially attacking an actual physical system and, therefore, cannot tell that the system is actually an instrumented honeypot that monitors the attacker activity from the introspection module. When an attacker connects to a network port and begins interacting with a virtualized decoy operating system 112, the introspection module monitors and captures information from the connection, including port numbers, data

IPR2025-00069
CrowdStrike EX1002 Page 14

streams, file uploads, keystrokes, ASCII or binary files, malicious payloads, memory manipulation attempts, and any other data transfers or malicious attempts.

[0054] In some embodiments, the introspection module monitors all activity (e.g., system calls, library calls, kernel calls, etc.) on virtualized decoy operating systems 112. In other embodiments, the introspection module, instead of monitoring all activity on virtualized decoy operating systems 112, monitors activity on virtualized decoy operating system 112 based on a monitoring priority (e.g., key system calls and kernel calls). The monitoring priority may be set based on the type of unauthorized activities. For example, in some embodiments, incoming network packets are given high priorities, and therefore, the incoming network packets are thoroughly monitored and analyzed. In some other embodiments, system calls are given high priorities. In yet other embodiments, a virtualized decoy operating system (e.g., 112-1) on a virtual machine 1 (e.g., 113-1) is given a high priority than other virtualized decoy operating system, when the virtual machine 1 is experiencing a high frequency of unauthorized activities. Also a combination of the factors stated above can be used to determine the monitoring priority. In some embodiments, the monitoring priority is user-configurable.

[0055] In use, the introspection module captures (through the introspection) raw attack information. The raw attack information is then communicated to and stored on the database server 128 as forensic data 236 for later analysis. The fingerprint generation engine 130 or the trace analyzer 226 then uses this raw forensic information 236 to generate a signature of the attack. In some embodiments, the fingerprint generation engine 130 or the trace analyzer 226 uses the raw attack information to generate a signature of the attack without storing the raw attack information (i.e., unauthorized activity data) in a database server (e.g., database server 128) first. In some embodiments, the fingerprint generation engine 130 or the trace analyzer 226 uses the raw attack information to generate a signature of the attack without storing the raw attack information in persistent data storage (e.g., database server 128) at all. It should be appreciated that although the signature of the attack may be used to generate an attack signature suitable for use in security applications (e.g., IPS, AV, etc.), the signature of the attack is distinct from the attack signature. The signature (also called a fingerprint) may be used for providing detailed forensic analysis of the character and nature of the attack and its impact on the target operating system, which can be used as the basis for

IPR2025-00069
CrowdStrike EX1002 Page 15

generating triggers. Such triggers may be used to deny malicious system or library calls on the decoy operating system 112.

[0056] In some embodiments, the entire process from attack detection through fingerprint generation occurs automatically, *i.e.,* without any human intervention, at a timescale ranging from nearly immediate to several minutes. The IDS/IPS system 142 uses the attack signature to identify and prevent subsequent attacks.

[0057] In one or more embodiments, the signature may be sent from the fingerprint generation engine 130 to the intrusion detection and/or prevention (IDS/IPS) signature library 134 through a second network connection 140, which is used by the fingerprint generation engine 130 to directly interact with the IDS/IPS system 142.

[0058] After collecting unauthorized activity data, the introspection module 120 may easily clean the virtualized decoy operating system 112 at any time by removing the running system image of the compromised virtualized decoy operating system and replacing it with a pre-attack system image. Thus the introspection module 120 can cleanse or reset the virtualized decoy operating system 112 of any malicious software or payload, removing the possibility that attacker(s) can use that virtualized decoy operating system 112 for further attacks on other networks. In this manner, the attack can be thwarted, and the operating system does not become a tool of the attacker(s). This procedure may also be automated, i.e., may occur without further human intervention.

[0059] Figures 3A-3D and 4A-4E illustrate exemplary network diagrams representing unauthorized activity on a computer system (e.g., the virtual machine 113-1), in accordance with various embodiments. Although Figures 3A-3D and 4A-4E illustrate unauthorized activities on the virtual machine 113-1, analogous methods can be used to represent and analyze unauthorized activities on non-virtualized computer systems.

[0060] Figure 3A-3D illustrate exemplary network diagrams 300 representing unauthorized activities on a network socket (e.g., the virtual machine 113-1), in accordance with some embodiments. In Figure 3A, a data packet stream 304 at a socket 306 of the virtual machine 113-1 is detected by the virtual machine 113-1 and monitored by the virtual machine monitor 214. When the virtual machine 113-1 is a decoy system, the virtual machine 113-1 typically does not actively send and receive packet streams over the network (because the purpose of the decoy system is to wait for a potential attack from an attacker), and any incoming packet stream 304 of data is treated as an

IPR2025-00069
CrowdStrike EX1002 Page 16

unauthorized activity (e.g., an attempt by a hacker to probe a security system of the virtual machine 113-1). In some embodiments, any request to access a computer that does not exist on the protected computer network is treated as an unauthorized activity, and such request is routed to one of the decoy systems (e.g., a virtual machine 113-1 on the decoy network device 106), which is monitored for additional unauthorized activities. In some embodiments, an attacker 302 who sends the packet stream 304 to the socket 306 is identified (e.g., by the Internet Protocol (IP) address).

[0061] Once the packet stream 304 and the socket 306 are identified as affected by unauthorized activities, related unauthorized activities are identified. Figure 3B shows that the packet stream 304 received by the socket 306 is directed to a process A 308, and the process A 308 is treated as affected by unauthorized activities. In turn, in Figure 3C, the process A 308 accesses a file X 310 and a file Y 312, and both the file X 310 and the file Y 312 are treated as affected by unauthorized activities. Thereafter, the file X 310 initiates a process B 314, and the process B is treated as affected by unauthorized activities.

[0062] By analyzing these activities, the fingerprint of the unauthorized activities can be identified (e.g., the unauthorized activities start with the packet stream 304; the unauthorized activities send the packet stream 304 into the computer system 398 through the socket 306; the packet stream 304 is directed to the process A 308; etc.). By using this information, the security of the protected network devices 136 can be improved (e.g., the socket 306 can be closed; the process A 308 can be modified to not respond to data similar to the packet stream 304; etc.).

[0063] Figures 4A-4D illustrate exemplary network diagrams 400 representing unauthorized activities on files in a computer system (e.g., the virtual machine 113-1), in accordance with some embodiments. In Figure 4A, unauthorized activities on the file X 310 and the file Y 312 in the virtual machine 113-1 are detected. For example, the unauthorized activity may be detected by using checksum values of the file X 310 and the file Y 312 (e.g., a different checksum value can indicate that a corresponding file has been modified by an unauthorized process). Alternatively, the unauthorized activity may be detected by monitoring data execution prevention (DEP) exceptions associated with the file X 310 and the file Y 312, generated by the one or more processors (e.g., 202 in Figure 2); or by a manual selection from a system administrator (e.g., based on a file corruption or an erratic behavior).

IPR2025-00069
CrowdStrike EX1002 Page 17

[0064] Figure 4B shows that the process A 308 accesses both the file X 310 and the file Y 312, and the process A 308 is treated as affected by unauthorized activities. Also in Figure 4B, the file X 310 initiates the process B 314, and the process B is treated as affected by unauthorized activities.

[0065] In Figure 4C, data from the socket 306 is directed to the process A 308, and the socket 306 is treated as affected by unauthorized activities. Figure 4D shows that the socket 306 receives the packet stream 304, and the packet stream 304 is treated as affected by unauthorized activities. In some embodiments, the attacker 302 who sends the packet stream 304 to the socket 306 is identified (e.g., by the IP address).

[0066] Figure 4E illustrates an exemplary network diagram 420 representing unauthorized activities on a computer system (e.g., the virtual machine 113-1), in accordance with some embodiments. In Figure 4E, multiple packets of data streams (e.g., 304-1 and 304-2) are detected, and all activity on the computer system 498 are monitored and recorded. When the type of associations is identified (e.g., malignant, benign, etc., as described in more detail below with reference to a type 516 in Figure 5A), at least a subset of the associations can be visually distinguished (e.g., a respective bold arrow representing a malignant association; a regular arrow representing a benign association; alternatively, any other graphical scheme can be used to visually distinguish the subset of the associations, such as color, font, shape, icons, etc.). It is also noted that certain objects drawn with dashed lines (e.g., files, processes, etc.) may have been identified as affected by unauthorized activities, but their associations with other objects may not have been identified.

[0067] Figure 5A is a block diagram illustrating exemplary data structures of unauthorized activity data 502 and unauthorized activity entries 505 in the unauthorized activity data 502, in accordance with some embodiments. Unauthorized activity data 502 includes unauthorized activity entries 505. In some embodiments, the unauthorized activity entries are grouped into one or more sets (e.g., 504) based on time (e.g., time when the entries are recorded or time window of recorded activity), association types (e.g., malicious associations v. benign associations), source types, target types, and other characteristics of the unauthorized activities.

IPR2025-00069
CrowdStrike EX1002 Page 18

[0068] The unauthorized activity data 502 shown in Figure 5A is grouped based on time (e.g., when the entries are recorded). Each set optionally includes one or more of the following set variables 503:

- status 506, which indicates whether the unauthorized activity data 502 is complete or incomplete; the set (e.g., 504-1) is determined to be complete if associations for all objects (e.g., activity sources and activity targets) affected by unauthorized activities are identified; the set (e.g., 504-1) is determined to be incomplete if an association for any object affected by unauthorized activities is not identified;
- frequency 508, which indicates a number of unauthorized activities on the computer system (e.g., virtual machine 113) during a predefined time interval (e.g., one second, five seconds, one minute, five minutes, one hour, five hours, one day, two days, etc.); in some embodiments, the frequency 508 is a relative frequency measured by a number of computer processes affected by unauthorized activities and a total number of computer processes running on the computer system; for example, if the computer system (e.g., virtual machine 113) runs fifty total processes including ten processes affected by unauthorized activities, the frequency 508 is 20% (= 10 / 50); and
- a global time stamp 510, which represents the time when the data in the set (e.g., 504-1) was collected.

[0069] Each set 504 in the unauthorized activity data 502 in Figure 5A also includes one or more unauthorized activity entries 505 (e.g., 505-1, 505-2, 505-3, 505-4, and 505-5). Each unauthorized activity entry 505 includes one or more of the following:

- an activity source 512, which calls, accesses, or executes the activity target 514; the activity source 512 may be one of the following: access to a particular file, access from a particular user, an Internet Protocol address, an instruction, a message, data stream, a hardware component, and a network port; for example, when an instruction A accesses a file X, the instruction A is the activity source, and the file X is the activity target 514;
- an activity target 514, which is called, accessed, or executed by the activity source 512. The activity target 514 may be one of the following: a file, an Internet Protocol address, an instruction, a message, data stream, a hardware component, and a network port; and

IPR2025-00069
CrowdStrike EX1002 Page 19

- an action 515, which represents an event or operation occurring between the activity source 512 and the activity target 514. The action 515 is typically one of: calling, executing, modifying, or accessing operation, such as system calls and library calls.
- An (optional) association type 516, which when identified, represents the type of association between the activity source 512 and the activity target 514; the association type may be one of the following:
    - malignant, which represents that the activity source 512 has modified the activity target 514 to perform unauthorized activities;
    - benign, which represents that the activity source 512 has interacted with the activity target 514 but has not modified the activity target 514 to perform unauthorized activities (e.g., the instruction A reads the file X, but does not modify the file X); and
    - remission, which represents that the activity source 512 is determined to be no longer active in propagating unauthorized activity; for example, the activity source 514 may be modified to remove malicious data and/or to stop unauthorized activities (e.g., by the IDS/IPS system 142);
- (optional) probability 518, which when identified, represents a probability that the corresponding association is malignant; and
- (optional) time stamp 520, which when identified, represents the time when the activity source 512 associates with the activity target 514 (e.g., when the activity source 512 calls, accesses, or executes the activity target 514).

[0070] Figures 5B illustrates an exemplary data structure of fingerprint 580, in accordance with some embodiments. In Figure 5B, the fingerprint 580-1 includes one or more of the following: an (optional) status 506, an activity source 512, an activity target 514, an (optional) association type 516, and an (optional) time stamp 520, all of which are described above.

[0071] The fingerprint 580-1 can be used to prevent future attacks on the computer system or other computer systems, by modifying the activity targets 514 (e.g., increasing privileges, changing the file/instruction name, changing the file/instruction structure, moving the file/instruction to a different location, blocking a particular port,

IPR2025-00069
CrowdStrike EX1002 Page 20

encrypting the file, etc.) to protect the activity targets 514 or blocking the same or similar (e.g., at least partially matching) pattern or sequence of activities (e.g., if the fingerprint of the unauthorized activities starts with sending packets A, B, and C in order, blocking the receipt of the packet C after receiving the packets A and B).

[0072] In some embodiments, the fingerprint 580 consists of respective pairs of activity sources and activity targets, when the association type for a respective pair is malignant. This reduces the size of the fingerprint 580.

[0073] Figures 5C illustrates another exemplary data structure of fingerprint 580, in accordance with some embodiments. In Figure 5C, the fingerprint 580-2 includes the following, or a subset or superset thereof:

- (one or more) activity sources 512, as described above;
- a reference value 522, which is used to identify a particular activity source 512; for example, the reference value 522 can be a file size, a checksum value, one or more portions of the file, instruction, or data packet;
- an (optional) method 524, which is used to indicate how the reference value 522 is used to identify a corresponding activity source 512, or how the activity source is processed to obtain a measured value which can be compared with the reference value 522 to identify the activity source 512. For example, the method can be "checksum," which requires determining a checksum value of the activity source 512, or "match," which requires matching the reference value with the activity source 512. The method 524 is typically omitted when a default method is used to identify the source 512.

[0074] The fingerprint 580-2 can be used to prevent future attacks on the computer system or other computer systems, by blocking activity sources that match a pattern of unauthorized activities (e.g., the reference value 522). For example, if the fingerprint of the activity source includes a data stream with a repeated character of a predefined length (e.g., a 2KB long string of a repeated character), the IDS/IPS can block such data stream by using the reference value 522.

[0075] In some embodiments, the fingerprint 580-2 includes activity targets 514 in lieu of, or in addition to, the activity sources 512.

IPR2025-00069
CrowdStrike EX1002 Page 21

[0076] In some embodiments, the fingerprint 580 includes one or more of: system calls, arguments of system calls, returns of system calls, device and memory input-output, driver information, library calls, branching information, instruction pointer jumps, and raw network information collected from a respective virtual machine 113 or a respective decoy operating system 112 (not shown).

[0077] Figures 6A-6C are flowcharts representing a method 600 of identifying unauthorized activities on a computer system (e.g., the virtual machine 113-1) attached to a computer network, in accordance with some embodiments. The computer-implemented method 600 is performed at a decoy network device (e.g., 106 in Figure 1B) having one or more processors and memory storing a virtual machine and a virtual machine monitor supervising the virtual machine. The memory also stores one or more programs for execution by the one or more processors to perform the method. Typically, the one or more programs executed by the one or more processors to perform the method are executed at the virtual machine monitor.

[0078] The decoy network device monitors (602) activity on the virtual machine. In some embodiments, the decoy network device monitors a predefined set of activity on the virtual machine. In some embodiments, the decoy network device monitors all activity related to incoming data stream on the virtual machine, based on an assumption that all incoming data stream on the virtual machine is unauthorized (e.g., Figures 3A-3D). In some embodiments, the decoy network device monitors activity based on the monitoring priority.

[0079] In some embodiments, the monitoring further includes monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed (603) to be unauthorized, because the virtual machine is not configured to provide user services (e.g., email, web, or file services, etc.) and no authorized user would need to access the virtual machine. In some embodiments, all incoming data packet on the virtual machine is assumed to be unauthorized.

[0080] The decoy network device identifies (604) a plurality of activities being performed at the virtual machine. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. For example, the activity between the file X 310 and the process B 314 in Figure 3D includes

IPR2025-00069
CrowdStrike EX1002 Page 22

the file X 310 as an activity source, the process B 314 as an activity target, and the association represented by the arrow from the file X 310 to the process B 314.

[0081] In some embodiments, a respective activity target comprises (606) one of: a file, a user, an instruction (such as computer processes or system calls), a thread (e.g., a thread of processes), data stream (e.g., network packets), and network socket connections (or sockets). In some embodiments, the respective activity target is an Internet Protocol address.

[0082] In some embodiments, a respective activity source comprises (608) one of: a file, a user, an instruction (such as computer processes or system calls), a thread (e.g., a thread of processes), data stream (e.g., network packets), and network socket connections (or sockets). In some embodiments, the respective activity source is an Internet Protocol address.

[0083] In some embodiments, the decoy network device identifies (610) a respective association between a first activity source and a first activity target as unauthorized. The first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target. For example, we turn to illustrations in Figures 3B-3C. Data from the socket 306 modifies the process A 308 so that the process A 308 performs unauthorized activities (Figure 3B). Therefore, the socket 306 is an activity source in relation to the process A 308, which is an activity target in relation to the socket 306. Then, as shown in Figure 3C, the process A 308 modifies the file X 310, performing unauthorized activities (e.g., corrupting data or writing a malicious code). The process A 308, as an activity source to the file X 310, causes unauthorized activities on the file X 310. By identifying that the process A 308 performed unauthorized activities, the process A 308 is determined to be affected by the unauthorized activities, and the association between the socket 306 and the process A 308 is determined to be malicious (i.e., unauthorized).

[0084] In some embodiments, the decoy network device tracks (612) a transfer of malicious associations over time. For example, as shown in Figure 5A, the decoy network device stores propagation of unauthorized activities (or malicious associations) as a function of time. This allows time-based analysis of the unauthorized activities, and preventing unauthorized activities based on time or sequence-based filters.

IPR2025-00069
CrowdStrike EX1002 Page 23

[0085] In some embodiments, the decoy network device identifies (614) activity sources that are affected by unauthorized activities. In some embodiments, the identifying activity sources that are affected by unauthorized activities includes (616) identifying activity sources that request to access a portion of memory that is set as non-executable. This can be achieved by data execution prevention (DEP) mechanisms. For example, microprocessors manufactured by Intel Corporation (Santa Clara, CA) allow setting one or more portions of the memory as non-executable (e.g., using a non-executable bit in respective page table entries), and generate an exception when there is an attempt to execute an instruction that is set as non-executable. Similarly, operating systems sold by Microsoft Corporation (Redmond, WA) has an analogous function implemented in the operating system (e.g., Windows XP, Windows 7, etc.).

[0086] In some embodiments, instructions executed by the one or more processors have (618) respective privilege levels. Respective activity sources have respective privilege levels, and the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute unprivileged instructions. For example, low level processes (or fundamental OS processes) typically require a fundamental privilege level (e.g., privilege levels 0, 1, and 2 in a microprocessor architecture provided by Intel Corporation), and most applications run at a different privilege level (e.g., privilege level 3 in Intel Architecture). An application running at the privilege level 3 is unprivileged to run a privilege level 0 process. When the privilege level 3 application attempts to run a privilege level 0 process, such activity is identified as an unauthorized activity.

[0087] In some embodiments, the identifying activity sources that are affected by unauthorized activities includes (620) receiving a selection of one or more activity sources from a system administrator. For example, a system administrator may suspect that a certain file or process is affected by unauthorized activities, and select the file or process as affected. The decoy network device monitors activity sources and activity targets associated with the selected file or process, thereby identifying additional unauthorized activities.

[0088] In some embodiments, the identifying activity sources that are affected by unauthorized activities includes (622) identifying a data stream incoming from outside the computer system. As discussed above, all incoming data stream on a decoy system is assumed to be affected by unauthorized activities.

IPR2025-00069
CrowdStrike EX1002 Page 24

[0089] The decoy network device stores (624) the activity sources, activity targets, and associations in the memory. For example, the decoy network device 106 stores unauthorized activity data 502 (e.g., as illustrated in Figure 5A) in memory 206 (as shown in Figure 2) or in the database server 128 (as shown in Figure 2).

[0090] In some embodiments, the decoy network device graphically displays (626) at least a subset of the stored activities. For example, the graphical representation can be an activity diagram as shown in Figures 3A-3D and 4A-4E.

[0091] In some embodiments, the displaying includes (628) visually distinguishing at least a subset of the associations (e.g., in Figure 4E, certain associations are visually distinguished with bold lines. Alternatively, certain associations are visually distinguished with any other visual indications, such as color, shape, icons, etc.). In some embodiments, the visually distinguishing includes visually distinguishing at least a subset of the associations based on the associated probability.

[0092] In some embodiments, the subset of activities includes (630) a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity. For example, Figure 3C illustrates the first activity between the socket 306 and the process A 308 and the second activity between the process A 308 and the file X 310. The process A 308 is the activity target of the first activity and the activity source of the second activity. In other words, the first activity and the second activity are connected through the process A 308. In Figure 3C, both the first activity and the second activity are graphically illustrated.

[0093] In some embodiments, the decoy network device determines (632) an activity status for the stored events. The activity status includes one of: a complete status and an incomplete status. The complete status represents that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations (e.g., in Figure 4D, each activity is associated with the source, packet stream 304 through one or more associations). The incomplete status represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations (e.g., in Figure 4A, the source is not identified, and activities are not associated with the source).

IPR2025-00069
CrowdStrike EX1002 Page 25

[0094] In some embodiments, the decoy network device determines (634) an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval (e.g., frequency 508 in Figure 5A).

[0095] In some embodiments, the decoy network device determines a probability of a respective association (or a probability/confidence of an unauthorized association). The probability represents likelihood that the association is malignant (or benign). For example, if the process A 308 reads the file Y 312 (in Figure 4B), the file Y 312 is not modified, and the association is not malignant. The probability for the association between the process A 308 and the file Y 312 is 0%. However, if the process A 308 writes to (or modifies) the file X 310 (in Figure 4B), the association can be malignant. If we know that the process A 308 is affected by the unauthorized activities, the probability for the association between the process A 308 and the file X 310 is 100%. If we do not know that the process A 308 is affected by the unauthorized activities, the probability for the association between the process A 308 and the file X 310 is a predefined number (e.g., 50%). If the file X 310, in turn, calls the process B 314, the association between the file X 310 and the process B 314 can be assigned a probability based on a predefined rule (e.g., 25% = 50% of the probability associated with the file X 310, which is 50%).

[0096] In some embodiments, the probability is used to adjust monitoring priority for the introspection module. For example, if the association between the process A 308 and the file Y 312 has 0% probability, the association between the process A 308 and the file X 310 has 50% probability, and the association between the file X 310 and the process B 314 has 25% probability, the monitoring priority would be placed in the order of the process A 308 (which can be 100% affected by unauthorized activities), the file X 310 with a 50% probability association, the process B 314 with a 25% probability association, and the file Y 312 with a 0% probability association.

[0097] The decoy network device creates (636) a fingerprint indicative of the activity on the virtual machine from the stored activities. For example, the fingerprint can be fingerprint 580-1 in Figure 5B, fingerprint 580-2 in Figure 5C, or any other fingerprint described herein. The fingerprint 580-1 can be created directly from the stored activities (e.g., unauthorized activity data 502). The fingerprint 580-2 can be created by analyzing unauthorized activity data 502 (in particular the activity sources

IPR2025-00069
CrowdStrike EX1002 Page 26

512) or collecting additional data associated with the activity sources 512 (e.g., calculating a checksum value of an activity source 512, etc.).

[0098] In some embodiments, the fingerprint includes (638) files that are affected by unauthorized activities on the virtual machine. For example, the activity source 512 in the fingerprint 580-1 can be a file or file information (e.g., file name, location, size, checksum value, etc.).

[0099] In some embodiments, the fingerprint includes (640) processes that are affected by the unauthorized activities on the virtual machine. For example, the activity source 512 in the fingerprint 580-1 can be a process or process information (e.g., process name, size, privilege level, related processes, etc.).

[00100] In some embodiments, the fingerprint includes one or more of: system calls' arguments and returns, device and memory input-output, driver calls' arguments and returns, library calls' arguments and returns, branching information, instruction pointer jumps, and raw network information collected from a respective virtual machine 113 or a respective decoy operating system 112.

[00101] In some embodiments, the fingerprint includes one or more of: port numbers, data streams, file uploads, file downloads, keystrokes, ASCII or binary files, malicious payloads, operating system configuration changes (e.g., new or updated registry keys in windows) and memory manipulation attempts.

[00102] In some embodiments, the activities comprise (642) two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

[00103] The decoy network device transmits (644) the fingerprint to one or more protected network devices 136 to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the decoy network device transmits the fingerprint to the IDS/IPS system 142 to prevent future attacks that comprise the same or similar activities on one or more protected network devices 136.

[00104] In some embodiments, one or more other computer systems (e.g., protected network devices 136) on the network are modified (646) to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (e.g., in Figure 1A, the IDS/IPS system modifies at least one of the protected network device(s) 136 to prevent future attacks that comprise the same or similar activities).

IPR2025-00069
CrowdStrike EX1002 Page 27

[00105] The foregoing description, for purpose of explanation, has been described with reference to specific embodiments. However, the illustrative discussions above are not intended to be exhaustive or to limit the invention to the precise forms disclosed. Many modifications and variations are possible in view of the above teachings. The embodiments were chosen and described in order to best explain the principles of the invention and its practical applications, to thereby enable others skilled in the art to best utilize the invention and various embodiments with various modifications as are suited to the particular use contemplated.

[00106] For example, although the activity source 512 and the activity target 514 are described with respect to processes, threads, files, addresses, instructions, messages, hardware components, etc., persons skilled in the art would recognize that similar methods can be used with respect to other types of activity sources and activity targets. In some embodiments, the analysis engine is configured to maintain several layers of network diagrams, where each layer uses the layer beneath it as input and providing more generalized representations of the unauthorized activity as output. For example, a low-level layer might consist of a process reading from a file and subsequently writing many new files. In some cases, the analysis engine might identify this low level pattern as a representation of a file archive being unpacked, and generate a higher-level layer that includes an unpacking process. This exemplary generalization allows the system to identify common elements of attacks, identify classes of attack that have not been seen before (e.g., zero-day attacks), and generate higher-quality signatures. A layer including the level of detail appropriate to the context may be selected for analysis.

[00107] Moreover, the methods described herein need not be restricted to analysis of a single virtualized operating system but, rather, are able to follow a chain of unauthorized activity across multiple virtualized operating systems. This is important in identifying and thwarting advanced threats that involve multiple attackers spread across multiple systems and that evolve over long periods of time.

[00108] Furthermore, although the methods are described with respect to security application, it should be appreciated that similar methods can be used generally for monitoring behavior of a computer system that follows a source event. For example, similar methods can be used for tracking a user behavior on a system, and/or profiling application behavior for performance improvement or debugging purposes.

IPR2025-00069
CrowdStrike EX1002 Page 28

What is claimed is:

1. A computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises:

one or more processors; and

memory storing:

a virtual machine; and

a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

2. The method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.

3. The method of claim 1, wherein the fingerprint includes files that are affected by the unauthorized activities on the virtual machine.

4. The method of claim 1, wherein the fingerprint includes processes that are affected by the unauthorized activities on the virtual machine.

5. The method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

6. The method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

IPR2025-00069
CrowdStrike EX1002 Page 29

7. The method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

8. The method of claim 1, further comprising graphically displaying at least a subset of the stored activities.

9. The method of claim 8, wherein the displaying includes visually distinguishing at least a subset of the associations.

10. The method of claim 8, wherein the subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity.

11. The method of claim 1, further comprising identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.

12. The method of claim 11, further comprising tracking a transfer of malicious associations over time.

13. The method of claim 1, further comprising identifying activity sources that are affected by unauthorized activities.

14. The method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.

15. The method of claim 13, wherein:

instructions executed by the one or more processors have respective privilege levels;

respective activity sources have respective privilege levels; and

the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions.

IPR2025-00069
CrowdStrike EX1002 Page 30

16. The method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system.

17. The method of claim 1, further comprising determining an activity status for the stored events, the activity status comprising one of:

a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and

an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.

18. The method of claim 1, further comprising determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval.

19. A system, comprising:

one or more processors; and

memory storing:

a virtual machine;

a virtual machine monitor supervising the virtual machine; and

one or more programs, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

IPR2025-00069
CrowdStrike EX1002 Page 31

20. A computer readable storage medium, including one or more programs for execution by one or more processors of a computer system, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

IPR2025-00069
CrowdStrike EX1002 Page 32

ABSTRACT OF THE DISCLOSURE

A computer implemented method includes monitoring activity on the virtual machine. A plurality of activities being performed at the virtual machine is identified. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target. The activity sources, activity targets, and associations are stored in the memory. A fingerprint indicative of the activity on the virtual machine is created from the stored activities. The fingerprint is transmitted to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

IPR2025-00069
CrowdStrike EX1002 Page 33

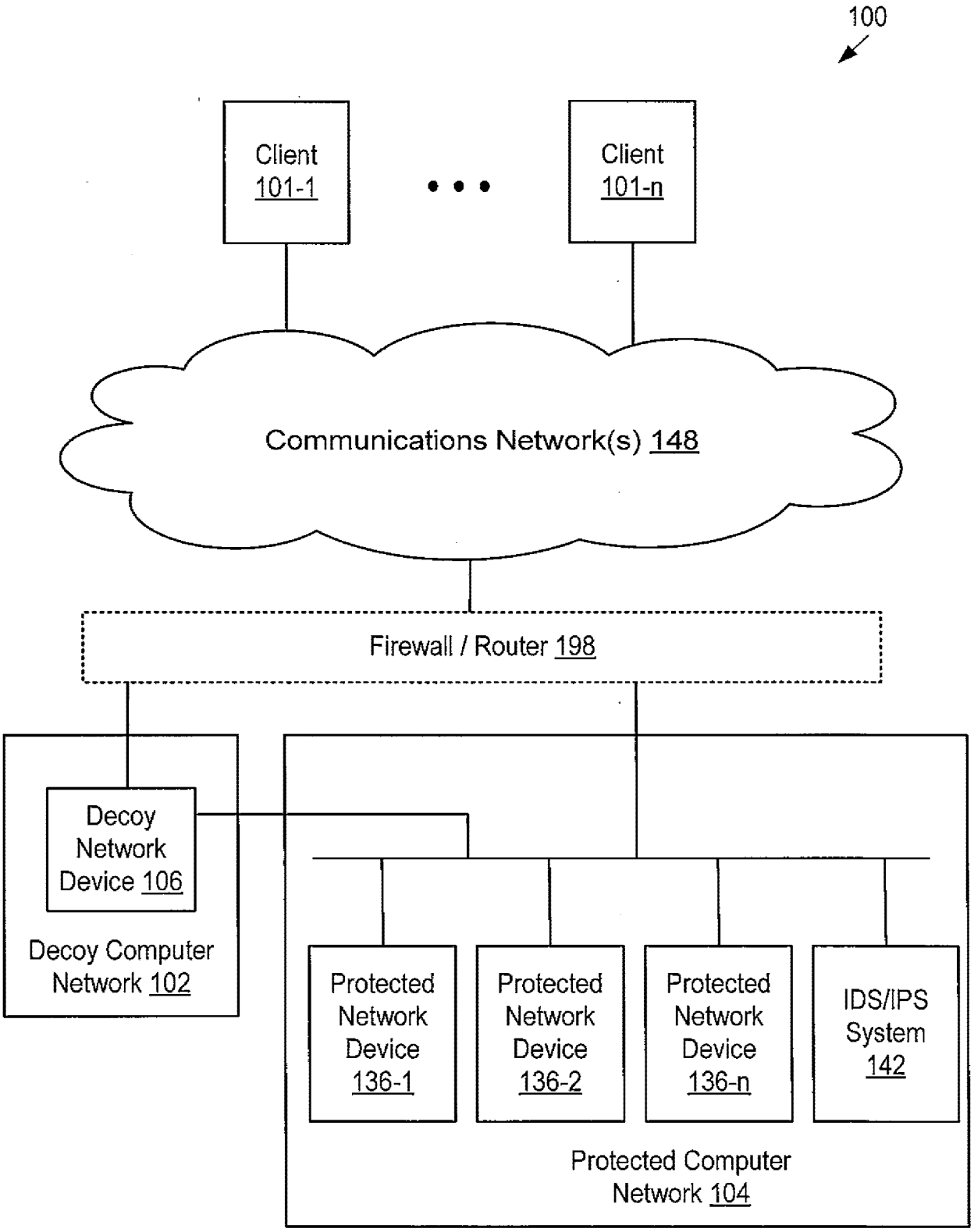

100
Client 101-1
Client 101-n
Communications Network(s) 148
Firewall / Router 198
Decoy Network Device 106
Decoy Computer Network 102
Protected Network Device 136-1
Protected Network Device 136-2
Protected Network Device 136-n
IDS/IPS System 142
Protected Computer Network 104

Figure 1

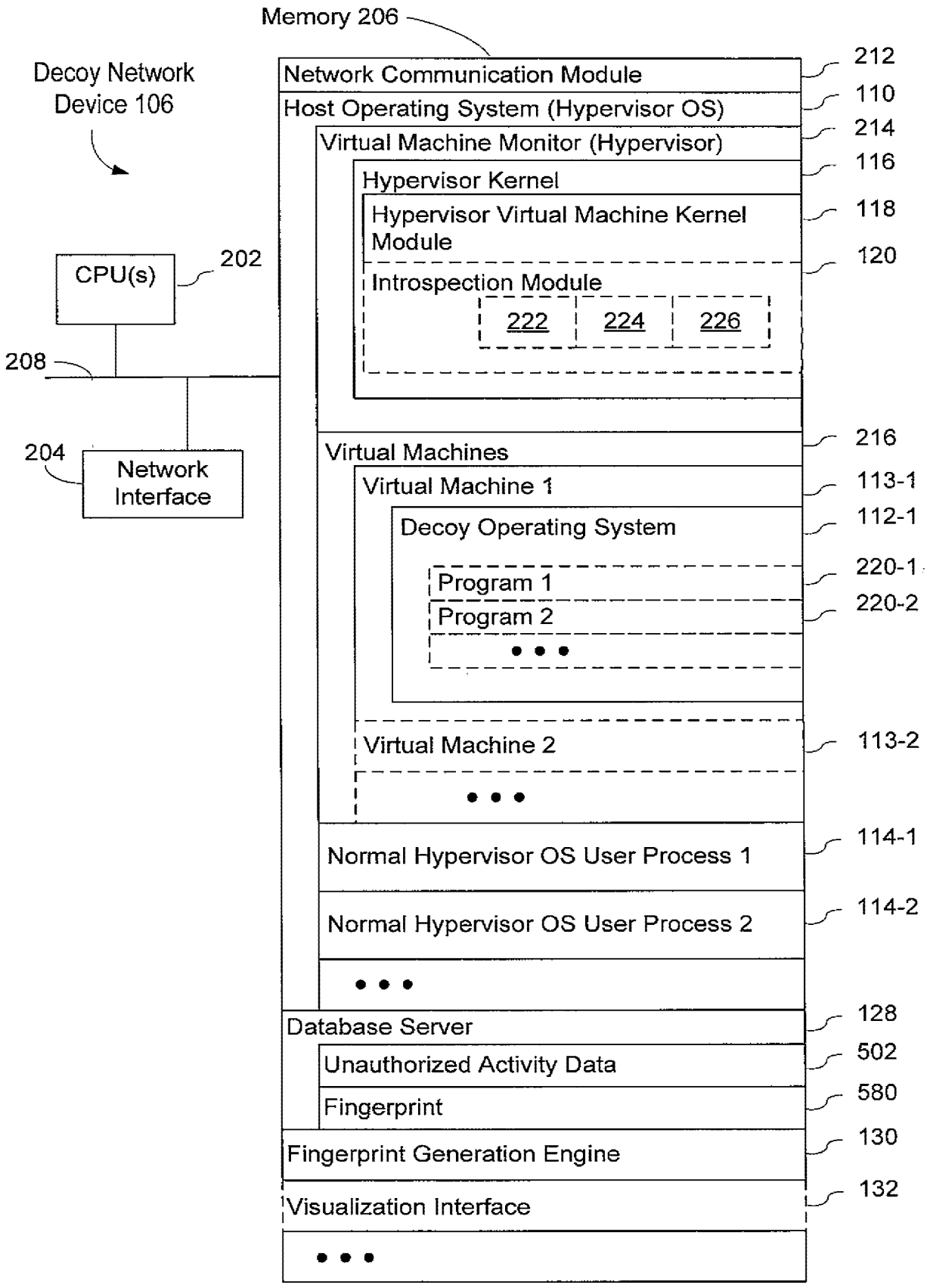

Memory 206
Decoy Network Device 106
CPU(s)
202
208
204
Network Interface
Network Communication Module
212
Host Operating System (Hypervisor OS)
110
Virtual Machine Monitor (Hypervisor)
214
Hypervisor Kernel
116
Hypervisor Virtual Machine Kernel Module
118
Introspection Module
120
222
224
226
Virtual Machines
216
Virtual Machine 1
113-1
Decoy Operating System
112-1
Program 1
220-1
Program 2
220-2
Virtual Machine 2
113-2
Normal Hypervisor OS User Process 1
114-1
Normal Hypervisor OS User Process 2
114-2
Database Server
128
Unauthorized Activity Data
502
Fingerprint
580
Fingerprint Generation Engine
130
Visualization Interface
132

Figure 2

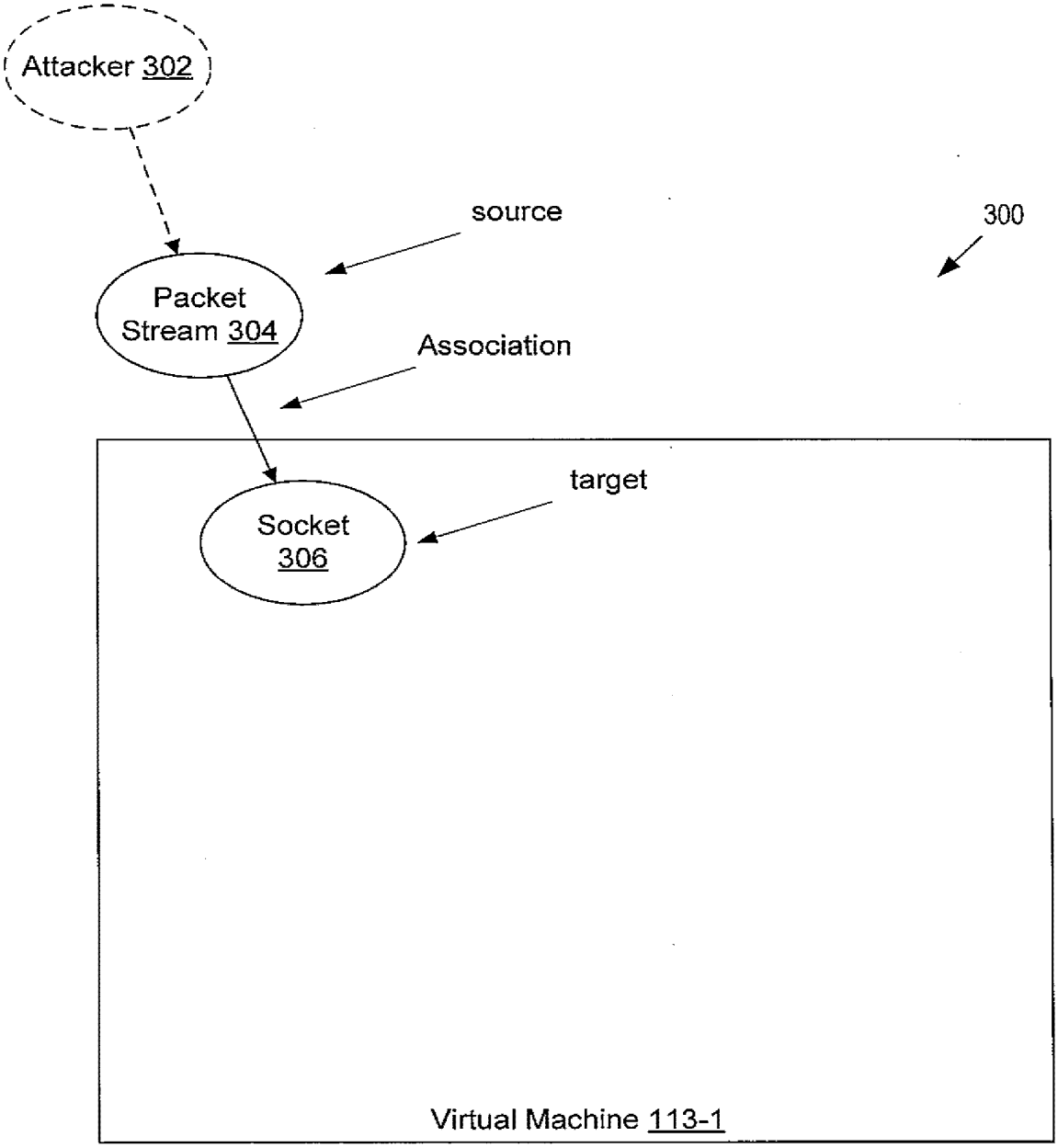

Attacker 302
source
300
Packet
Stream 304
Association
target
Socket
306
Virtual Machine 113-1

Figure 3A

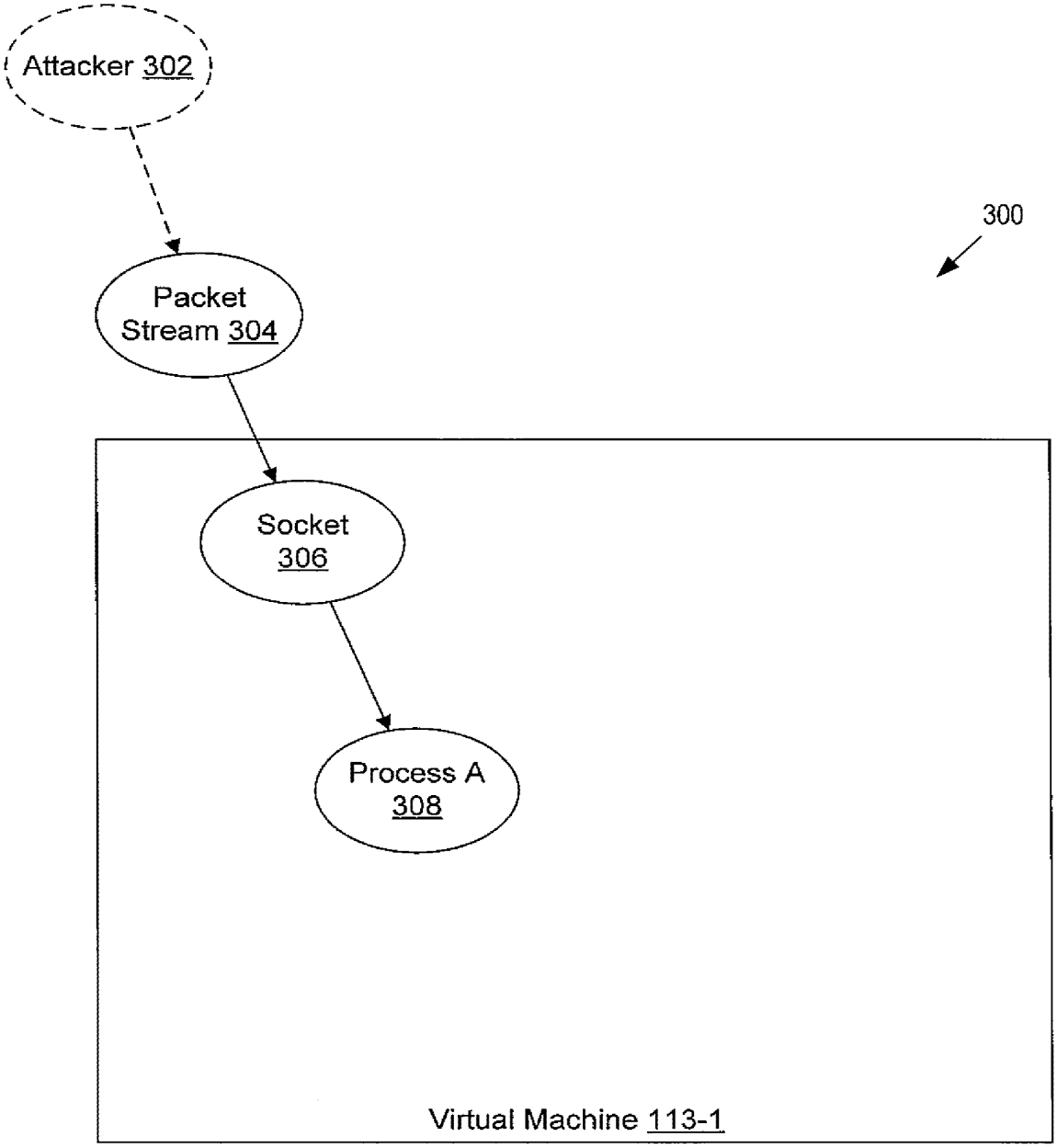

Attacker 302
300
Packet Stream 304
Socket 306
Process A 308
Virtual Machine 113-1

Figure 3B

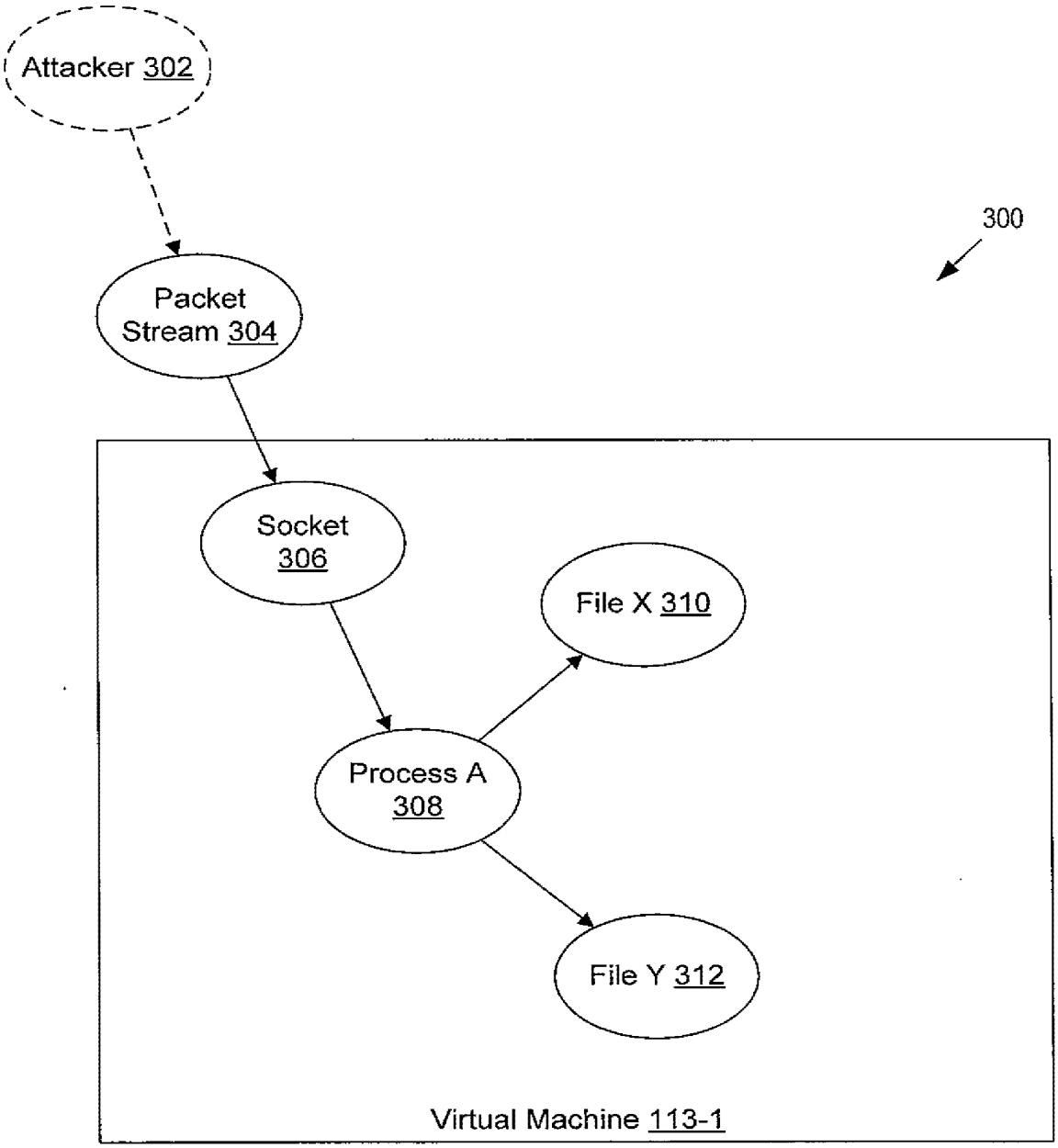

Attacker 302
300
Packet Stream 304
Socket 306
File X 310
Process A 308
File Y 312
Virtual Machine 113-1

Figure 3C

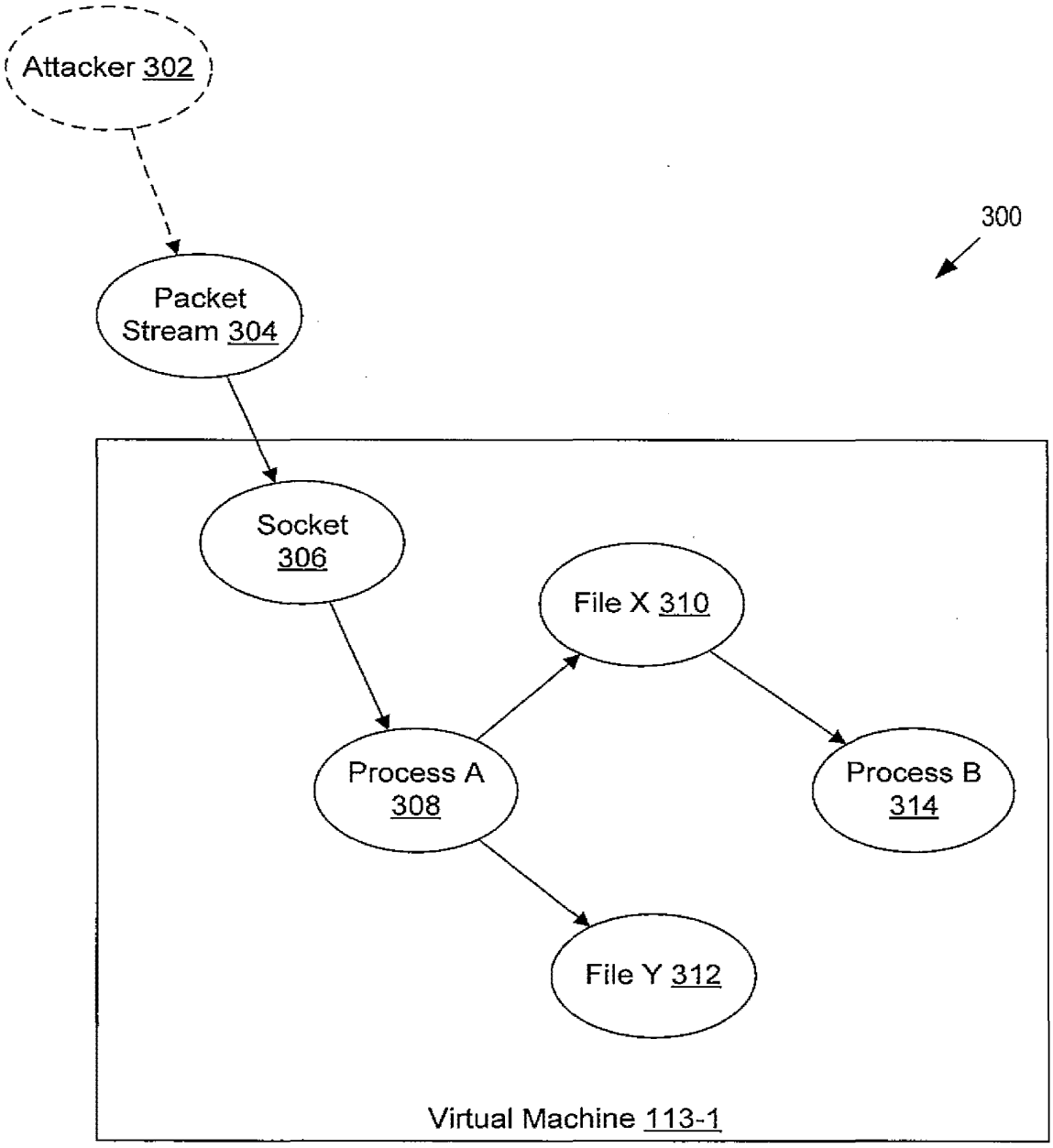

Attacker 302
300
Packet Stream 304
Socket 306
File X 310
Process A 308
Process B 314
File Y 312
Virtual Machine 113-1

Figure 3D

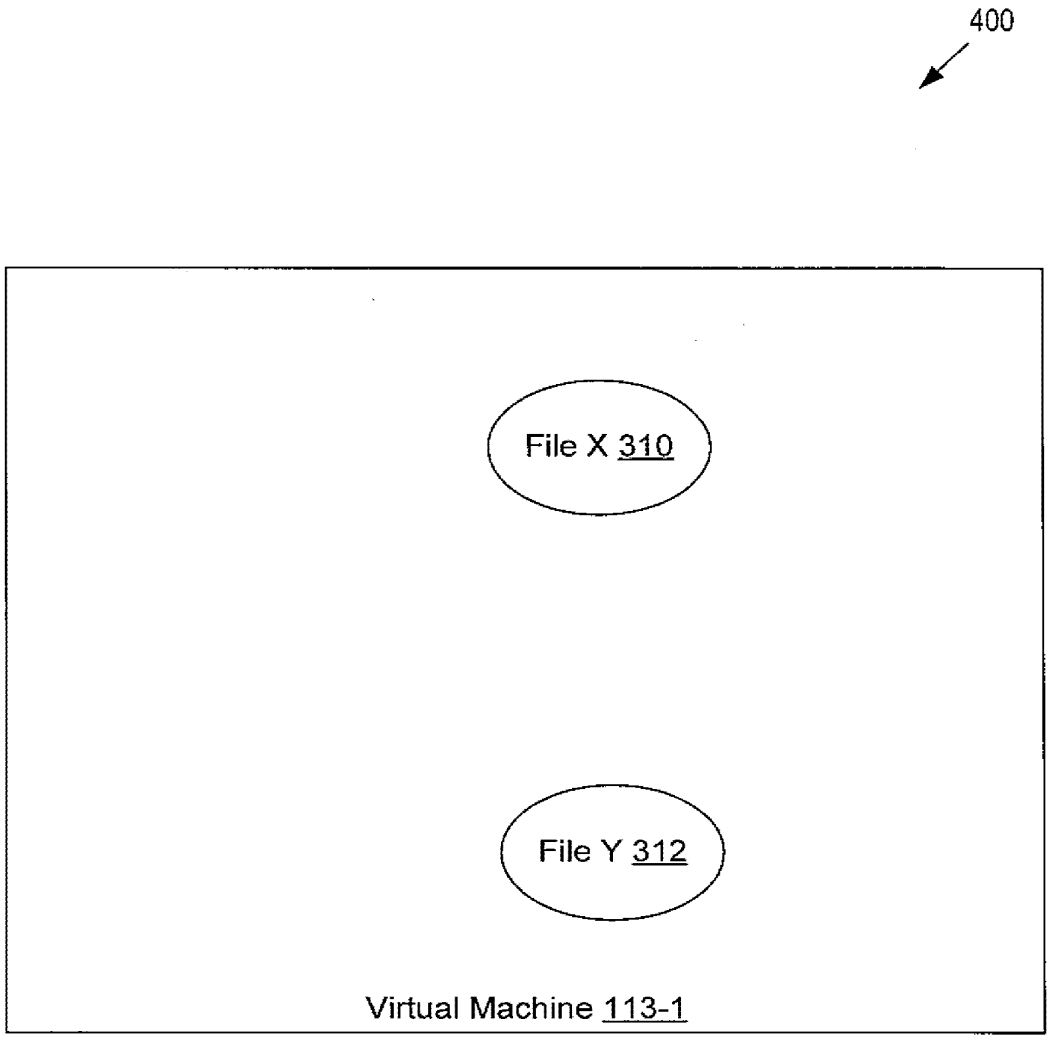


Figure 4A

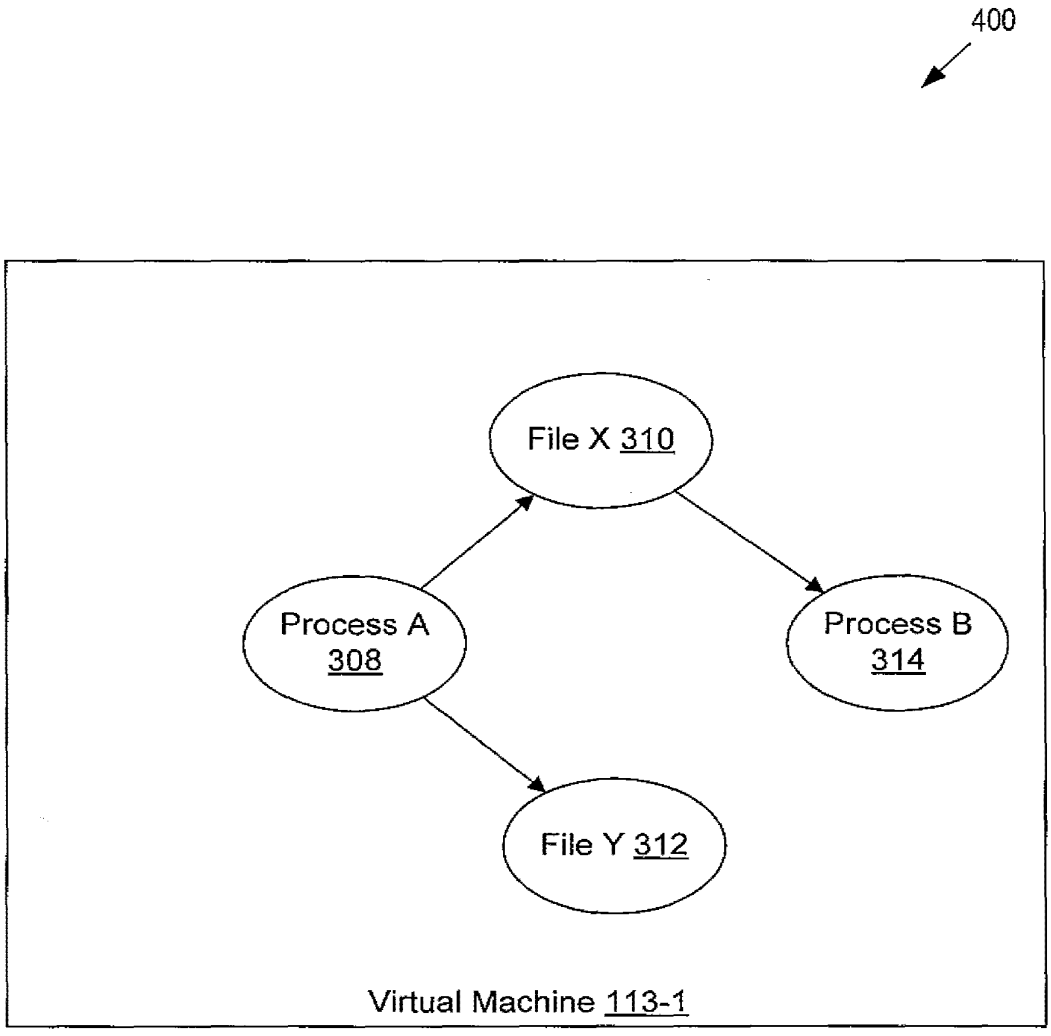

400
File X 310
Process A
308
Process B
314
File Y 312
Virtual Machine 113-1

Figure 4B

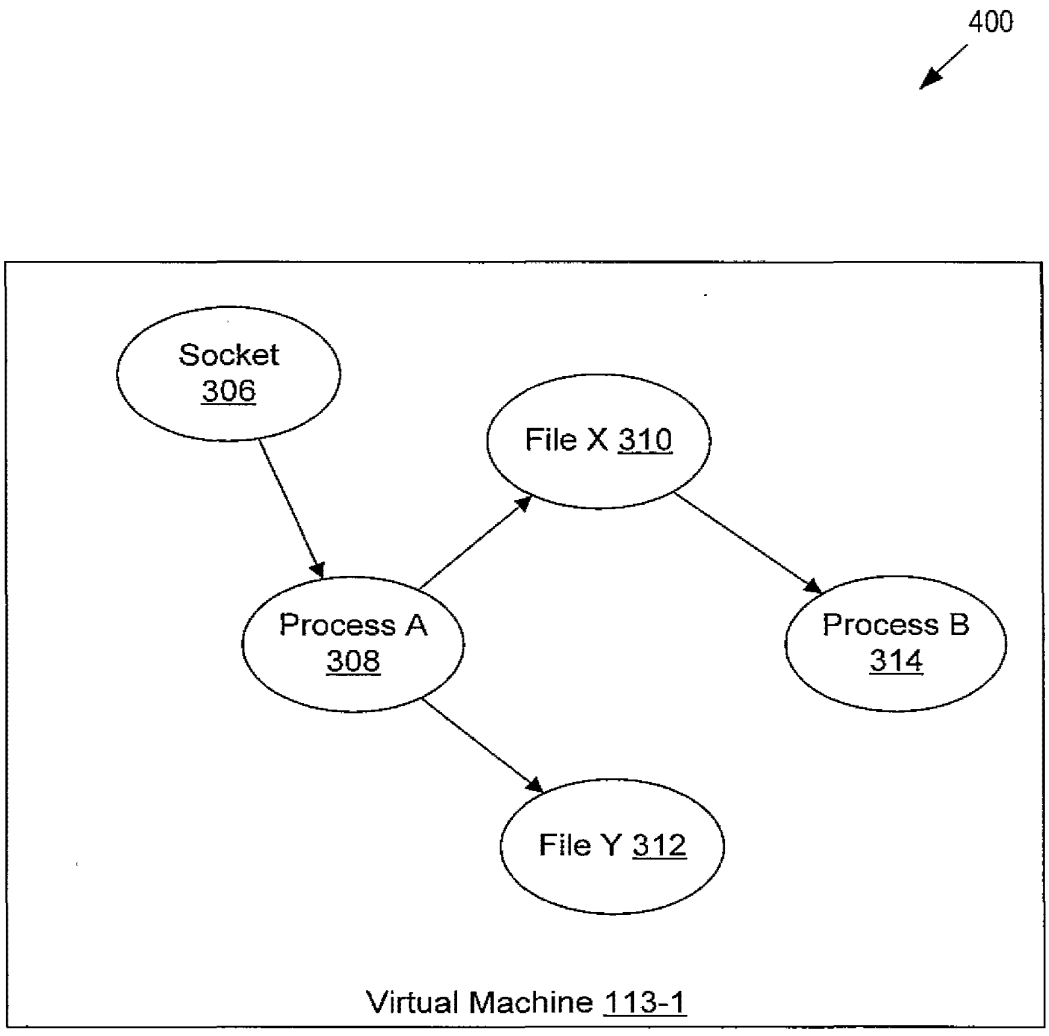

400
Socket
306
File X 310
Process A
308
Process B
314
File Y 312
Virtual Machine 113-1

Figure 4C

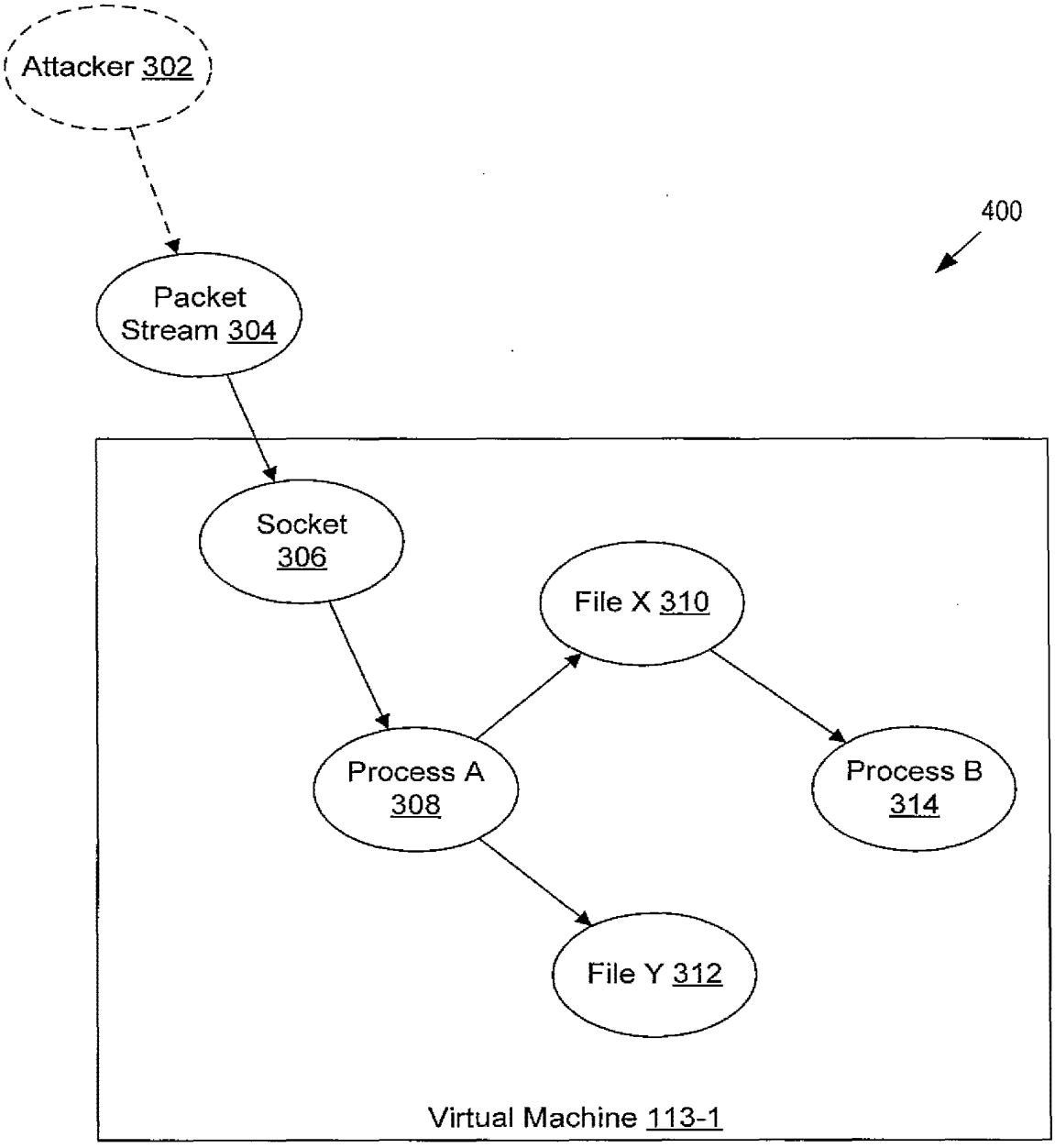

Attacker 302
400
Packet Stream 304
Socket 306
File X 310
Process A 308
Process B 314
File Y 312
Virtual Machine 113-1

Figure 4D

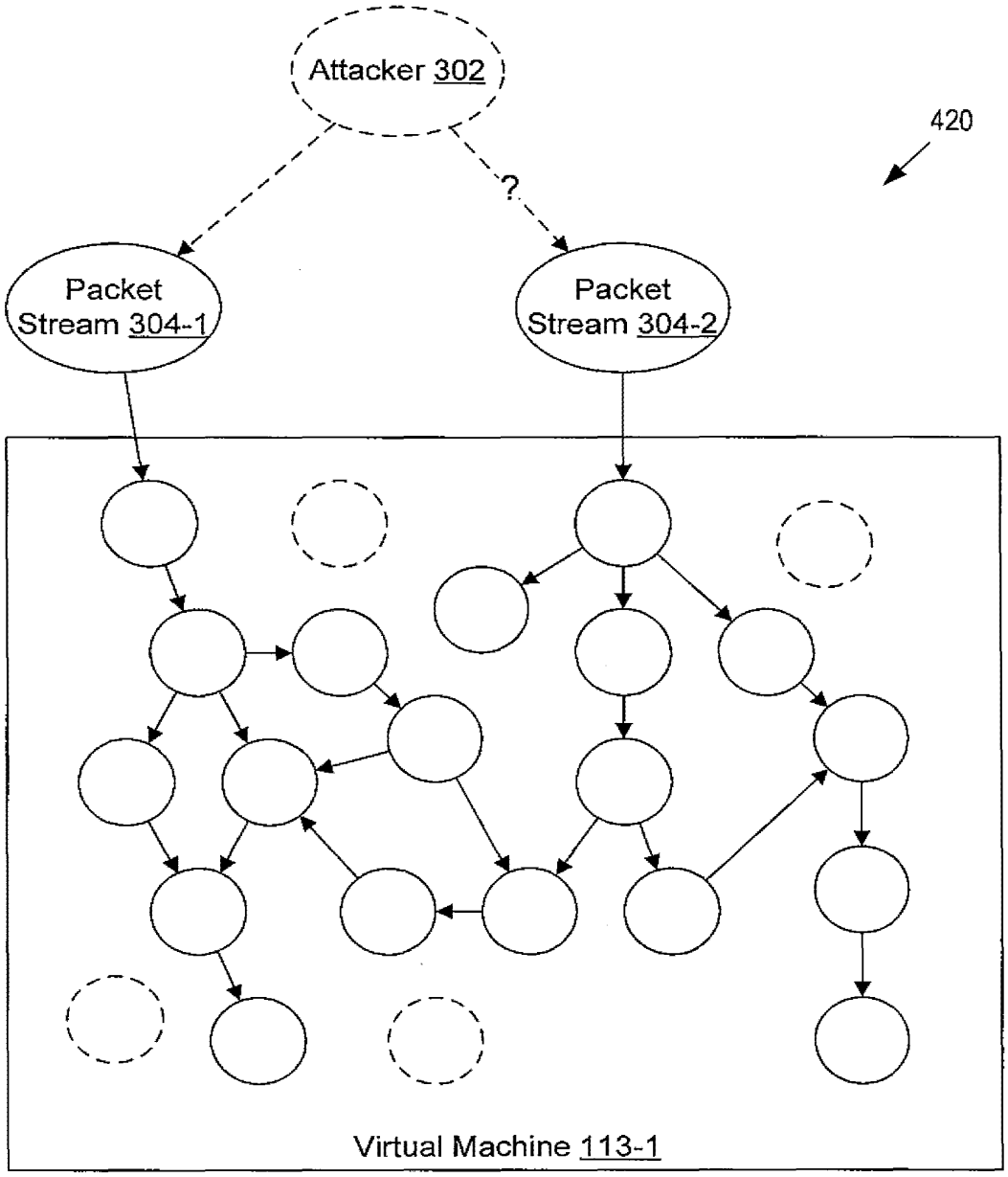

Attacker 302
420
?
Packet Stream 304-1
Packet Stream 304-2
Virtual Machine 113-1

Figure 4E

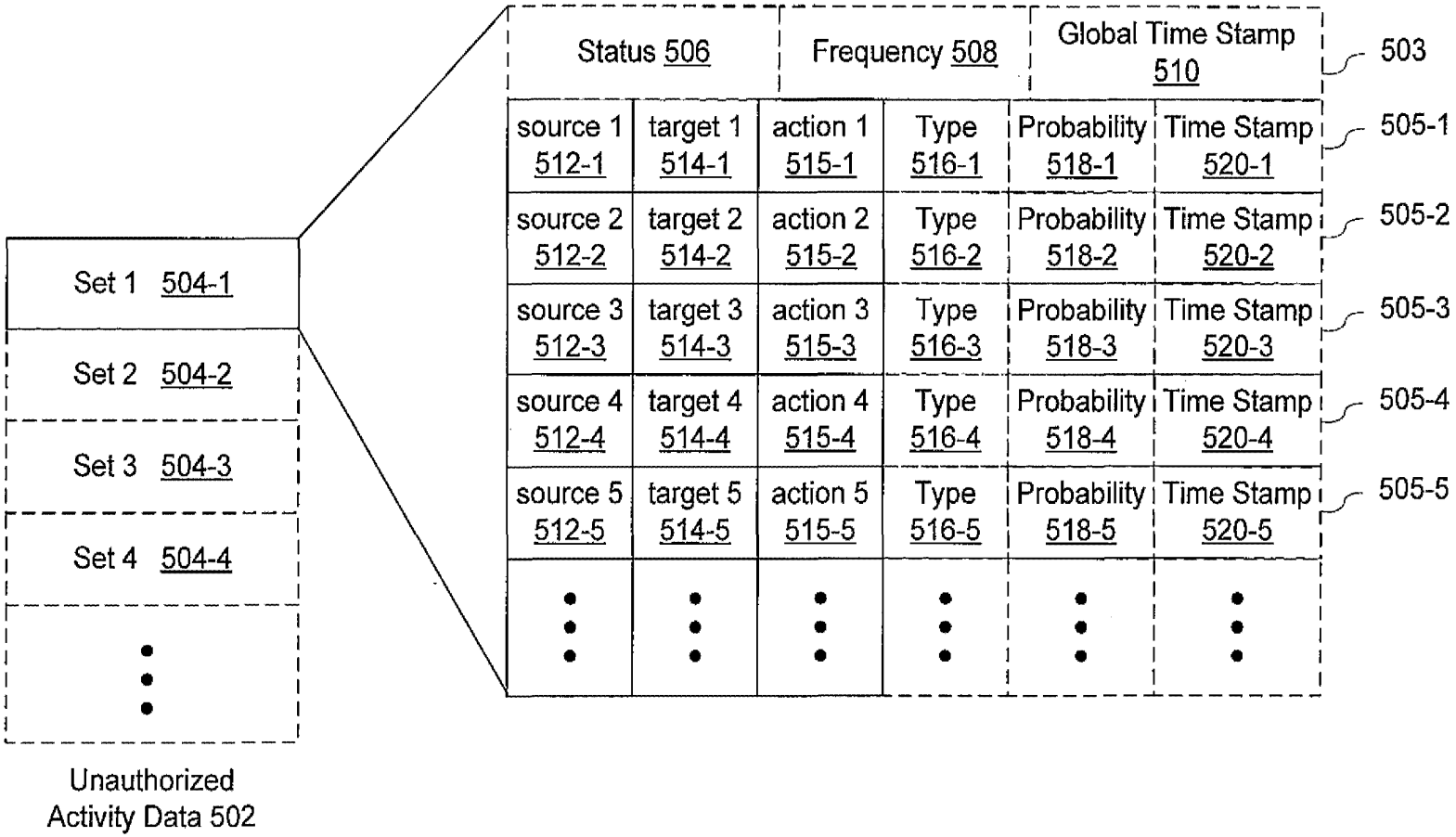

Set 1 504-1
Set 2 504-2
Set 3 504-3
Set 4 504-4
Unauthorized Activity Data 502
Status 506
Frequency 508
Global Time Stamp 510
503
source 1 512-1
target 1 514-1
action 1 515-1
Type 516-1
Probability 518-1
Time Stamp 520-1
505-1
source 2 512-2
target 2 514-2
action 2 515-2
Type 516-2
Probability 518-2
Time Stamp 520-2
505-2
source 3 512-3
target 3 514-3
action 3 515-3
Type 516-3
Probability 518-3
Time Stamp 520-3
505-3
source 4 512-4
target 4 514-4
action 4 515-4
Type 516-4
Probability 518-4
Time Stamp 520-4
505-4
source 5 512-5
target 5 514-5
action 5 515-5
Type 516-5
Probability 518-5
Time Stamp 520-5
505-5

Figure 5A

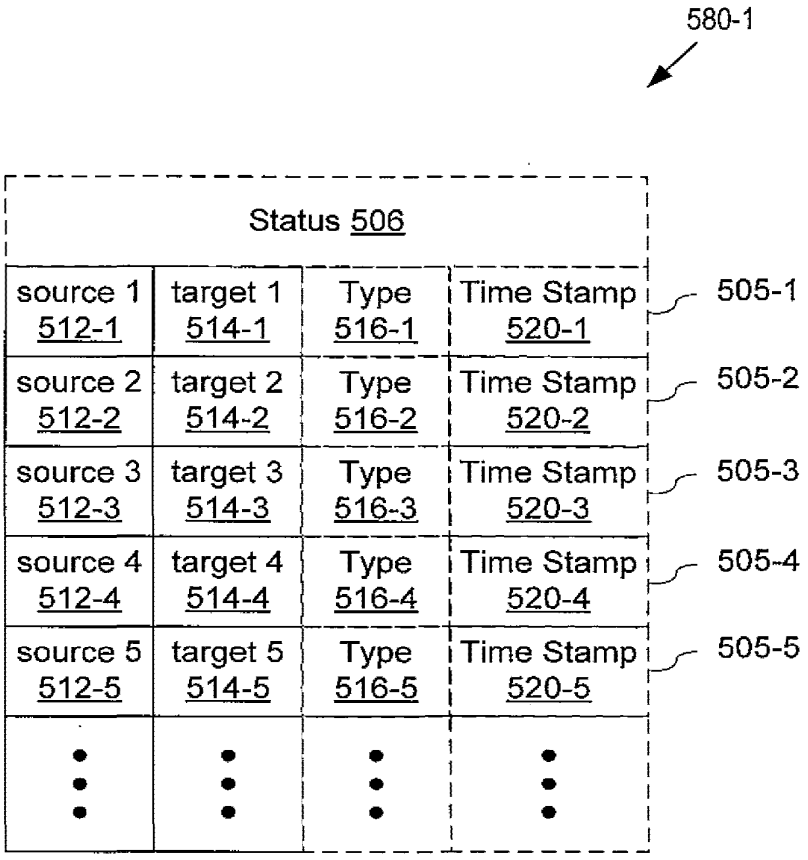

580-1
Status 506
source 1 512-1
target 1 514-1
Type 516-1
Time Stamp 520-1
505-1
source 2 512-2
target 2 514-2
Type 516-2
Time Stamp 520-2
505-2
source 3 512-3
target 3 514-3
Type 516-3
Time Stamp 520-3
505-3
source 4 512-4
target 4 514-4
Type 516-4
Time Stamp 520-4
505-4
source 5 512-5
target 5 514-5
Type 516-5
Time Stamp 520-5
505-5

Figure 5B

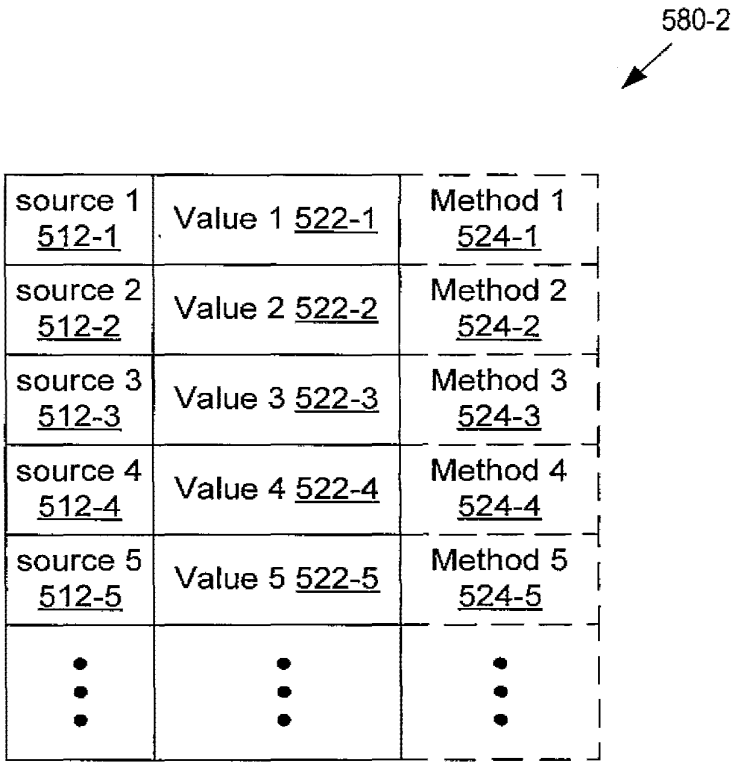

580-2
source 1 512-1
Value 1 522-1
Method 1 524-1
source 2 512-2
Value 2 522-2
Method 2 524-2
source 3 512-3
Value 3 522-3
Method 3 524-3
source 4 512-4
Value 4 522-4
Method 4 524-4
source 5 512-5
Value 5 522-5
Method 5 524-5

Figure 5C

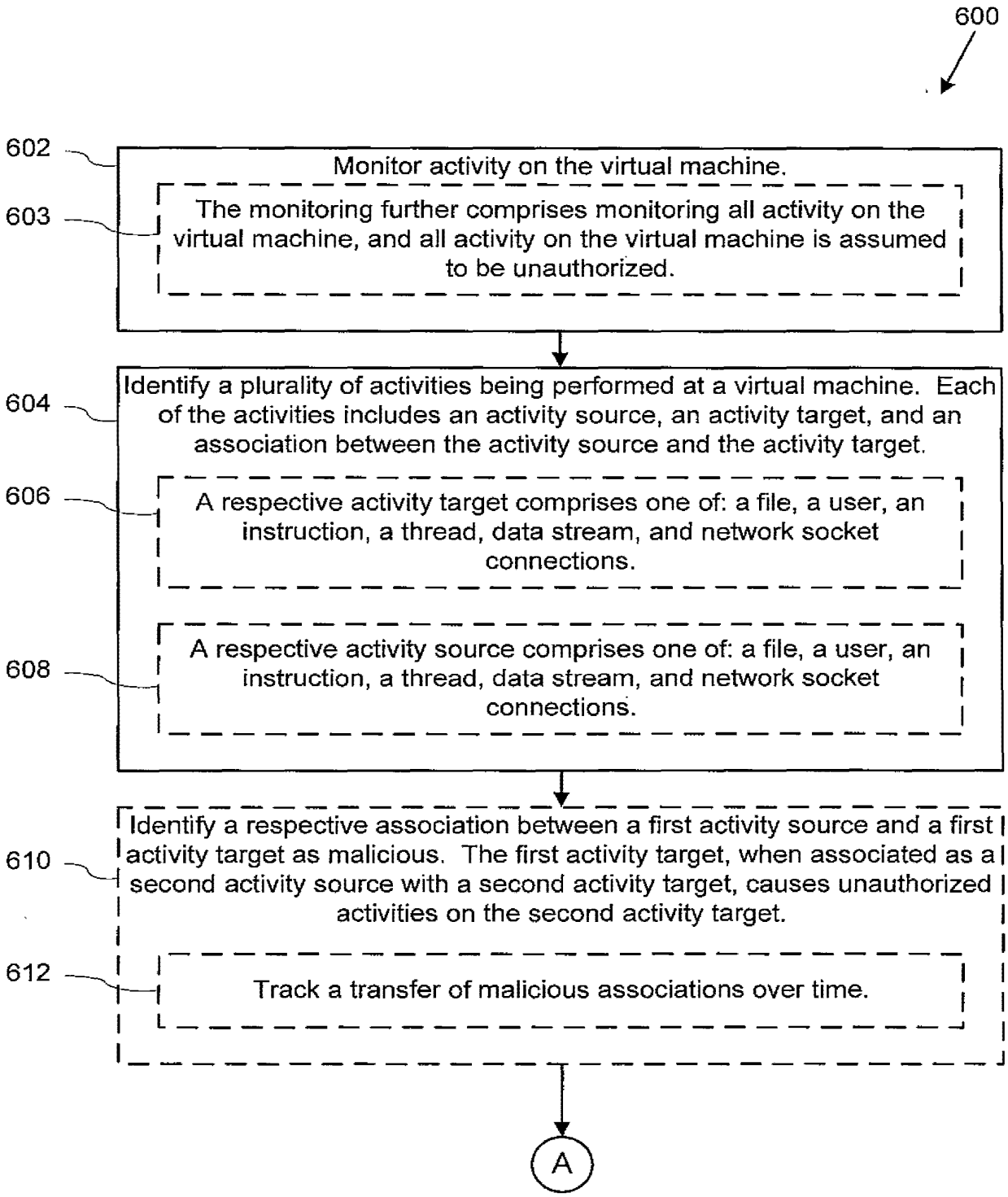

600
602
Monitor activity on the virtual machine.
603
The monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.
604
Identify a plurality of activities being performed at a virtual machine. Each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target.
606
A respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.
608
A respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.
610
Identify a respective association between a first activity source and a first activity target as malicious. The first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.
612
Track a transfer of malicious associations over time.
A

Figure 6A

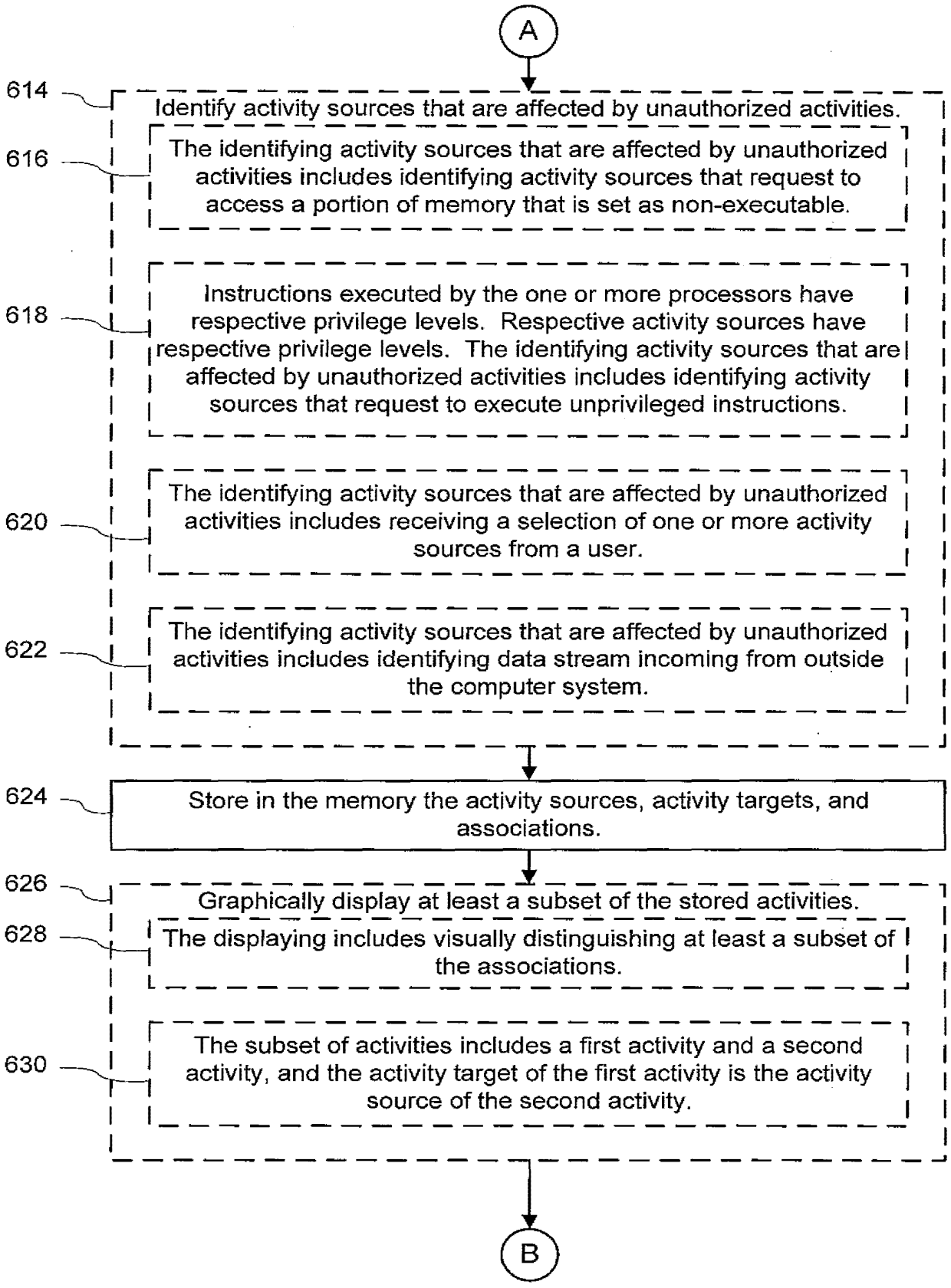

A
614
Identify activity sources that are affected by unauthorized activities.
616
The identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.
618
Instructions executed by the one or more processors have respective privilege levels. Respective activity sources have respective privilege levels. The identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute unprivileged instructions.
620
The identifying activity sources that are affected by unauthorized activities includes receiving a selection of one or more activity sources from a user.
622
The identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system.
624
Store in the memory the activity sources, activity targets, and associations.
626
Graphically display at least a subset of the stored activities.
628
The displaying includes visually distinguishing at least a subset of the associations.
630
The subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity.
B

Figure 6B

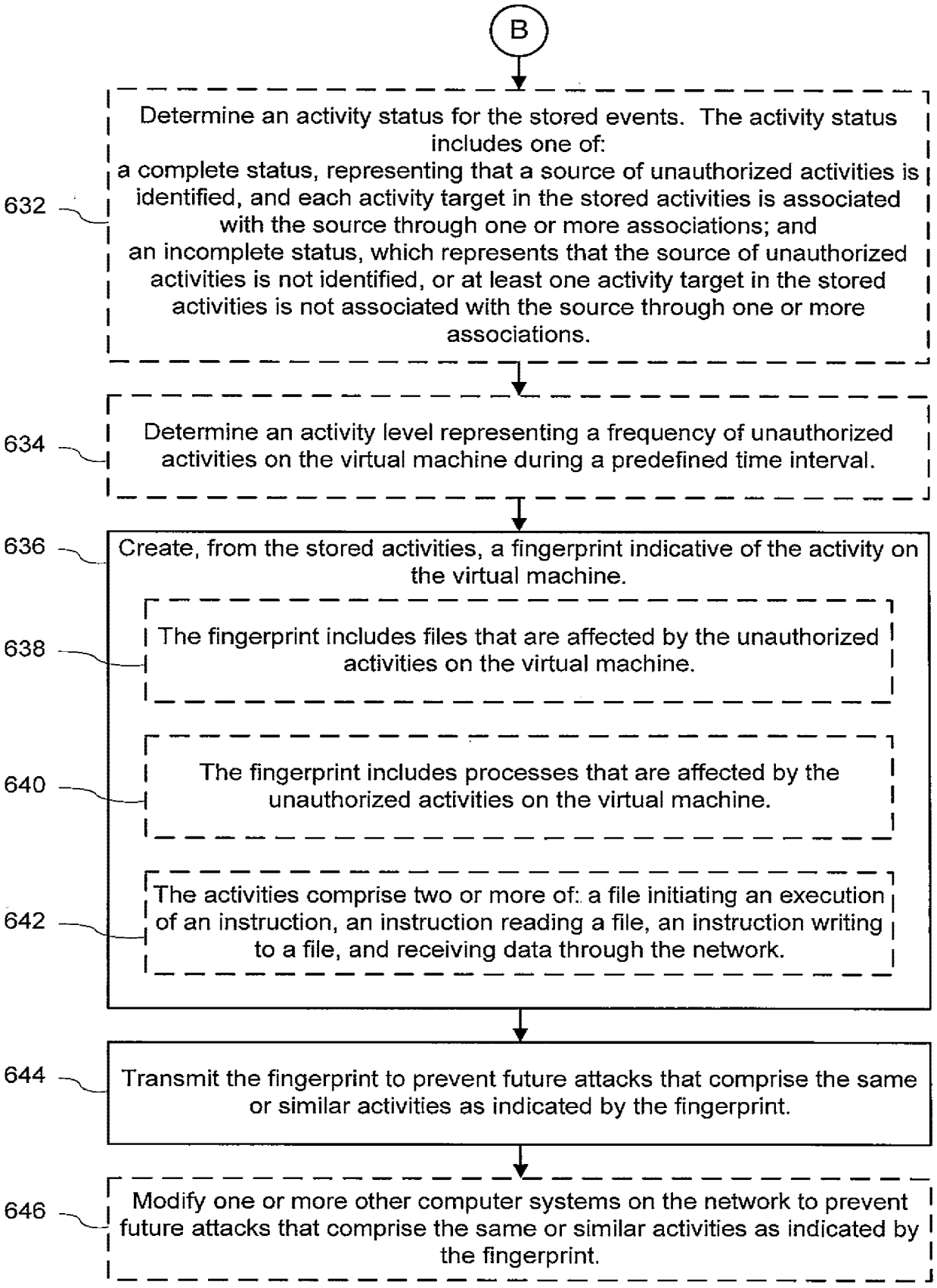

B
Determine an activity status for the stored events. The activity status includes one of:
a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and
an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.
632
Determine an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval.
634
Create, from the stored activities, a fingerprint indicative of the activity on the virtual machine.
636
The fingerprint includes files that are affected by the unauthorized activities on the virtual machine.
638
The fingerprint includes processes that are affected by the unauthorized activities on the virtual machine.
640
The activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.
642
Transmit the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.
644
Modify one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.
646

Figure 6C

DECLARATION FOR NON-PROVISIONAL PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below at 201 et seq. beneath my name.

I believe I am the original, first and sole inventor if only one name is listed at 201 below, or an original, first and joint inventor if plural names are listed at 201 et seq. below, of the subject matter which is claimed and for which a patent is sought on the invention entitled **System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model**

and for which a patent application:

☒ is attached hereto and includes amendment(s) filed on (if applicable)

☐ was filed in the United States on as Application No.

☐ was filed as PCT international Application No. on and was amended under PCT Article 19 on (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information known to me to be material to patentability as defined in 37 C.F.R. §1.56.

I hereby claim foreign priority benefits under 35 U.S.C. §119(a)-(d) or (f) or 365(b) of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

EARLIEST FOREIGN APPLICATION(S), IF ANY, FILED PRIOR TO THE FILING DATE OF THE APPLICATION				
APPLICATION NUMBER	COUNTRY	DATE OF FILING (day, month, year)	PRIORITY CLAIMED	
			YES ☐	NO ☐
			YES ☐	NO ☐

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under § 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

201					
	FULL NAME OF INVENTOR	LAST NAME: CAPALIK	FIRST NAME: ALEN	MIDDLE NAME:	
	RESIDENCE & CITIZENSHIP	CITY: Pacific Palisades	STATE OR FOREIGN COUNTRY: California	COUNTRY OF CITIZENSHIP: US	
	POST OFFICE ADDRESS	STREET: 17020 W. Sunset Blvd., Apt. 12A	CITY: Pacific Palisades	STATE OR COUNTRY: CA	ZIP CODE: 90272
		SIGNATURE OF INVENTOR 201:		DATE: 5/13/2011	

IPR2025-00069
CrowdStrike EX1002 Page 51

202	FULL NAME OF INVENTOR	LAST NAME ANDREWS	FIRST NAME DAVID	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY Los Angeles	STATE OR FOREIGN COUNTRY California	COUNTRY OF CITIZENSHIP Australia	
	POST OFFICE ADDRESS	STREET 10748 Westminster Ave.	CITY Los Angeles	STATE OR COUNTRY CA	ZIP CODE 90034
		SIGNATURE OF INVENTOR 202		DATE 5/13/11	
203	FULL NAME OF INVENTOR	LAST NAME BECKER	FIRST NAME BEN	MIDDLE NAME	
	RESIDENCE & CITIZENSHIP	CITY Santa Monica	STATE OR FOREIGN COUNTRY California	COUNTRY OF CITIZENSHIP US	
	POST OFFICE ADDRESS	STREET 1217 25th Street, Apt. A	CITY Santa Monica	STATE OR COUNTRY CA	ZIP CODE 90404
		SIGNATURE OF INVENTOR 202		DATE 5/13/11	

IPR2025-00069
CrowdStrike EX1002 Page 52

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Stucture Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Dion M. Bregman/Sherri Ballbach
Attorney Docket Number:	067292-5005-US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	82	82
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**462**

Electronic Acknowledgement Receipt

EFS ID:	10335627
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Stucture Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Sherri Ballbach
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	17-JUN-2011
Filing Date:	
Time Stamp:	19:47:57
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$462
RAM confirmation Number	6620
Deposit Account	500310
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

IPR2025-00069
CrowdStrike EX1002 Page 55

1		067292-5005-US_SpecificationAsFiled.pdf	1428585 a3d31b94b7fa5ec269aa2e9ed6202224833be98b	yes	50

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Transmittal of New Application	1	1
Specification	2	28
Claims	29	32
Abstract	33	33
Drawings-only black and white line drawings	34	50

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

2	Oath or Declaration filed	067292-5005-US_ExecutedDeclaration.pdf	83680 22909dce724e23622d8c672f173efcc9f8c92613	no	2

Warnings:

Information:

3	Fee Worksheet (SB06)	fee-info.pdf	33111 6028b5fbdce0060b9580986ba3db698370d7ebd4	no	2

Warnings:

Information:

Total Files Size (in bytes):	1545376

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/163,590	06/17/2011	2431	462	067292-5005-US	20	3

CONFIRMATION NO. 1008

24341
MORGAN, LEWIS & BOCKIUS, LLP. (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

FILING RECEIPT



Date Mailed: 07/01/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Alen Capalik, Pacific Palisades, CA;
David Andrews, Los angeles, CA;
Ben Becker, Santa Monica, CA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/358,367 06/24/2010

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 06/29/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/163,590**

Projected Publication Date: 12/29/2011

Non-Publication Request: No

Early Publication Request: No
** **SMALL ENTITY** **

IPR2025-00069
CrowdStrike EX1002 Page 58

Title

System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

Preliminary Class

726

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where

IPR2025-00069
CrowdStrike EX1002 Page 59

the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

IPR2025-00069
CrowdStrike EX1002 Page 60

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/163,590

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	82		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	270		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	110		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 26 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	x 110 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	462		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed October 3, 2011*	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Capalik, Alen
				Art Unit	2431
				Examiner Name	Not yet assigned
Sheet	1	of	2	**Attorney Docket Number**	067292-5005-US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1.	6,009,274	12-28-1999	Fletcher et al.	
	2.	6,279,113 B1	08-21-2001	Vaidya	
	3.	7,222,366 B2	05-22-2007	Bruton, III et al.	
	4.	7,392,543 B2	06-24-2008	Szor	
	5.	7,464,407 B2	12-09-2008	Nakae et al.	
	6.	US 2002/0099752 A1	07-25-2002	Markos et al.	
	7.	US 2002/0166063 A1	11-07-2002	Lachman, III et al.	
	8.	US 2003/0120935 A1	06-26-2003	Teal et al.	
	9.	US 2004/0225877 A1	11-11-2004	Huang	
	10.	US 2006/0018466 A1	01-26-2006	Adelstein et al.	
	11.	US 2006/0031673 A1	02-09-2006	Beck et al.	
	12.	US 2006/0136720 A1	06-22-2006	Armstrong et al.	
	13.	US 2006/0242703 A1	10-26-2006	Abeni	
	14.	US 2006/0288414 A1	12-21-2006	Kuroda	
	15.	US 2006/0294592 A1	12-28-2006	Polyakov et al.	
	16.	US 2007/0002689 A1	01-04-2007	Mateescu et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document Country Code[3] – Number[4] - Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	1.	European Network of Affined Honeypots, "D1.2 Attack Detection and Signature Generation," May 11, 2006, 79 pgs.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed October 3, 2011*	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Capalik, Alen
				Art Unit	2431
				Examiner Name	Not yet assigned
Sheet	2	of	2	**Attorney Docket Number**	067292-5005-US

	2.	SHIBUYA et al., "A Study for Some Experiences of the Operation of Highly Interactive Decoy System," Information Processing Society of Japan, Volume 45, No. 8, August 2004, 34 pgs.
	3.	Honeypot (computing)-Wikipedia, the free encyclopedia, downloaded July 17, 2006, 4 pgs., http://en.wikipedia.or/wiki/Honeypot_(computing)
	4.	Intrusion-detection system-Wikipedia, the free encyclopedia, downloaded July 17, 2006, 3 pgs., http://en.wikipedia.or/wiki/Intrusion_detection_system
	5.	International Search Report and Written Opinion for PCT/US08/60336 dated August 11, 2008, 9 pgs.
	6.	Office Action for 11/488,743 dated July 30, 2009, 21 pgs.
	7.	Office Action for 11/488,743 dated February 16, 2010, 23 pgs.
	8.	Office Action for 11/488,743 dated August 4, 2010, 21 pgs.
	9.	Office Action for 11/488,743 dated January 18, 2011, 23 pgs.
	10.	Office Action for 11/488,795 dated June 9, 2010, 13 pgs.
	11.	Office Action for 11/488, 795 dated December 1, 2010, 18 pgs.
	12.	Examiner's Answer for 11/488,795 dated May 31, 2011, 19 pgs.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Electronic Acknowledgement Receipt

EFS ID:	11098130
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Angela Hobson
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	03-OCT-2011
Filing Date:	17-JUN-2011
Time Stamp:	14:12:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292_5005US_IDS.pdf	301078 1109cc6dc29227dfd7380227df90bbb96deb1852	yes	6

	Multipart Description/PDF files in .zip description					
	Document Description			Start		End
	Transmittal Letter			1		4
	Information Disclosure Statement (IDS) Form (SB08)			5		6
Warnings:						
Information:						
2	Non Patent Literature	European.pdf	3592158 5ac13661a885a621dd221d93b6de1a4ba7253cbb		no	78
Warnings:						
Information:						
3	Non Patent Literature	Shibuya.pdf	1173013 1cd8d7b0a85ea237a42b07953d4a63df98eef5e6		no	34
Warnings:						
Information:						
4	Non Patent Literature	Honeypot.pdf	239264 232c1d3a361b2c00cdf9e60be4857f777efc9764		no	4
Warnings:						
Information:						
5	Non Patent Literature	Intrusion_detection_system.pdf	176746 30bb7334112999918b21907c734233d2100149a7		no	3
Warnings:						
Information:						
6	Non Patent Literature	ISR_WO.pdf	551771 362e1544fd0ffafe2835ee0a0f0a3065f8066637		no	9
Warnings:						
Information:						
7	Non Patent Literature	OA_743_1.pdf	761889 f8fff0b7bd4b887c6e8c7d30ab753de198967dff		no	21
Warnings:						
Information:						
8	Non Patent Literature	OA_743_2.pdf	843344 f2868cc7f4d4764eb84e83362d2561e9900c484d		no	23
Warnings:						
Information:						

9	Non Patent Literature	OA_743_3.pdf	755671 3399fcec1a3b461b8ed7eb244e714524a67a0f2f	no	21
Warnings:					
Information:					
10	Non Patent Literature	OA_743_4.pdf	890481 c6453c8e7826e1c81b3e84fb87bf23cfbf6d81dc	no	23
Warnings:					
Information:					
11	Non Patent Literature	OA_795_1.pdf	438289 da0739c69a6f1da3930f80afcd2f903e12e545b6	no	13
Warnings:					
Information:					
12	Non Patent Literature	OA_795_2.pdf	637411 099306366028303 7cf73d24176aba6f2e501d3f2	no	18
Warnings:					
Information:					
13	Non Patent Literature	Examiners_Answer.pdf	627386 01203a62cddb07b111d8d43f4505942a09d754f2	no	19
Warnings:					
Information:					
			Total Files Size (in bytes):	10988501	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed October 3, 2011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	CAPALIK et al.	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2431
Filed:	June 17, 2011	Examiner:	Not yet assigned
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☐ Each foreign patent;

☒ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☒ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

IPR2025-00069
CrowdStrike EX1002 Page 67

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☒ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a or 3b)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is:
☐ enclosed
☐ to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Item 3b to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a and 4b)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4.b ☐ The $180.00 fee set forth in 37 C.F.R. §1.17(p) is:
☐ enclosed.
☐ to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application,

and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: October 3, 2011

45,645

Dion M. Bregman (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed November 3, 2011*	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Capalik, Alen
				Art Unit	2431
				Examiner Name	Not yet assigned
Sheet	1	of	1	Attorney Docket Number	067292-5005-US

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	5,664,159	09-02-1997	Richter et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code[3] – Number[4] - Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	B1	WO 2006/113781 A1	10-26-2006	The Trustees of Columbia University in the City of New York		

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	C1	ASRIGO et al., "Using VMM-Based Sensors to Monitor Honeypots," Department of Electrical and Computer Engineering, VEE'06, June 14-16, 2006, pgs. 13-23.
	C2	Debug Register, "Aus Lowlevel," March 22, 2010, 5 pgs.
	C3	JOSHI et al., "Detecting Past and Present Intrusions Through Vulnerability-Specific Predicates," Department of Electrical Engineering and Computer Science, SOSP'05, October 23-26, 2005, 14 pgs.
	C4	KRAPF et al., "XEN Memory Management (Intel IA-32)," October 30, 2007, 6 pgs.
	C5	LITTY et al., "Hypervisor Support for Identifying Covertly Executing Binaries," SS'08 Proceedings of the 17th Conference on Security Symposium, December 31, 2008, 1-16 pgs.
	C6	PROVOS, "A Virtual Honeypot Framework," October 21, 2003, 11pgs.
	C7	NEURALIQ, Inc., PCT/US2011/041122, June 20, 2011, International Search Report and Written Opinion mailed September 21, 2011, 14 pgs.
	C8	NEURALIQ, Inc., PCT/US2011/041119, June 20, 2011, International Search Report and Written Opinion mailed October 4, 2011, 14 pgs.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

WO2006113781

Publication Title:

SYSTEMS AND METHODS FOR DETECTING AND INHIBITING ATTACKS USING HONEYPOTS

Abstract:

In accordance with some embodiments of the present invention, systems and methods that protect an application from attacks are provided. In some embodiments of the present invention, traffic from a communication network is received by an anomaly detection component. The anomaly detection component monitors the received traffic and routes the traffic either to the protected application or to a honeypot, where the honeypot shares all state information with the application. If the received traffic is routed to the honeypot, the honeypot monitors the traffic for an attack. If an attack occurs, the honeypot repairs the protected application (e.g., discarding any state changes incurred from the attack, reverting to previously saved state information, etc.).

Courtesy of http://worldwide.espacenet.com

This Patent PDF Generated by Patent Fetcher(R), a service of Stroke of Color, Inc.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
26 October 2006 (26.10.2006)

PCT

(10) International Publication Number
WO 2006/113781 A1

(51) International Patent Classification:
G06F 11/00 (2006.01) *G06F 11/30* (2006.01)
G06F 11/22 (2006.01)

(21) International Application Number:
PCT/US2006/014704

(22) International Filing Date: 18 April 2006 (18.04.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/672,280 18 April 2005 (18.04.2005) US

(71) Applicant *(for all designated States except US)*: **THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK** [US/US]; 412 LOW MEMORIAL LIBRARY, 535 West 116th Street, New York, NY 10027 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SIDIROGLOU, Stylianos** [US/US]; 1214 Amsterdam Avenue, New York, New York 10027 (US). **KEROMYTIS, Angelos, D.** [GR/US]; 1214 Amsterdam Avenue, New York, NY 10027 (US). **ANAGNOSTAKIS, Kostas, G.** [GR/US]; 200 S. 33rd Street, Philadelphia, Pennsylvania 19104 (US).

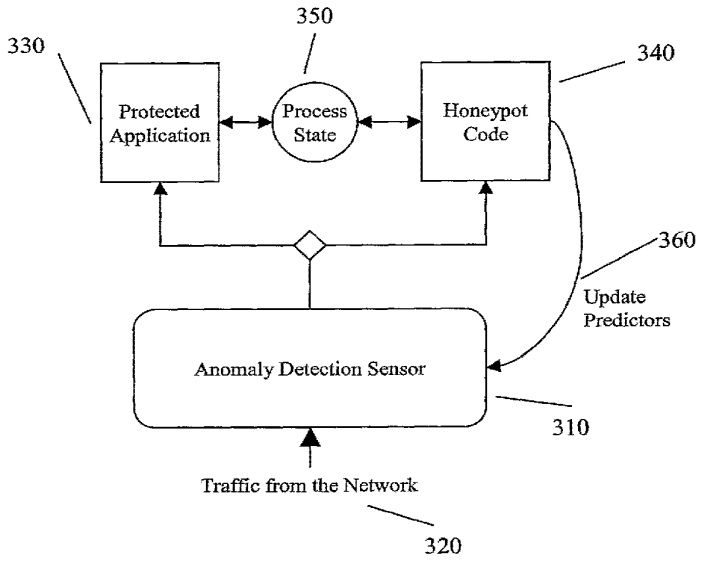
(74) Agents: **WALPERT, Gary, A.** et al.; WILMER CUTLER PICKERING HALE AND DORR LLP, 399 Park Avenue, New York, NY 10022 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR DETECTING AND INHIBITING ATTACKS USING HONEYPOTS



(57) Abstract: In accordance with some embodiments of the present invention, systems and methods that protect an application from attacks are provided. In some embodiments of the present invention, traffic from a communication network is received by an anomaly detection component. The anomaly detection component monitors the received traffic and routes the traffic either to the protected application or to a honeypot, where the honeypot shares all state information with the application. If the received traffic is routed to the honeypot, the honeypot monitors the traffic for an attack. If an attack occurs, the honeypot repairs the protected application (e.g., discarding any state changes incurred from the attack, reverting to previously saved state information, etc.).

WO 2006/113781 A1

IPR2025-00069
CrowdStrike EX1002 Page 73

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEMS AND METHODS FOR DETECTING AND INHIBITING ATTACKS USING HONEYPOTS

Cross-Reference to Related Application

[0001] This application claims the benefit under 35 U.S.C. § 119(e) of United States Provisional Patent Application No. 60/672,280, filed April 18, 2005, which is hereby incorporated by reference herein in its entirety.

Field of the Invention

[0002] The present invention relates to the field of computer security. More particularly, the present invention relates to systems and methods for detecting and inhibiting software attacks.

Background of the Invention

[0003] Computer viruses, worms, trojans, hackers, key recovery attacks, malicious executables, probes, etc. are a menace to users of computers connected to public computer networks (such as the Internet) and/or private networks (such as corporate computer networks). In response to these threats, many computers are protected by antivirus software and firewalls. However, these preventative measures are not always adequate. For example, there have been many instances where worms and other attacks have taken advantage of a known vulnerability in computer software (e.g., in firewall technology) the day after the public became aware of the vulnerability. Because of such a rapid launch, the patch necessary to correct the vulnerability could not be deployed in time to prevent the attack. Similar, most antivirus software relies on updates to that software so that signatures of known viruses can be utilized to recognize threats. In the case of a "zero-day" worm or virus (e.g., a worm or virus that has just been launched), most computer systems are completely vulnerable to attack because no known patch or signature update has yet been made available.

[0004] Due to the level of malicious activity on the Internet, organizations are deploying mechanisms for detecting and responding to new attacks or suspicious activity, sometimes referred to as intrusion prevention systems. However, many of these intrusion prevention

IPR2025-00069
CrowdStrike EX1002 Page 75

systems are limited to protecting against already known attacks because they use rule-based intrusion detection systems.

[0005] Detection mechanisms, such as honeypots and anomaly detection systems, have been developed for use in more powerful reactive-defense systems. In contrast with intrusion detection systems, honeypots and anomaly detection systems offer the possibility of detecting and responding to previously unknown attacks or "zero-day" attacks. A honeypot is generally defined as a trap that is set to detect or deflect attempts at unauthorized use of information systems. However, it should be noted that honeypots do not see legitimate traffic or activity. One reason for this is because honeypots are often placed at a network location that legitimate traffic would have no reason to access. Another reason is that honeypots are usually too slow to process traffic in the time required for real world applications. Yet another reason is that honeypots do not have the capabilities to fully service the legitimate traffic because, for example, honeypots do not fully share state with the actual system. Anomaly detection systems protect a resource by monitoring attempted accesses to it and using heuristics to classify the accesses as normal or anomalous. Honeypots and anomaly detection systems offer different tradeoffs between accuracy and the scope of attacks that can be detected.

[0006] Honeypots can be heavily instrumented to accurately detect attacks, but they depend on an attacker attempting to exploit a vulnerability against them. This makes honeypots good for detecting scanning worms, but ineffective against manually directed attacks or topological and hit-list worms. Furthermore, honeypots are typically used only for server-type applications.

[0007] Anomaly detection systems can theoretically detect both types of attacks, but are usually much less accurate than honeypots. Most anomaly detection systems offer a tradeoff between false positive and false negative detection rates. For example, it is often possible to tune the system to detect more potential attacks, however, this is at an increased risk of misclassifying legitimate traffic. While it is possible to make an anomaly detection system more insensitive to attacks, this creates the risk of missing some actual attacks. Because anomaly detection systems can adversely affect legitimate traffic by, for example, dropping legitimate requests, system designers often tune the system for low false positive rates which may misclassify attacks as legitimate traffic.

IPR2025-00069
CrowdStrike EX1002 Page 76

[0008] Accordingly, it is desirable to provide systems and methods that overcome these and other deficiencies of the prior art.

Summary of the Invention

[0009] In some embodiments of the present invention, systems and methods for protecting applications from attacks are provided. The received traffic (e.g., network traffic) is transmitted through an anomaly detection component. The anomaly detection component predicts whether the received traffic is a potential attack on the application and the anomaly detection component is tuned to achieve a low false negative rate. In response to receiving an indication from the anomaly detection component that the traffic may be an attack, transmitting the received traffic to a honeypot. The honeypot can be an instrumented instance of the application that shares state information with the application. It should be noted that, in some embodiments, the honeypot can be at least a portion of the protected application itself. The honeypot monitors the received traffic for attacks on the application. In response to receiving an indication from the honeypot that the received traffic is an attack on the application, the honeypot provides an instruction to repair the state information of the application.

[0010] In some embodiments, the repair can include rolling back the state information of the application to previously saved state information. In some embodiments, the repair can include discarding the state information of the application. In some embodiments, the repair can include initiating a new instance of the application with previously saved state information.

[0011] In some embodiments, a filter can be provided that filters traffic prior to transmitting the received traffic to the anomaly detection component. The filtering can be based on at least one of payload content and source of the attack.

[0012] In some embodiments, feedback may be provided by the honeypot. In some embodiments, feedback from the honeypot can be used to update the anomaly detection component (e.g., the predictors and models associated with the anomaly detection component) and/or the filter. In some embodiments, the feedback can be used to automatically tune the anomaly detection component and/or the filter.

[0013] There has thus been outlined, rather broadly, the more important features of the invention in order that the detailed description thereof that follows may be better understood,

IPR2025-00069
CrowdStrike EX1002 Page 77

and in order that the present contribution to the art may be better appreciated. There are, of course, additional features of the invention that will be described hereinafter and which will form the subject matter of the claims appended hereto.

[0014] In this respect, before explaining at least one embodiment of the invention in detail, it is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

[0015] As such, those skilled in the art will appreciate that the conception, upon which this disclosure is based, may readily be utilized as a basis for the designing of other structures, methods and systems for carrying out the several purposes of the present invention. It is important, therefore, that the claims be regarded as including such equivalent constructions insofar as they do not depart from the spirit and scope of the present invention.

[0016] These together with other objects of the invention, along with the various features of novelty that characterize the invention, are pointed out with particularity in the claims annexed to and forming a part of this disclosure. For a better understanding of the invention, its operating advantages and the specific objects attained by its uses, reference should be had to the accompanying drawings and descriptive matter in which there are illustrated preferred embodiments of the invention.

Brief Description of the Drawings

[0017] The above and other advantages of the present invention will be apparent upon consideration of the following detailed description, taken in conjunction with accompanying drawings, in which like reference characters refer to like parts throughout, and in which:

[0018] FIG. 1 is a schematic diagram of an illustrative system suitable for implementation of an application that monitors traffic and protects applications from attacks in accordance with some embodiments of the present invention;

[0019] FIG. 2 is a detailed example of the server and one of the clients of FIG. 1 that may be used in accordance with some embodiments of the present invention;

IPR2025-00069
CrowdStrike EX1002 Page 78

[0020] FIG. 3 is a schematic diagram of another illustrative arrangement suitable for monitoring traffic and protecting applications from attacks in accordance with some embodiments of the present invention;

[0021] FIG. 4 is an illustrative flow diagram for protecting an application from attacks in accordance with some embodiments of the present invention;

[0022] FIG. 5 is a schematic diagram of another illustrative arrangement suitable for monitoring traffic and protecting applications from attacks in accordance with some embodiments of the present invention;

[0023] FIG. 6 is a schematic diagram of another illustrative arrangement suitable for monitoring traffic and protecting applications from attacks in accordance with some embodiments of the present invention;

[0024] FIG. 7 is an example of a pmalloc()-based memory allocation as used in accordance with some embodiments of the present invention; and

[0025] FIG. 8 is an example of a transformation of C code as performed in accordance with some embodiments of the present invention.

Detailed Description of the Invention

[0026] In the following description, numerous specific details are set forth regarding the systems and methods of the present invention and the environment in which such systems and methods may operate, etc., in order to provide a thorough understanding of the present invention. It will be apparent to one skilled in the art, however, that the present invention may be practiced without such specific details, and that certain features which are well known in the art are not described in detail in order to avoid complication of the subject matter of the present invention. In addition, it will be understood that the examples provided below are exemplary, and that it is contemplated that there are other methods and systems that are within the scope of the present invention.

[0027] In accordance with the present invention, systems and methods for improved protection from attacks on an application are provided. These systems and methods provide at least one anomaly detector and at least one honeypot (sometimes referred to as a "shadow honeypot"). These shadow honeypots enable signs of an attack to be detected and enable the application to be protected from such an attack. The anomaly detector monitors all traffic routed to a protected application. Instead of allowing the application to process traffic that is

IPR2025-00069
CrowdStrike EX1002 Page 79

considered anomalous, anomalous traffic is processed by the honeypot. As used herein, the honeypot is an instance of the protected application that shares substantially all internal state with a regular instance of the application. However, the honeypot can be provided in various approaches. For example, in some embodiments, the honeypot application can be at least a portion of the protected application itself. Using the honeypot, attacks against the honeypot are detected and the honeypot repairs the application (e.g., any incurred state changes are discarded). In other embodiments, the application can be restarted and loaded with state information that was saved prior to the attack. Legitimate traffic that is misclassified by the anomaly detector can be validated by the honeypot and can be processed correctly by the system and transparently to the user. It should be noted that a shadow honeypot can be used for protection of both server and client applications.

[0028] Some embodiments of the present invention allow system designers to tune the anomaly detection system for low false negative rates, thereby minimizing the risk of misclassifying a real attack as legitimate traffic, since the honeypot removes any false positives (or a falsely triggered indication of an attack). The present invention can defend against attacks that are tailored against a specific site with a particular internal state.

[0029] FIG. 1 is a schematic diagram of an illustrative system 100 suitable for implementation of systems and methods for protecting an application from attack in accordance with some embodiments of the present invention. Referring to FIG. 1, an exemplary system 100 for implementing the present invention is shown. As illustrated, system 100 can include one or more clients 102. Clients 102 can be local to each other or remote from each other, and are connected by one or more communications links 104 to a communications network 106 that is linked via a communications link 108 to a server 110. Various embodiments of the present application can be implemented on at least of the server and the clients.

[0030] In system 100, server 110 can be any suitable server for executing an application, such as a processor, a computer, a data processing device, or a combination of such devices. Communications network 106 can be any suitable computer network including the Internet, an intranet, a wide-area network (WAN), a local-area network (LAN), a wireless network, a digital subscriber line (DSL) network, a frame relay network, an asynchronous transfer mode (ATM) network, a virtual private network (VPN), or any combination of any of the same. Communications links 104 and 108 can be any communications links suitable for

IPR2025-00069
CrowdStrike EX1002 Page 80

communicating data between clients 102 and server 110, such as network links, dial-up links, wireless links, hard-wired links, etc. Clients 102 can be personal computers, laptop computers, mainframe computers, dumb terminals, data displays, Internet browsers, personal digital assistants (PDAs), two-way pagers, wireless terminals, portable telephones, etc., or any combination of the same. Clients 102 and server 110 can be located at any suitable location. In one embodiment, clients 102 and server 110 can be located within an organization. Alternatively, clients 102 and server 110 can be distributed between multiple organizations.

[0031] The server and one of the clients, which are depicted in FIG. 1, are illustrated in more detail in FIG. 2. Referring to FIG. 2, client 102 can include processor 202, display 204, input device 206, and memory 208, which can be interconnected. In a preferred embodiment, memory 208 contains a storage device for storing a client program for controlling processor 202. Memory 208 can also contain an application for protecting at least one other application from attacks. In some embodiments, applications can be resident in the memory of client 102 or server 110.

[0032] Although the methods and systems of the present invention are described herein as being implemented on a client or server, this is only illustrative. The application can be implemented on any suitable platform (e.g., a personal computer (PC), a mainframe computer, a dumb terminal, a data display, a two-way pager, a wireless terminal, a portable telephone, a portable computer, a palmtop computer, a H/PC, an automobile PC, a laptop computer, a personal digital assistant (PDA), a combined cellular phone and PDA, etc.) to provide such features.

[0033] A simplified illustration of the system of some embodiments according to the present invention is illustrated in FIG. 3. As shown, system 300 includes an anomaly detection sensor 310. Anomaly detection sensor 310 receives traffic from the network 320. Anomaly detection sensor 310 can route traffic to either a protected application 330 or a honeypot version of the application 340. In some embodiments, anomaly detection sensor 310 can route traffic to protected application 330 or the honeypot 340 based on a prediction made by anomaly detection sensor 310. For example, anomaly detection sensor 310 can make a prediction on traffic from the network 320 based at least in part on performing a payload analysis or analyzing network behavior.

IPR2025-00069
CrowdStrike EX1002 Page 81

[0034] As described previously, the honeypot version of the application 340 is an instance of the protected application 330 that shares substantially all internal state with a regular instance of the application. In some embodiments, the honeypot application can be at least a portion of the protected application itself. Using honeypot 340, attacks against the honeypot 340 are detected and any incurred state changes are discarded. Traffic 320 that is misclassified by the anomaly detection sensor 310 can be validated by the honeypot 340 and can be processed correctly by the system 300 and transparently to the user. Both the honeypot 340 and the protected application 330 are connected to the same process state information 350. Generally, process state information 350 can include, for example, variable values, memory allocation information, state information related to associated components or devices, or any other suitable information that may be needed to define the current state of a process.

[0035] In some embodiments, honeypots, such as honeypot 340, can provide anomaly detection sensors or any other suitable component of system 300 with feedback. As shown in FIG. 3, honeypot 340 can provide feedback 360 to anomaly detection sensor 310. For example, honeypot 340 can provide information relating to the attack to the anomaly detection sensor 310. Anomaly detection sensor 310 can use the feedback 360 from honeypot 340 to update the predictors used within anomaly detection sensor 310 or use the feedback 360 in any other suitable approach for tuning anomaly detection sensor 310.

[0036] FIG. 4 is an illustrative flow diagram illustrating the interaction of the anomaly detection sensor and the honeypot in accordance with some embodiments of the present invention. Traffic from a network is received by the system at the anomaly detection sensor (410 in FIG. 4). The anomaly detection sensor determines whether or not the received traffic is an attack on the application (420 in FIG. 4).

[0037] If the anomaly detection sensor predicts that the received traffic is an attack, the received traffic is routed to the honeypot (430 in FIG. 4). Traffic that reaches the honeypot is processed by the honeypot and monitored for attacks (440 in FIG. 4). If no attack is detected by the honeypot, the processing of the code is handled transparently by the system (450 in FIG. 4). From the user's point of view, it appears as though the traffic was processed by the protected application. The honeypot can also inform the anomaly detection sensor that it made a wrong prediction (450 in FIG. 4). The anomaly detection sensor can use this information to improve future predictions made by the anomaly detection sensor. Otherwise,

IPR2025-00069
CrowdStrike EX1002 Page 82

if the honeypot determines that the received traffic is an attack, the honeypot can discard any state changes caused by the attack (460 in FIG. 4). The honeypot can also inform the anomaly detection sensor of a correct prediction. Information relating to correct predictions can also be used to improve future predictions made by the anomaly detection sensor.

[0038] Alternatively, if the anomaly detection sensor predicts that the received traffic is not an attack, the received traffic is routed to the protected application (470 in FIG. 4). In this case, the received traffic is not routed to the honeypot version.

[0039] FIG. 5 shows another illustrative arrangement for the attack detection system in accordance with some embodiments of the present invention. In the arrangement of FIG. 5, system 500 includes a filtering engine 510, an array of anomaly detection sensors 520, a honeypot version of the application 530, a protected application 540, a current process state 550, and a saved process statement for rollback 560.

[0040] Filtering engine 510 receives traffic from the network 570. Filtering engine 510 can be used by system 500 to block known attacks within the received traffic 570. The filtering can be done, for example, based on payload content, source of the attack, a combination of any suitable filtering methodology, or by any other suitable approach for filtering the received traffic. As shown in FIG. 5, filtering engine 510 can be configured as a layer between the array of anomaly detection sensors 520 and the traffic from the network 570. Filtering engine 510 can be used to drop specific types of traffic before any additional processing is performed.

[0041] If traffic from the network 570 passes through filtering engine 510, the array of one or more anomaly detection sensors 520 can be used to process the received traffic 570. Examples of types of anomaly detection sensors 520 that can be used in system 500 include sensors that perform payload analysis and network behavior anomaly detectors. However, it should be noted that any suitable anomaly detection sensor can be used in accordance with the present invention.

It should be noted that results can improve if the anomaly detection sensors 520 are tuned to a high sensitivity. While this increases the amount of false positives reported by the anomaly detection sensors 520, it further ensure that attacks do not reach the protected application 540.

[0042] Based at least in part on the prediction of the one or more anomaly detection sensors 520, system 500 invokes either the regular instance of the protected application 540 or the honeypot version of the application 530. As described previously, the honeypot

IPR2025-00069
CrowdStrike EX1002 Page 83

version of the application 530 is an instrumented instance of the application that shares substantially all internal state with a regular instance of the application. Using honeypot 530, attacks against the honeypot 530 are detected and any incurred state changes are discarded. Both the honeypot 530 and the protected application 540 are connected to the same process state information 550.

However, in response to detecting an attack or failure, honeypot 530 can rollback any state changes to a known good state. For example, honeypot 530 can rollback to the state the protected application 540 had prior to processing the malicious request (e.g., a saved process statement for rollback 560). Alternatively, honeypot 530 can restart the application or initiate a new instance of the application having previously saved state information in response to detecting an attack.

[0043] In some embodiments, honeypot 530 can provide filtering engine 510, one or more anomaly detection sensors 520, or any other suitable component of system 500 with feedback. For example, in response to the honeypot 530 detecting an actual attack, determining a false positive, or detecting no attacks, honeypot 530 can provide information to one or more of the anomaly detection sensors 520. The one or more anomaly detection sensors 520 can use the feedback 580 from honeypot 530 to update the predictors used within the one or more anomaly detection sensors 520 or use the feedback 580 in any other suitable approach for tuning the one or more anomaly detection sensors 520. For example, the one or more anomaly detection sensors 520 can use the information to block similar attacks in the future and/or learn from past correct and incorrect predictions. In another example, predictors or prediction models can be updated if no attacks are detected. Any other suitable approach for self-tuning and updating the one or more anomaly detection sensors 520 can also be used.

[0044] In another example, in response to the honeypot 530 detecting an actual attack, determining a false positive, or detecting no attacks, honeypot 530 can provide information (e.g., feedback 590) to filtering engine 510. Filtering engine 510 can use the feedback 590 from honeypot 530 to update the filters used by filtering engine 510 or use the feedback 590 in any other suitable approach for tuning the filtering engine 510. For example, filtering engine 510 can use the feedback 590 to block similar attacks in the future and/or learn from past correct and incorrect predictions. Any other suitable approach for self-tuning and updating the filtering engine 510 can also be used.

IPR2025-00069
CrowdStrike EX1002 Page 84

[0045] It should be noted that traffic through system 500, including attack traffic, can interact with the protected application through processing by filtering engine 510 and one or more anomaly detection sensors 520, where side channel access is not permitted.

[0046] Certain embodiments of the present invention can be integrated with both servers and clients.

[0047] In some embodiments, the shadow honeypot can be tightly coupled with a server. The server application can be protected by having suspicious requests diverted to a honeypot version of the server application in which the server application and the honeypot have mirrored functionality and state. The protected application can be, for example, a web server.

[0048] In some embodiments, the shadow honeypot can be tightly coupled with a client. The client application can be protected from, for example, passive attacks where the attacker lures a user of the client to download data containing an attack (e.g., the recent buffer overflow vulnerability in Microsoft Internet Explorer's JPEG handling). The protected application can be used to protect, for example, a web browser or any other application on the client from an attack contained in a single packet, an entire flow, or a set of flows.

[0049] Although the present invention has been described and illustrated in the foregoing exemplary embodiments as tightly coupled so that attackers cannot exploit the differences between the state of the honeypot and the state of application because both share the same state, it should be noted that the present disclosure has been made only by way of example, and that numerous changes in the details of construction and combination and arrangement of processes and equipment can be made without departing from the spirit and scope of the invention. For example, a loosely coupled configuration in accordance with some embodiments of the present invention can be provided. The honeypot can reside on a different system and would not share state with the protected application. This loosely coupled embodiment allows the honeypot to be managed by a separate entity, thereby providing the user with the ability to outsource the management of the honeypot.

[0050] As shown, the filtering and anomaly detection components (e.g., filtering engine 510 and one or more anomaly detection sensors 520) can be tightly coupled with the protected application. Alternatively, the filtering and anomaly detection components can be centralized at a natural aggregation point in the network topology, such as the firewall.

[0051] FIG. 6 shows a diagram of another illustrative arrangement for the attack detection system in accordance with some embodiments of the present invention. As shown

IPR2025-00069
CrowdStrike EX1002 Page 85

in the arrangement of FIG. 6, the filtering and anomaly detection components can be implemented with a network processor as a scalable custom load balancer and an array of snort sensors running on computers connected to the network processor board that implement all detection heuristics. For example, the selected network processor can be an IXP1200 network processor. In some embodiments, none of the detection heuristics are implemented on it as network processors are designed for simple forwarding and lack the processing capacity required for the necessary speeds and can be harder to program and debug than other processors. However, in some embodiments, detection heuristics can be implemented on the network processor.

[0052] The anomaly detection component provides the ability to divert potentially malicious requests to the honeypot. For example, in web servers, a reasonable definition of the attack context is an HTTP request. For this purpose, the anomaly detection component constructs a request, runs the anomaly detection heuristics, and forwards the request depending on the outcome. Since this processing can be performed at the HTTP level, a HTTP proxy-like function is provided. The anomaly detection components for the tightly coupled honeypot server can be implemented by augmenting an HTTP proxy with the ability to apply the Abstract Payload Execution detection heuristic on incoming request and route them according to its decision.

[0053] For the client scenario, an alternating solution based on passive monitoring can be used. In this configuration, the TCP streams of HTTP connections can be reconstructed and the HTTP protocol can be decoded to extract suspicious objects. An object can then be examined directly by applying a heuristic algorithm. If the object is deemed suspicious, a server is launched that replays the suspicious response and directs a honeypot browser to this server.

[0054] Payload sifting and buffer overflow detection via abstract payload execution can be used as heuristics for anomaly detection. The payload sifting algorithm derives fingerprints of rapidly spreading worms by identifying popular substrings in network traffic. Buffer overflow detection via abstract payload execution detects buffer overflow attacks by searching for sufficiently long sequences of valid instructions in network traffic. Long sequences of valid instructions can appear in non-malicious data and this is where the honeypot can be implemented. This detection mechanism is attractive because it can be applied to individual attacks and triggers detection upon encountering the first instance of an

IPR2025-00069
CrowdStrike EX1002 Page 86

attack. This is unlike many anomaly detection mechanisms that are required to witness multiple attacks before flagging the attacks as anomalous.

[0055] In some embodiments, a code transformation tool can be used to create a honeypot. This tool receives the original application as input and inserts in the honeypot code. While memory-violation errors are primarily described in these embodiments, it should be noted that the present invention can also be used to catch and detect other violations. TXL, a hybrid functional and rule based language, can be used to perform the code transformations, where GCC C (GNU C Compiler) can be used as the front end. TXL is well suited for performing source-to-source transformation, however a very wide variety of languages could also be used. The grammar responsible for parsing the source input is specified in a notation similar to Extended Backus Naur.

[0056] In some embodiments, the honeypot is created by moving all static buffers to the heap. Static buffers can be moved to the heap by dynamically allocating each buffer upon entering the function in which it was previously declared. These buffers can be de-allocated upon exiting the function, whether implicitly (e.g., by reaching the end of the function body) or explicitly (e.g., through a return statement). It should be noted that because the allocated memory regions are instrumented, illegal accesses regarding pointer aliasing are detected.

[0057] For memory allocation, a new version of malloc(), called pmalloc(), was created. FIG. 7 is an illustrative example of a pmalloc()-based memory allocation in accordance with some embodiments of the present invention. As shown in FIG. 7, the pmalloc()-based memory allocation allocates three memory pages 710. Besides the basic one page, pmalloc() allocates two additional zero filled, write-protected pages 720 that bracket the requested buffer. The extra pages can be mmap()'ed from /dev/zero as read-only. Because mmap() operates at memory page granularity, memory requests are rounded up to the nearest page. The pointer 730 that is returned by pmalloc() can be adjusted to immediately catch any buffer overflow or underflow.

[0058] FIG. 8 shows an example of a code translation in accordance with some embodiments of the present invention. The original code is shown in block 810 and the translated code is shown in block 820. Buffers that are allocated via malloc() can be switched to pmalloc() 830. This can be achieved by examining declarations in the source and transforming them to pointers where the size is allocated with a malloc() function call. The C grammar can also be adjusted to free the memory 840 before the function returns.

IPR2025-00069
CrowdStrike EX1002 Page 87

[0059] Any overflow or underflow on a buffer allocated via pmalloc() can cause the process to receive a Segmentation Violation (SEGV) signal, which is caught by a signal handler that is added to the source code in main(). The signal handler notifies the operating system to abort all state changes made by the process while processing this request. To do this, a new system call to the operating system can be added called transaction(). The transaction() function is conditionally invoked at three location in the code at the discretion of the shadow_enable() function. The shadow_enable() function returns true when the honeypot version of the code is running.

[0060] The first location that transaction() is placed is inside the main processing loop prior to beginning the handling of a new request. This indicates to the operating system that a new transaction has begun. The operating system makes a backup of all memory page permissions and marks all heap memory pages as read-only. As the process executes and modifies these pages, the operating system maintains a copy of the original page and allocates a new page, which is given the permissions the original page from the backup, for the process to use. This is done in the same way that copy-on-write works in modern operating systems. This call to transaction() can be placed manually by, for example, the programmer or system designer. Both copies of the page are maintained until transaction() is called again, as will be described below.

[0061] After the end of handling a request, inside the main processing loop, is the second location transaction() can be invoked. It is done here to indicate to the operating system that a transaction has successfully completed. The operating system then discards all original copies of memory pages that have been modified during processing the request. This call to transaction can also be placed manually.

[0062] The third location that transaction can be invoked is inside the signal handler. This location can be installed automatically by embodiments of the present invention. This is done to indicate to the operating system that an attack (exception) has been detected. The operating system then discards all modified memory pages by restoring the original pages.

[0063] In some embodiments, a similar mechanism as the one described above can be built around a file system. This can be done, for example, by using a private copy of a buffer cache for the processing done in the honeypot version of the code.

[0064] It is to be understood that the invention is not limited in its application to the details of construction and to the arrangements of the components set forth in the following

IPR2025-00069
CrowdStrike EX1002 Page 88

description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced and carried out in various ways. Also, it is to be understood that the phraseology and terminology employed herein are for the purpose of description and should not be regarded as limiting.

[0065] As such, those skilled in the art will appreciate that the conception, upon which this disclosure is based, can readily be utilized as a basis for the designing of other structures, methods and systems for carrying out the several purposes of the present invention. It is important, therefore, that the claims be regarded as including such equivalent constructions insofar as they do not depart from the spirit and scope of the present invention.

[0066] Although the present invention has been described and illustrated in the foregoing exemplary embodiments, it is understood that the present disclosure has been made only by way of example, and that numerous changes in the details of implementation of the invention can be made without departing from the spirit and scope of the invention, which is limited only by the claims which follow.

IPR2025-00069
CrowdStrike EX1002 Page 89

What is claimed is:

1. A method for protecting applications from attacks, the method comprising:

receiving traffic from a communication network that is attempting to reach an application;

transmitting the received traffic through an anomaly detection component, wherein the anomaly detection component predicts whether the received traffic is a potential attack on the application and wherein the anomaly detection component is tuned to achieve a low false negative rate;

receiving an indication from the anomaly detection component relating to the prediction of the potential attack on the application;

in response to receiving the indication from the anomaly detection component, transmitting the received traffic to a honeypot, wherein the honeypot is an instance of the application that shares state information with the application and wherein the honeypot monitors the received traffic for attacks on the application;

receiving an indication from the honeypot that the received traffic is an attack on the application; and

receiving an instruction from the honeypot to repair the state information of the application.

2. The method of claim 1, wherein the repair further comprises rolling back the state information of the application to previously saved state information.

3. The method of claim 1, wherein the repair further comprises discarding the state information of the application.

4. The method of claim 1, wherein the repair further comprises initiating a new instance of the application with previously saved state information.

5. The method of claim 1, further comprising filtering the received traffic prior to transmitting the received traffic to the anomaly detection component.

IPR2025-00069
CrowdStrike EX1002 Page 90

6. The method of claim 5, where the filtering is based on at least one of payload content and source of the attack.

7. The method of claim 1, further comprising transmitting feedback from the honeypot to the anomaly detection component.

8. The method of claim 7, further comprising updating the anomaly detection component based at least in part on the feedback from the honeypot.

9. The method of claim 7, further comprising updating at least one of predictors and models associated with the anomaly detection component.

10. The method of claim 7, further comprising using the feedback to automatically tune the anomaly detection component.

11. The method of claim 7, further comprising using the feedback to automatically tune a filter.

12. The method of claim 1, wherein the application is one of a server application, a client application, an operating system, and an application on a mainframe.

13. The method of claim 1, further comprising:
providing a filter before the anomaly detection component;
transmitting feedback from the honeypot to the filter; and
updating the filter based at least in part on the feedback from the honeypot.

14. A system for protecting applications from attacks, the system comprising:
an anomaly detection component that is tuned to achieve a low false negative rate, wherein the anomaly detection component is configured to:
receive traffic from a communication network that is attempting to reach an application; and

IPR2025-00069
CrowdStrike EX1002 Page 91

predict whether the received traffic is a potential attack on the application; and

a honeypot that is an instance of the application that shares state information with the application, wherein the honeypot is configured to:

receive an indication from the anomaly detection component relating to the prediction of the potential attack;

monitor the received traffic for attacks on the application; and

in response to determining that the received traffic is an attack on the application, repair the state information of the application.

15. The system of claim 14, wherein the honeypot is further configured to roll back the state information of the application to previously saved state information.

16. The system of claim 14, wherein the honeypot is further configured to discard the state information of the application.

17. The system of claim 14, wherein the honeypot is further configured to initiate a new instance of the application with previously saved state information.

18. The system of claim 14, further comprising a filter that filters the received traffic prior to transmitting the received traffic to the anomaly detection component.

19. The system of claim 14, wherein the honeypot is further configured to transmit feedback from the honeypot to the anomaly detection component.

20. The system of claim 19, wherein the anomaly detection component is further configured to update the anomaly detection component based at least in part on the feedback from the honeypot.

21. The system of claim 19, wherein the anomaly detection component is further configured to update at least one of predictors and models associated with the anomaly detection component.

IPR2025-00069
CrowdStrike EX1002 Page 92

22. The system of claim 19, wherein the anomaly detection component is further configured to tune the anomaly detection component based at least in part of the feedback.

23. The system of claim 14, further comprising a filter configured to receive the traffic before the anomaly detection component, wherein the filter receives feedback from the honeypot and is updated based at least in part on the feedback from the honeypot.

IPR2025-00069
CrowdStrike EX1002 Page 93

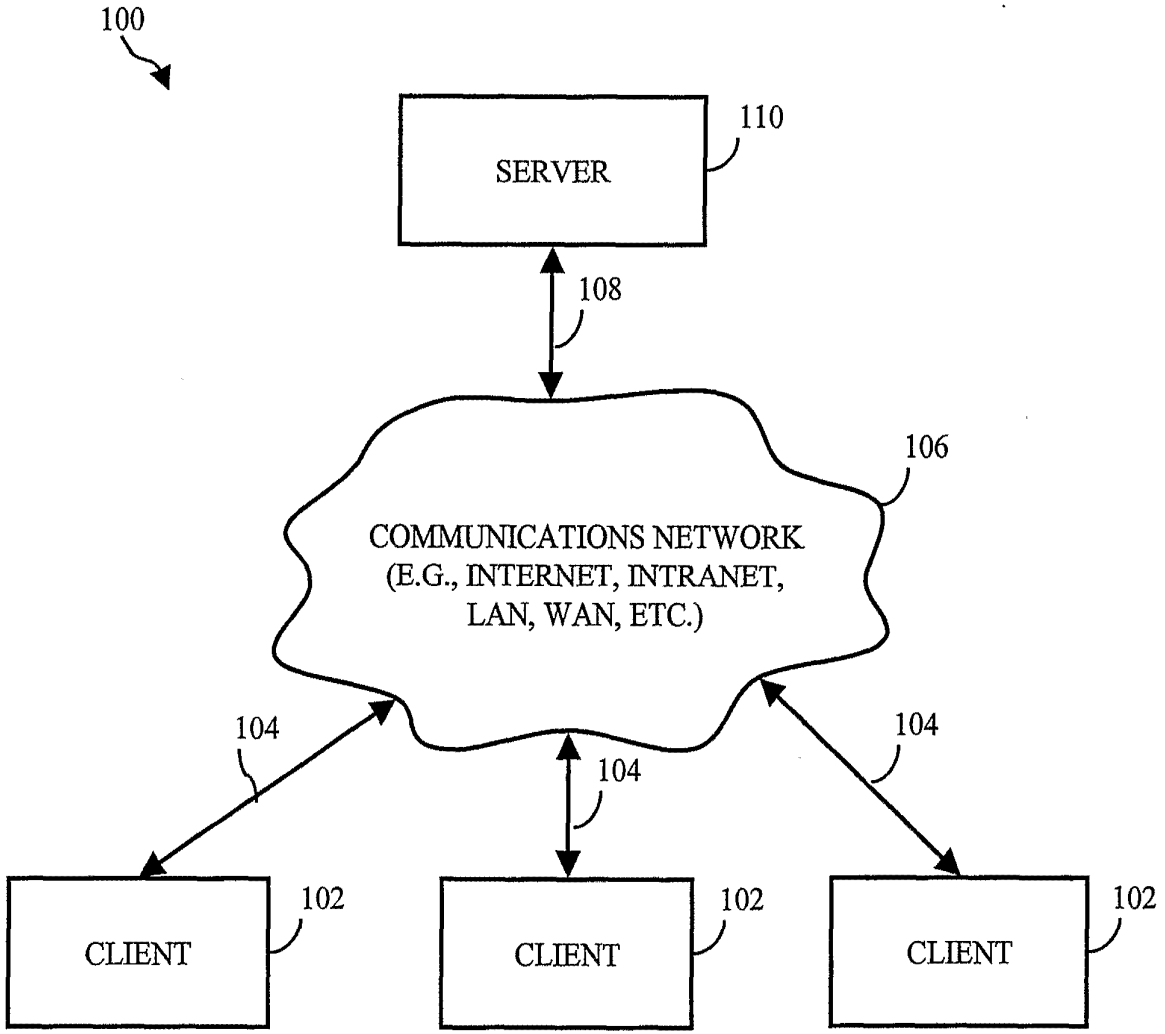

100
SERVER
110
108
106
COMMUNICATIONS NETWORK
(E.G., INTERNET, INTRANET,
LAN, WAN, ETC.)
104
104
104
CLIENT
102
CLIENT
102
CLIENT
102

FIG. 1

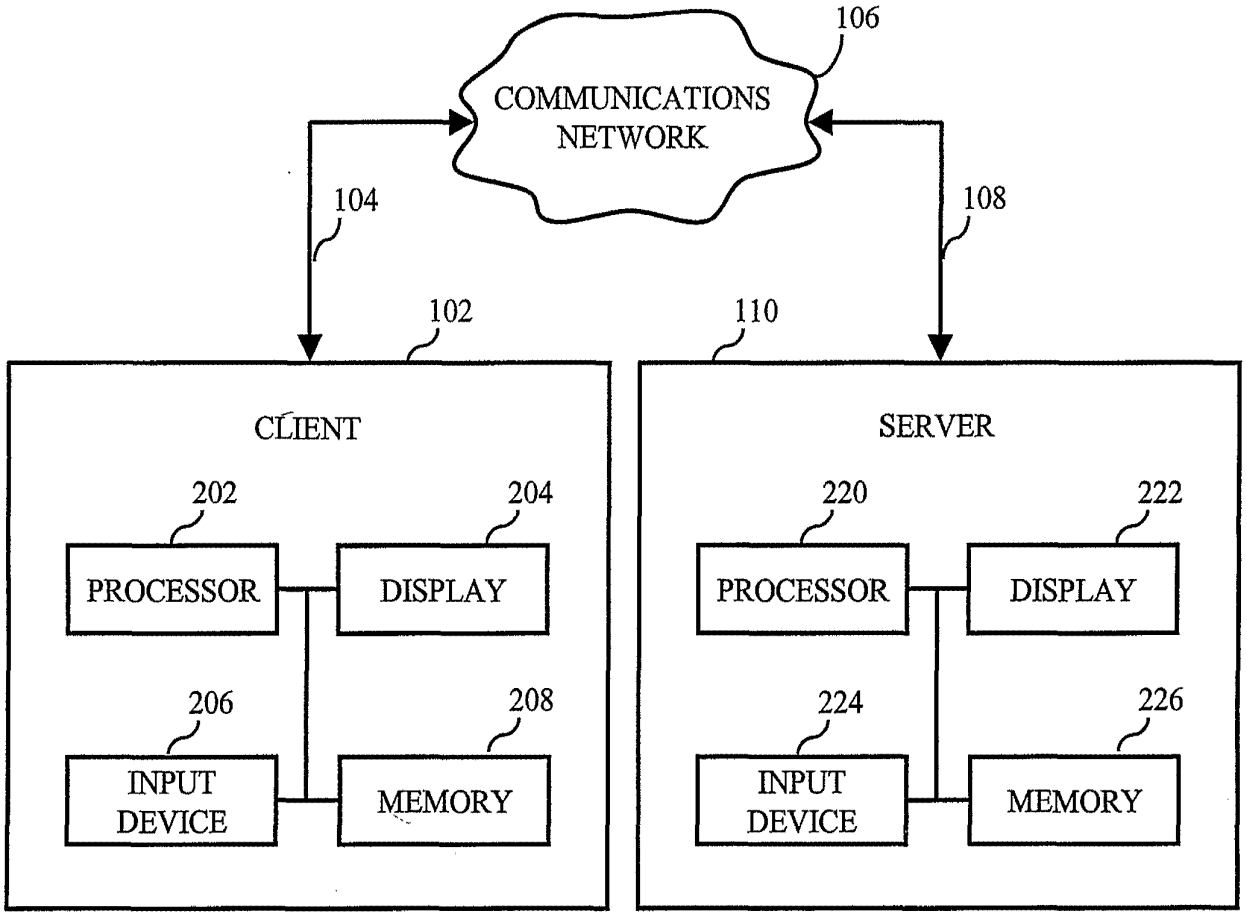

106
COMMUNICATIONS NETWORK
104
108
102
110
CLIENT
SERVER
202
204
220
222
PROCESSOR
DISPLAY
PROCESSOR
DISPLAY
206
208
224
226
INPUT DEVICE
MEMORY
INPUT DEVICE
MEMORY

FIG. 2

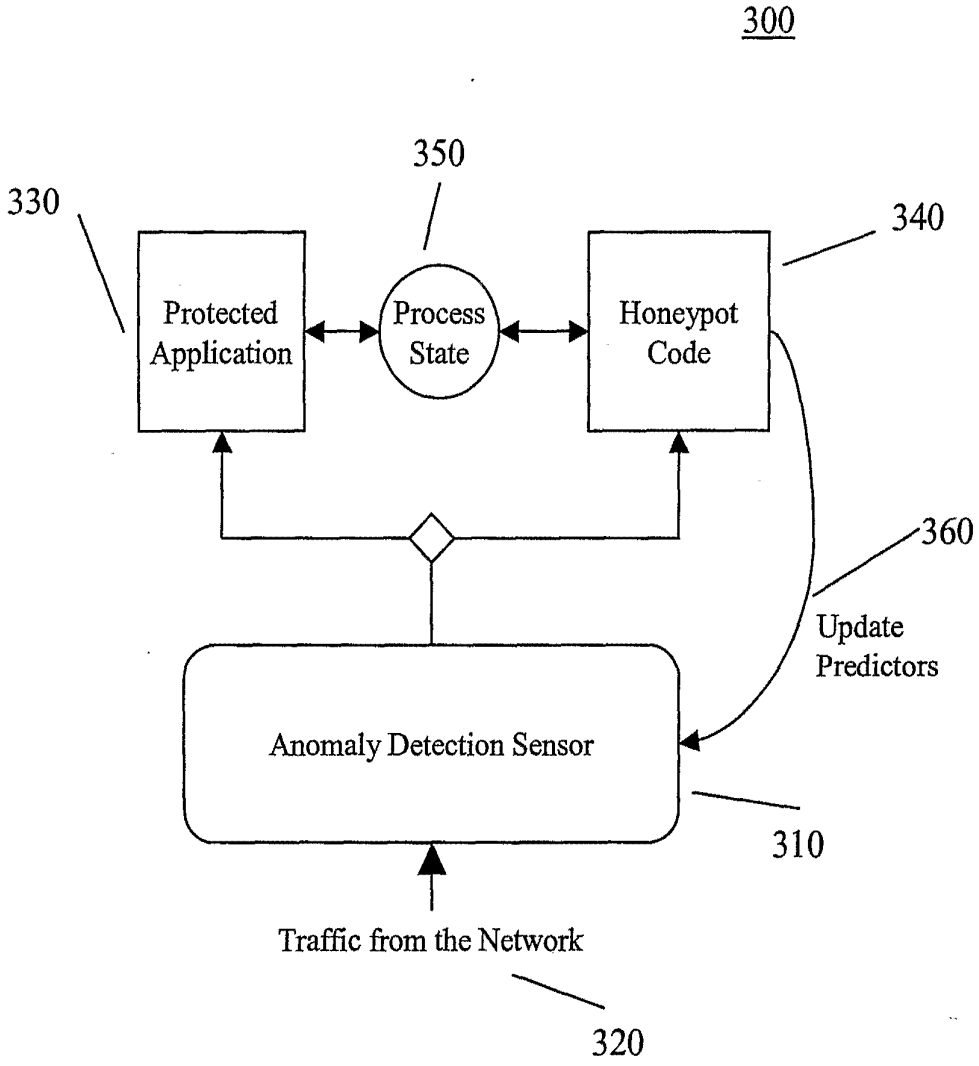

300
350
330
340
Protected Application
Process State
Honeypot Code
360
Update Predictors
Anomaly Detection Sensor
310
Traffic from the Network
320

FIG. 3

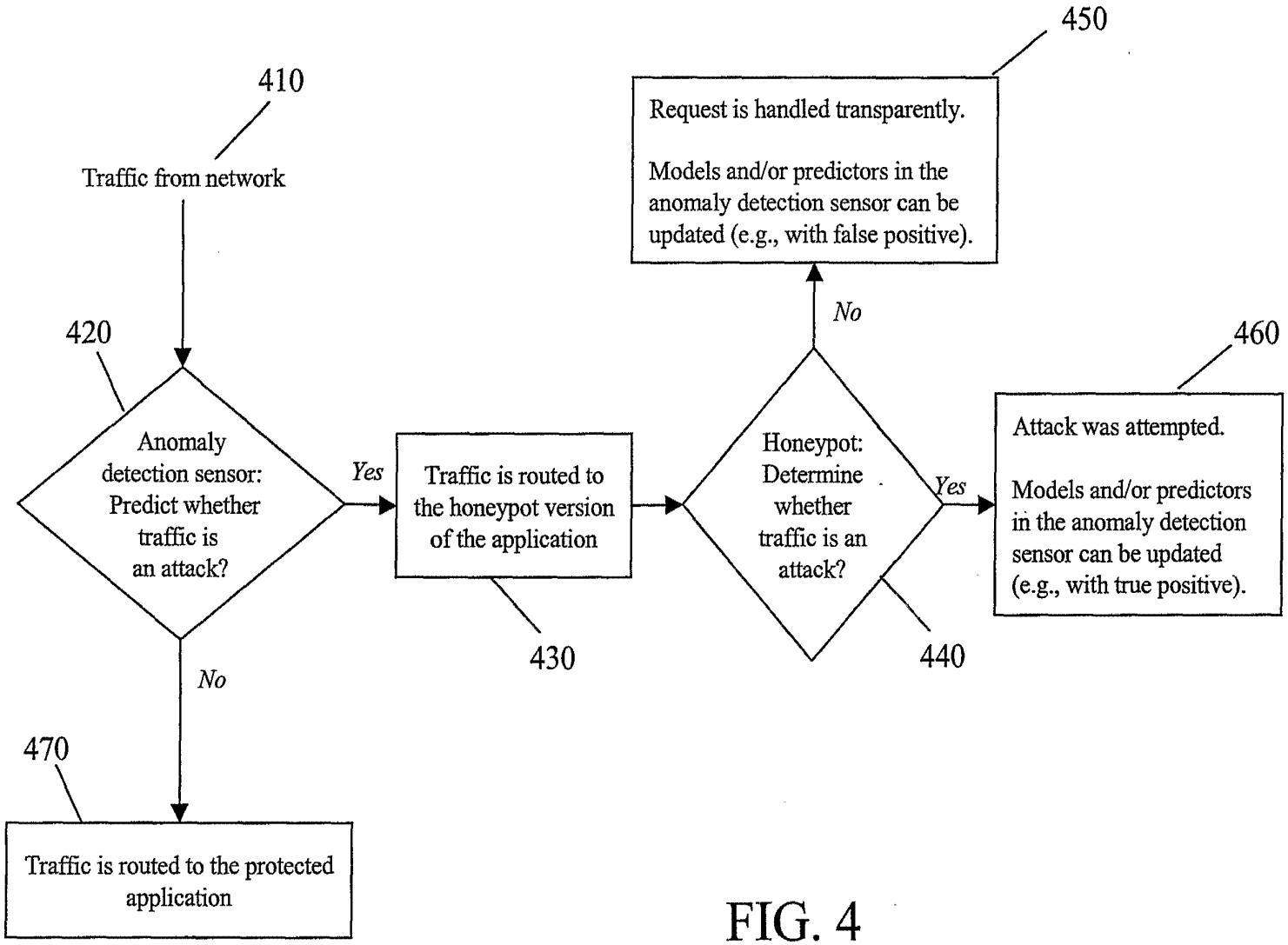

410
Traffic from network
420
Anomaly detection sensor: Predict whether traffic is an attack?
Yes
Traffic is routed to the honeypot version of the application
430
Honeypot: Determine whether traffic is an attack?
440
Yes
Attack was attempted.
Models and/or predictors in the anomaly detection sensor can be updated (e.g., with true positive).
460
No
Request is handled transparently.
Models and/or predictors in the anomaly detection sensor can be updated (e.g., with false positive).
450
No
470
Traffic is routed to the protected application

FIG. 4

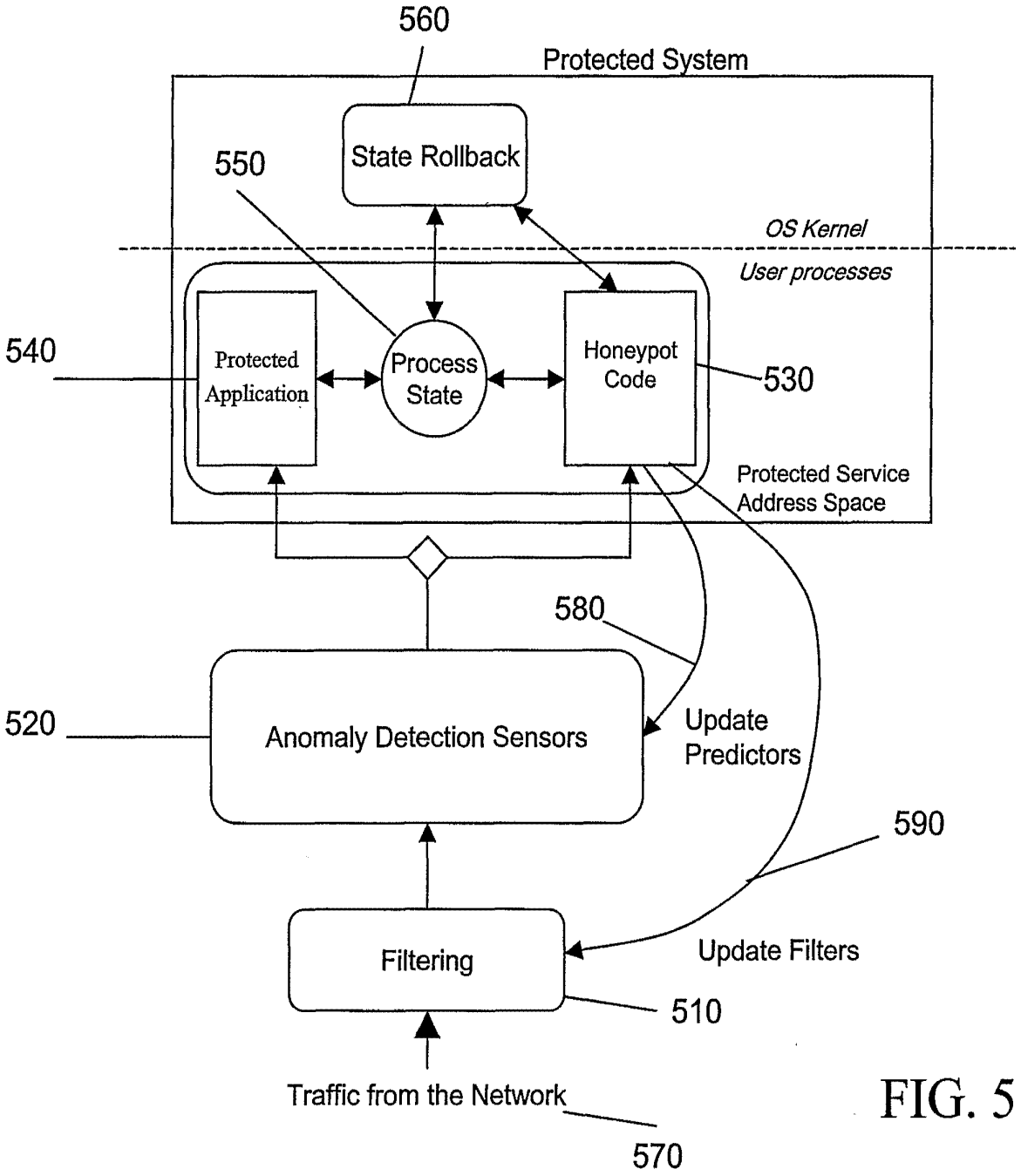

560
Protected System
State Rollback
550
OS Kernel
User processes
540
Protected Application
Process State
Honeypot Code
530
Protected Service Address Space
580
520
Anomaly Detection Sensors
Update Predictors
590
Filtering
Update Filters
510
Traffic from the Network
570

FIG. 5

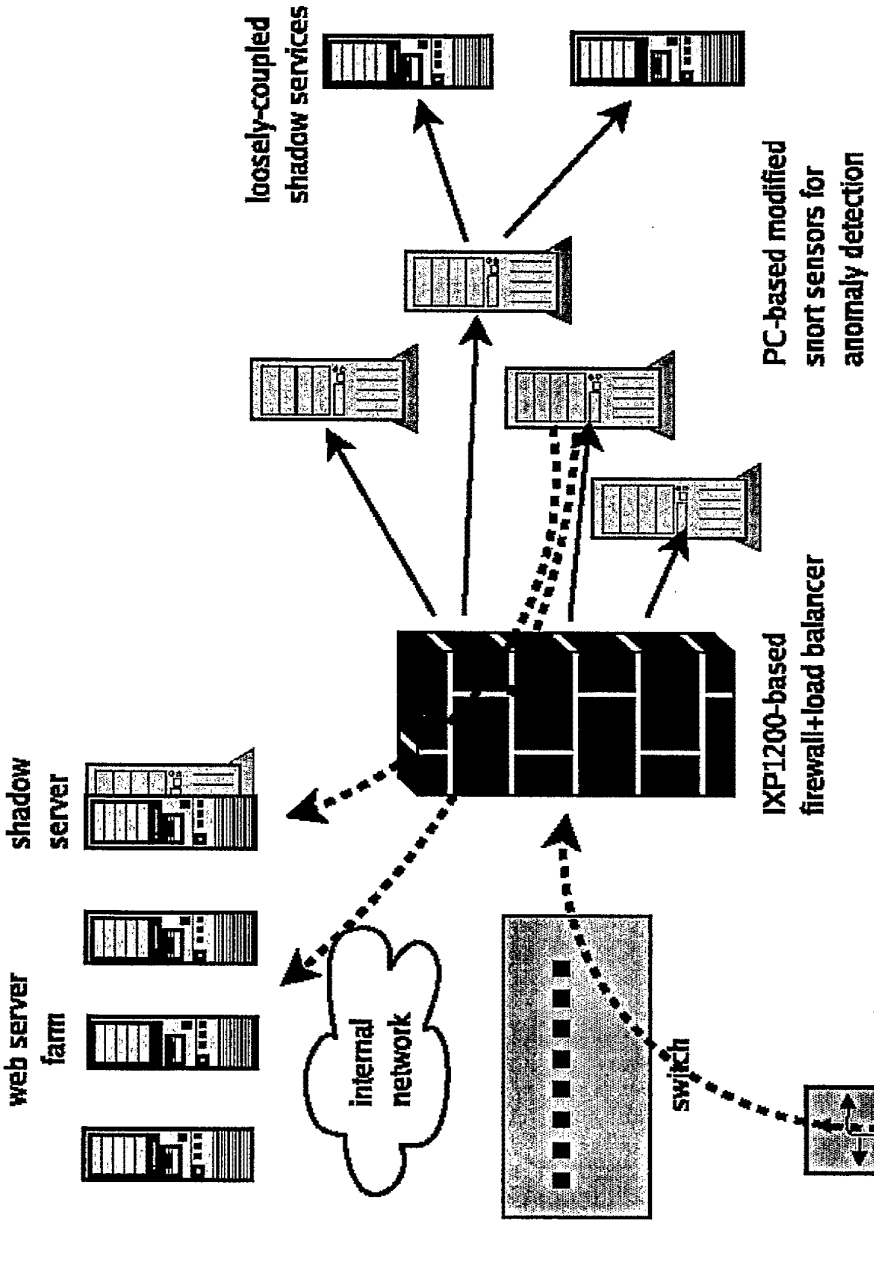


FIG. 6

IPR2025-00069
CrowdStrike EX1002 Page 99

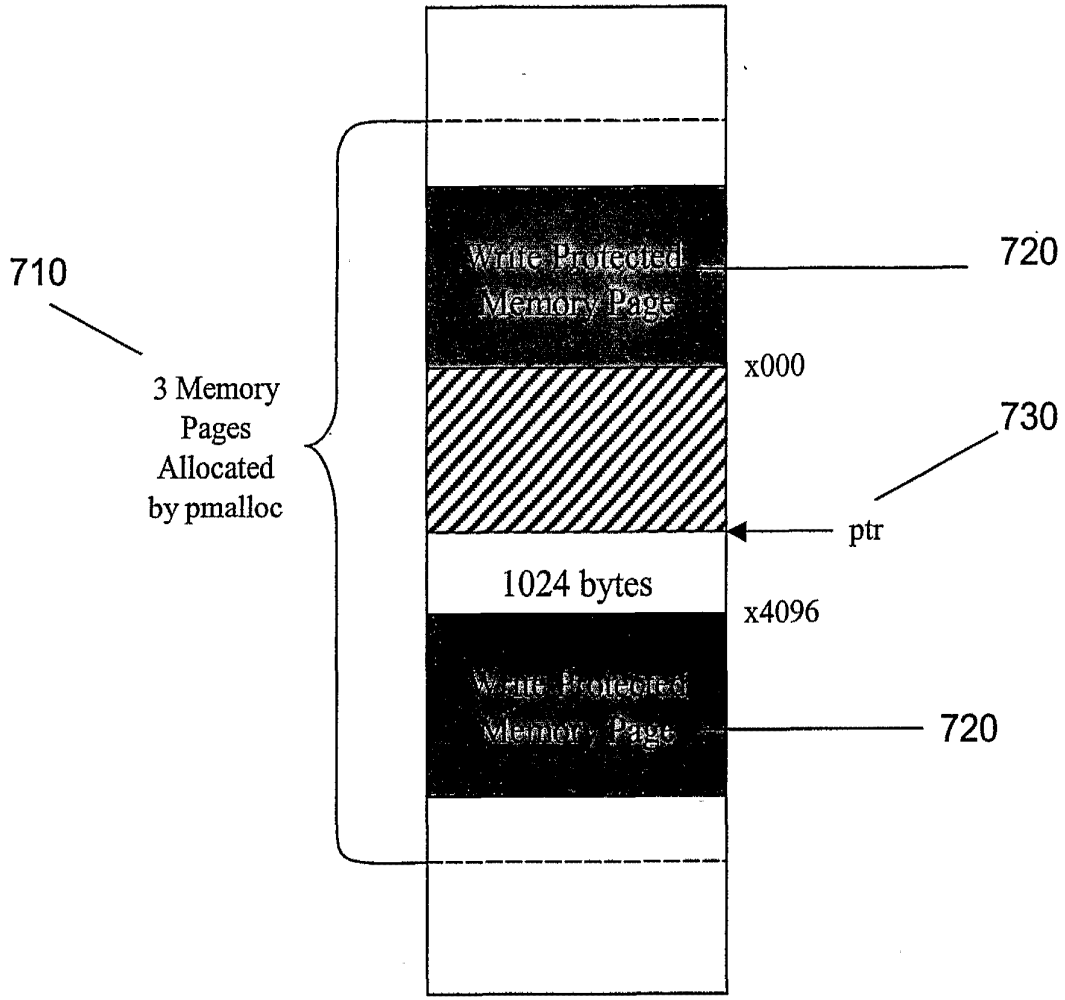

710
3 Memory Pages Allocated by pmalloc
Write Protected Memory Page
720
x000
730
ptr
1024 bytes
x4096
Write Protected Memory Page
720

FIG. 7

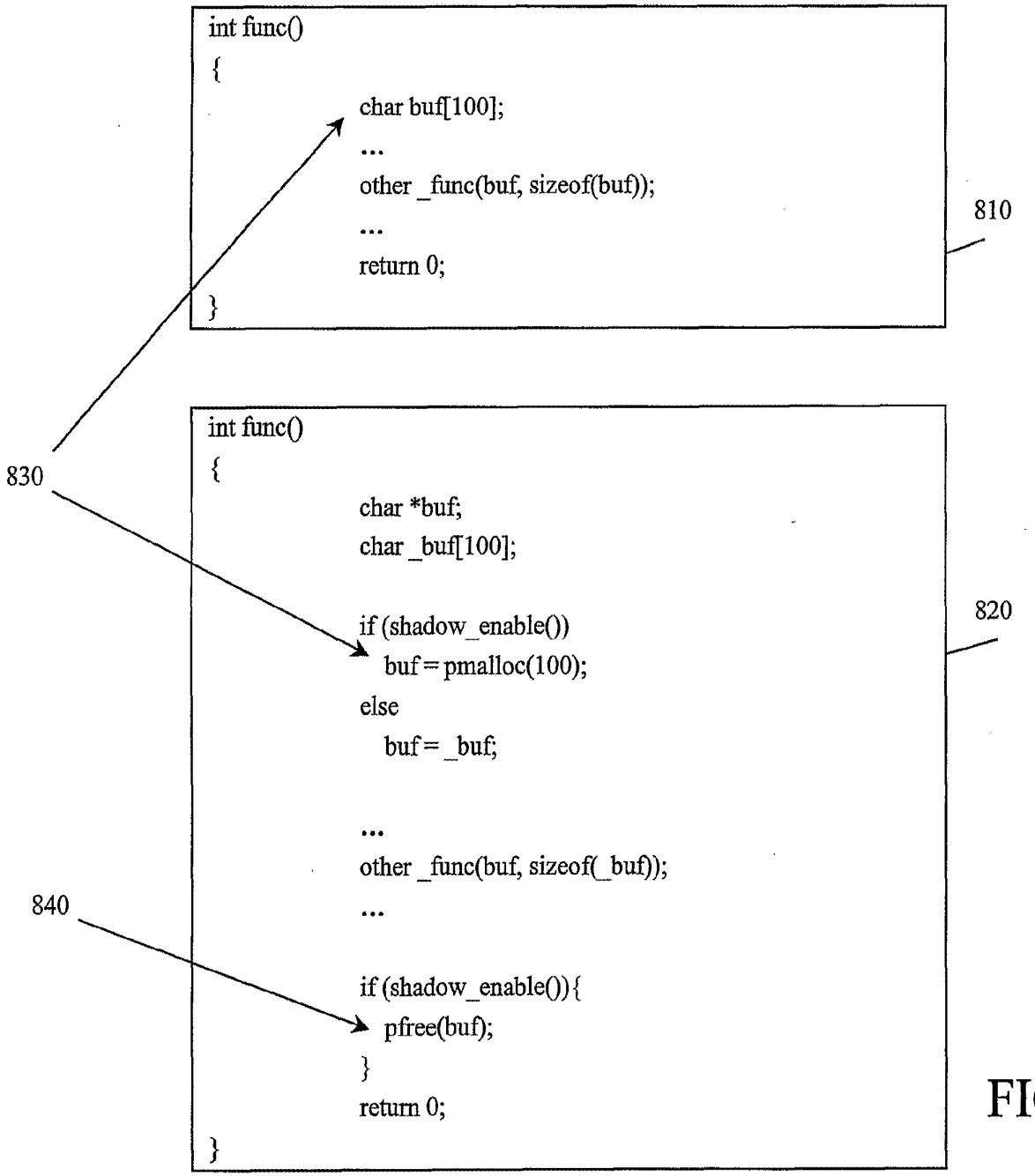


FIG. 8

IPR2025-00069
CrowdStrike EX1002 Page 101

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US06/14704

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **G06F 11/00**(2006.01),**11/22**(2006.01),**11/30**(2006.01)

USPC: 726/5,23,25
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 726/5, 23, 25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	US 2006/0068755 A1 (SHRAIM et al) 30 March 2006 (30.03.2006), [0041]; [0047]-[0048]; [0052]; [0056]-[0066]; [0071]; [0073]; [0074]; [0097]; [0069]-[0078]; [0080][0161]-[0162]; [0203]-[0205]	1-23

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
07 July 2006 (07.07.2006)

Date of mailing of the international search report
29 AUG 2006

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-3201

Authorized officer
Gilberto Barron

Telephone No. 571-272-2100

Form PCT/ISA/210 (second sheet) (April 2005)

67292-5004-WO
DMB / TWK

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

To:
Bregman, Dion M.
MORGAN LEWIS & BOCKIUS LLP
3000 El Camino Real, Suite 700
2 Palo Alto Square
Palo Alto, CA 94306
ETATS-UNIS D'AMERIQUE

DOCKETED

File Art. 19 Amendment Final: 04DEC2011
File Art. 34 Amendment Final: 24APR2012
US File IDS/PCT Search Report Due: 04JAN2012

Applicant's or agent's file reference 067292-5004WO ✓	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US2011/041119 ✓ PREVIOUSLY DOCKETED	International filing date *(day/month/year)* 20 June 2011 (20-06-2011) ✓
Applicant NEURALIQ, INC. ✓ File PCT Demand (19 mos.) Final: 24JAN2012	Date of mailing *(day/month/year)* 4 October 2011 (04-10-2011)

1. ☒ The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. ☐ **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   ☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   ☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer ZEISELMAIR, Sabine Tel: +49 (0)89 2399-2151

RECEIVED DOCKETING
OCT 04 2011

Form PCT/ISA/220 (July 2010)

MORGAN LEWIS
PALO ALTO OFFICE

IPR2025-00069
CrowdStrike EX1002 Page 103

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
067292-5004WO ✓		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2011/041119 ✓	20/06/2011 ✓	24/06/2010 ✓
Applicant		
NEURALIQ, INC. ✓		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title**,
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

IPR2025-00069
CrowdStrike EX1002 Page 104

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/041119

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00 G06F11/36
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Lionel Litty ET AL: "Hypervisor Support for Identifying Covertly Executing Binaries", SS'08 Proceedings of the 17th conference on Security symposium, 31 December 2008 (2008-12-31), pages 1-16, XP55007124, [retrieved on 2011-09-14]	17-20
Y	abstract; figure 1 page 1, column 1, paragraph 2 page 4, column 2, paragraph 5 page 5, column 1, paragraph 1 page 5, column 2, paragraph 2 page 10, column 2, paragraph 5	1-16

-/---

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 September 2011	04/10/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Koblitz, Birger

1

Form PCT/ISA/210 (second sheet) (April 2005)

IPR2025-00069
CrowdStrike EX1002 Page 105

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/041119

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 664 159 A (RICHTER DAVID E [US] ET AL) 2 September 1997 (1997-09-02)	1-16
A	abstract; figures 1,10 column 1, line 55 - column 2, line 29	17-20
A	KURNIADI ASRIGO ET AL: "Using VMM-Based Sensors to Monitor Honeypots", 20060614; 20060614 - 20060616, 14 June 2006 (2006-06-14), pages 13-23, XP007902017, ISBN: 978-1-59593-332-4 the whole document	1-20
A	Ashlesha Joshi ET AL: "Detecting Past and Present Intrusions through VulnerabilitySpecific Predicates", , 26 October 2005 (2005-10-26), pages 1-14, XP55006679, Brighton, United Kingdom Retrieved from the Internet: URL:http://www.cs.princeton.edu/courses/archive/spring06/cos592/bib/intrusions_sosp-joshi05.pdf [retrieved on 2011-09-09] the whole document	1-20
A	"Debug Register", , 22 March 2010 (2010-03-22), XP55007207, [retrieved on 2011-09-15] the whole document	1-20
A	Andrés Krapf: "XEN Memory Management (Intel IA-32)", , 30 October 2007 (2007-10-30), XP55007240, Retrieved from the Internet: URL:http://www-sop.inria.fr/everest/personnel/Andres.Krapf/docs/xen-mm.pdf [retrieved on 2011-09-15] the whole document	1-20

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

IPR2025-00069
CrowdStrike EX1002 Page 106

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2011/041119

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5664159 A	02-09-1997	US 5440710 A	08-08-1995
		US 5652872 A	29-07-1997
		US 5598553 A	28-01-1997

IPR2025-00069
CrowdStrike EX1002 Page 107

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2011/041119	20.06.2011	24.06.2010

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00 G06F11/36

Applicant
NEURALIQ, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☐ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Koblitz, Birger Telephone No. +49 89 2399-5890

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-16
	No:	Claims	17-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1 Lionel Litty ET AL: "Hypervisor Support for Identifying Covertly Executing Binaries",
SS'08 Proceedings of the 17th conference on Security symposium, 31 December 2008 (2008-12-31), pages 1-16, XP55007124,
[retrieved on 2011-09-14]

D2 US 5 664 159 A (RICHTER DAVID E [US] ET AL) 2 September 1997 (1997-09-02)

D3 KURNIADI ASRIGO ET AL: "Using VMM-Based Sensors to Monitor Honeypots",
20060614; 20060614 - 20060616, 14 June 2006 (2006-06-14), pages 13-23, XP007902017,
ISBN: 978-1-59593-332-4

D4 Ashlesha Joshi ET AL: "Detecting Past and Present Intrusions through VulnerabilitySpecific Predicates",
, 26 October 2005 (2005-10-26), pages 1-14, XP55006679,
Brighton, United Kingdom
Retrieved from the Internet:
URL:http://www.cs.princeton.edu/courses/archive/spring06/cos592/bib/intrusions_sosp-joshi05.pdf
[retrieved on 2011-09-09]

D5 "Debug Register",
, 22 March 2010 (2010-03-22), XP55007207,
[retrieved on 2011-09-15]

D6 Andrés Krapf: "XEN Memory Management (Intel IA-32)",
, 30 October 2007 (2007-10-30), XP55007240,
Retrieved from the Internet:
URL:http://www-sop.inria.fr/everest/personnel/Andres.Krapf/docs/xen-mm.pdf
[retrieved on 2011-09-15]

1 The present application does not meet the criteria of Article 33(3) PCT, because the subject-matter of claim 1 does not involve an inventive step.

1.1 Document D1 is regarded as being the prior art closest to the subject-matter of claim 1, and discloses (the references in parentheses referring to that D1):

A computer implemented method of identifying unauthorized activities on a computer system ("In this paper, we introduce Patagonix, a hypervisor-based system that detects and identifies covertly executing binaries...", page 1, column 1, paragraph 2), said computer system comprising: one or more processors (Patagonix runs on x86 processors, page 4, column 2, paragraph 5); and memory segmented into multiple pages (page 4, column 2, paragraph 5), said memory storing one or more programs for execution by the one or more processors (see above: covertly executing binaries), said method comprising:

locating a list of target addresses ("To identify code in memory, the identity oracles require the contents of the code page being executed, the virtual address at which the page is located, and the process the code comes from", page 5, column 1, last paragraph.);

while executing at least one of the one or more programs:

in response to detecting a request to execute an instruction located at a first address of a first page ("sets the NX-bit on all pages in the monitored VM so that it will receive a trap from the processor when a code page is executed", page 5, column 1, paragraph 1):

locating a first page table entry corresponding to the first page, the first page table entry having a first executability state (implicit: this is how an x86 processor with NX bit works); and

determining the first executability state (done when processor executes code on that page, see above);

when the first executability state is non-executable,

identifying a first set of one or more target addresses in the list of target addresses that correspond to the first page; identifying a second set of one or more target addresses in the list that correspond to one or more pages other than the first page (implicit to the implementation of the NX-bit in the page-table of the x86 architecture: the processor distinguishes between the page starting at the one target address corresponding to it, namely the start address of the page which then faults, and the rest of the page-start addresses in the page table, which are ignored) ;

IPR2025-00069
CrowdStrike EX1002 Page 111

~~storing one or more target addresses of the first set of target addresses in breakpoint registers of the computer system, each breakpoint register configured to store an address of a respective breakpoint in the memory;~~ (however, D1 discloses to use trap instructions written in target addresses to mark regions of interest in a sub-page level, see page 10, column 2, last paragraph)

setting the first executability state of the first page table entry as executable ("clears the NX-bit on the page", page 5, column 1, paragraph 1) ; and

setting the executability states of page table entries that correspond to the second set of target addresses as non-executable ("periodically instructs the hypervisor to perform a refresh, i.e, set all pages as non-executable" which covers the second set of pages, page 5, column 2, paragraph 2); and

when the first address corresponds to one of the target addresses ~~stored in the breakpoint registers,~~ recording forensic data associated with the request to execute the instruction located at the first address ("...to detect if the identified code is subsequently modified, the hypervisor component makes the page read-only...", page 5, column 1, paragraph 1).

1.2 The subject-matter of claim 1 therefore differs from this known D1 in that

- one or more target addresses of the first set of target addresses are stored in breakpoint registers of the computer system, each breakpoint register configured to store an address of a respective breakpoint in the memory (instead D1 uses trap instructions to trap at addresses within a page)

and is therefore new.

1.3 The problem to be solved by the present invention may therefore be regarded as finding an alternative mechanism to trap when executing at a particular memory address.

1.4 The solution proposed in claim 1 of the present application cannot be considered as involving an inventive step (Article 33(3) PCT) for the following reasons: since the use of breakpoint registers is a known alternative to using trap instructions (see D5: "Vergleich mit der Breakpoint-Instruktion"), such an alternative would be considered with the known advantages/disadvantages in mind without inventive skills. In particular, a system to use the limited number of breakpoint registers on a page that has faulted as the general region of

IPR2025-00069
CrowdStrike EX1002 Page 112

interest is disclosed in D2: "If the faulting page does contain a breakpoint, then this breakpoint is written to the single breakpoint register on the CPU.", see abstract, which discloses the additional subject-matter of claim 1. Note that in the system of D1 the page fault is due to the NX-bit violation (which on x86 processors results in a page fault). Multiple debug registers are also disclosed, see figure 10 and corresponding description at the end of column 11.

1.5 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent system and storage medium claims 15 and 16, which therefore are also considered not new.

2 Additionally, the present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 17 is not new in the sense of Article 33(2) PCT.

Document D1 discloses (the references in parentheses referring to that D1):

A computer implemented method of sampling data for identifying unauthorized activities on a computer system ("In this paper, we introduce Patagonix, a hypervisor-based system that detects and identifies covertly executing binaries...", page 1, column 1, paragraph 2), the computer system having one or more processors; and memory segmented into multiple pages, said memory storing one or more programs, the method comprising (see point 1 above):

running one or more virtual machines and at least one virtual machine monitor (hypervisor); and at the at least one virtual machine monitor (see figure 1):

receiving a first virtual memory address used in one of the one or more virtual machines (see point below);

identifying a first page corresponding to the first virtual memory address and a first page table entry corresponding to the first page, the first page table entry being associated with the virtual machine monitor ("the hypervisor component initially sets the NX-bit on all pages in the monitored VM so that it will receive a trap from the processor when a code page is executed", page 5, column 1, first paragraph. This implies receiving the virtual memory address, because x86 pages are handled by their start address.);

setting the executability state of the first page table entry as non-executable (see above);

and in response to detecting a request to execute an instruction located at a second virtual memory address that corresponds to the first page table entry (see above), recording forensic data associated with the request to execute the instruction located at the second virtual memory address ("detect if code is subsequently modified", page 5, column 1, first paragraph).

The same objection applies mutatis-mutandis to independent claim 19 and 20.

3 Dependent claims 2-14 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of inventive step, as they refer to common practices when using VMM based machines to monitor malware. In the following the more relevant claims are discussed:

4 The additional subject-matter of claims 2 and 3 is disclosed in D1, since D1 discloses "Patagonix can provide trustworthy information about the binaries running on a system, as well as detect when a rootkit is hiding or tampering with executing code", see abstract.

5 While D1 does not disclose that the system is used in connection with other computers to be protected, it is clear that, based on a business requirement, the system for malware detection can also be installed on other production machines (subject-matter of claim 4).

6 The additional subject-matter of claim 5 and 7 is disclosed in D2 (D2 using debug_registers, DB0-DB3 in figure 1, see also column 1, lines 55 to column 2, line 29).

7 The additional subject-matter of claim 6 is either disclosed in D1 (virtual machine and VMM setup) or not inventive, since VM based honeypot farms are well known applications of VMM protected VMs, see also citation 3 in D1, which is D3).

8 Concerning claims 8 and 9: Shadow page tables are part of the XEN memory management (see D6) and Extended Page Tables are part of the underlying X86 virtualization technology, so implicitly disclosed in D1.

9 The particular algorithm to cope with a limited set of debug registers for more breakpoints (subject-matter of claims 10 - 13) by defining per-page breakpoints is the subject of D2.

IPR2025-00069
CrowdStrike EX1002 Page 114

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information	For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.
Amending claims under Art. 19 PCT	Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.
Filing a demand for international preliminary examination	In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT). If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).
Filing informal comments	After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.
End of the international phase	At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).
Relevant PCT Rules and more information	Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

Bitte beachten Sie, dass angeführte Nichtpatentliteratur (wie z. B. wissenschaftliche oder technische Dokumente) je nach geltendem Recht dem Urheberrechtsschutz und/oder anderen Schutzarten für schriftliche Werke unterliegen könnte. Die Vervielfältigung urheberrechtlich geschützter Texte, ihre Verwendung in anderen elektronischen oder gedruckten Publikationen und ihre Weitergabe an Dritte ist ohne ausdrückliche Zustimmung des Rechtsinhabers nicht gestattet.

Veuillez noter que les ouvrages de la littérature non-brevets qui sont cités, par exemple les documents scientifiques ou techniques, etc., peuvent être protégés par des droits d'auteur et/ou toute autre protection des écrits prévue par les législations applicables. Les textes ainsi protégés ne peuvent être reproduits ni utilisés dans d'autres publications électroniques ou imprimées, ni rediffusés sans l'autorisation expresse du titulaire du droit d'auteur.

Please be aware that cited works of non-patent literature such as scientific or technical documents or the like may be subject to copyright protection and/or any other protection of written works as appropriate based on applicable laws. Copyrighted texts may not be copied or used in other electronic or printed publications or re-distributed without the express permission of the copyright holder.

XS CPRTENFRDE

WORKING 067292-5005-WO-
DMB/TWK-

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT AND THE WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

To:
Bregman, Dion M.
MORGAN LEWIS & BOCKIUS LLP
3000 El Camino Real, Suite 700
2 Palo Alto Square
Palo Alto, CA 94306
ETATS-UNIS D'AMERIQUE

DOCKETED

File Art.19 Amendment Final: 21NOV2011
File Art.34 Amendment Final: 24APR2012
US File IDS/PCT Search Report Due: 21DEC2011

Applicant's or agent's file reference 067292-5005WO ✓	Date of mailing *(day/month/year)* 21 September 2011 (21-09-2011) **FOR FURTHER ACTION** See paragraphs 1 and 4 below
International application No. PCT/US2011/041122 ✓ PREVIOUSLY DOCKETED	International filing date *(day/month/year)* 20 June 2011 (20-06-2011) ✓
Applicant NEURALIQ, INC. ✓ File PCT Demand (19 mos) Final: 24JAN2012	

1. [X] The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

   Filing of amendments and statement under Article 19:
   The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

   When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

   Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes 1211 Geneva 20, Switzerland, Fascimile No.: (41-22) 338.82.70

   For more detailed instructions, see *PCT Applicant's Guide*, International Phase, paragraphs 9.004 - 9.011.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. [ ] **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

   [ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

   [ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

   The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.

   Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau before completion of the technical preparations for international publication (Rules 90*bis*.1 and 90*bis*.3).

   Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

   In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

   For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	ZEISELMAIR, Sabine Tel: +49 (0)89 2399-2151

RECEIVED DOCKETING
SEP 27 2011

Form PCT/ISA/220 (July 2010)

MORGAN LEWIS
PALO ALTO OFFICE

IPR2025-00069
CrowdStrike EX1002 Page 117

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference	FOR FURTHER ACTION	see Form PCT/ISA/220 as well as, where applicable, item 5 below.
067292-5005WO ✓		
International application No.	International filing date *(day/month/year)*	(Earliest) Priority Date *(day/month/year)*
PCT/US2011/041122 ✓	20/06/2011 ✓	24/06/2010 ✓
Applicant		
NEURALIQ, INC. ✓		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the **language**, the international search was carried out on the basis of:
      [X] the international application in the language in which it was filed
      [ ] a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))
   b. [ ] This international search report has been established taking into account the **rectification** of an obvious mistake authorized by or notified to this Authority under Rule 91 (Rule 43.6*bis*(a)).
   c. [ ] With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. [ ] **Certain claims were found unsearchable** (See Box No. II)

3. [ ] **Unity of invention is lacking** (see Box No III)

4. With regard to the **title**,
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,
   [X] the text is approved as submitted by the applicant
   [ ] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,
   a. the figure of the **drawings** to be published with the abstract is Figure No. 1
      [X] as suggested by the applicant
      [ ] as selected by this Authority, because the applicant failed to suggest a figure
      [ ] as selected by this Authority, because this figure better characterizes the invention
   b. [ ] none of the figures is to be published with the abstract

IPR2025-00069
CrowdStrike EX1002 Page 118

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/041122

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KURNIADI ASRIGO ET AL: "Using VMM-Based Sensors to Monitor Honeypots", 20060614; 20060614 - 20060616, 14 June 2006 (2006-06-14), pages 13-23, XP007902017, ISBN: 978-1-59593-332-4 abstract page 1, column 1, paragraph 5 page 4, column 1, paragraph 4 table 2 page 9, column 1, paragraph 2 ----- -/--	1-20

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 September 2011	21/09/2011

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Koblitz, Birger

Form PCT/ISA/210 (second sheet) (April 2005)

IPR2025-00069
CrowdStrike EX1002 Page 119

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/041122

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	Ashlesha Joshi ET AL: "Detecting Past and Present Intrusions through VulnerabilitySpecific Predicates", , 26 October 2005 (2005-10-26), pages 1-14, XP55006679, Brighton, United Kingdom Retrieved from the Internet: URL:http://www.cs.princeton.edu/courses/archive/spring06/cos592/bib/intrusions_sosp-joshi05.pdf [retrieved on 2011-09-09] Sections 4.2, 7.1.figure 2; table 1	1-20
A	NIELS PROVOS: "A Virtual Honeypot Framework", INTERNET CITATION, 21 October 2003 (2003-10-21), XP002285472, Retrieved from the Internet: URL:www.citi.umich.edu/techreports/reports/citi-tr-03-01.pdf [retrieved on 2004-06-21] the whole document	1-20
A	WO 2006/113781 A1 (UNIV COLUMBIA [US]; SIDIROGLOU STYLIANOS [US]; KEROMYTIS ANGELOS D [US]) 26 October 2006 (2006-10-26) the whole document	1-20

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

IPR2025-00069
CrowdStrike EX1002 Page 120

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2011/041122

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2006113781 A1	26-10-2006	AU 2006236283 A1	26-10-2006
		BR PI0610855 A2	03-08-2010
		CA 2604544 A1	26-10-2006
		CN 101185063 A	21-05-2008
		EP 1872222 A1	02-01-2008
		JP 2008537267 A	11-09-2008
		US 2008141374 A1	12-06-2008

IPR2025-00069
CrowdStrike EX1002 Page 121

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

To:

see form PCT/ISA/220

PCT

WRITTEN OPINION OF THE INTERNATIONAL SEARCHING AUTHORITY

(PCT Rule 43*bis*.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US2011/041122	20.06.2011	24.06.2010

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00

Applicant
NEURALIQ, INC.

1. This opinion contains indications relating to the following items:

- ☒ Box No. I Basis of the opinion
- ☐ Box No. II Priority
- ☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- ☐ Box No. IV Lack of unity of invention
- ☒ Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- ☐ Box No. VI Certain documents cited
- ☐ Box No. VII Certain defects in the international application
- ☒ Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notifed the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:	Date of completion of this opinion	Authorized Officer
European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Fax: +49 89 2399 - 4465	see form PCT/ISA/210	Koblitz, Birger Telephone No. +49 89 2399-5890

Form PCT/ISA/237 (Cover Sheet) (July 2009)

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:

   ☒ the international application in the language in which it was filed

   ☐ a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).

2. ☐ This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:

   a. (means)

   ☐ on paper

   ☐ in electronic form

   b. (time)

   ☐ in the international application as filed

   ☐ together with the international application in electronic form

   ☐ subsequently to this Authority for the purposes of search

4. ☐ In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.

5. Additional comments:

Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	
	No:	Claims	1-20
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-20
Industrial applicability (IA)	Yes:	Claims	1-20
	No:	Claims	

2. Citations and explanations

see separate sheet

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

IPR2025-00069
CrowdStrike EX1002 Page 124

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

Reference is made to the following documents:

D1 KURNIADI ASRIGO ET AL: "Using VMM-Based Sensors to Monitor Honeypots",
20060614; 20060614 - 20060616, 14 June 2006 (2006-06-14), pages 13-23, XP007902017,
ISBN: 978-1-59593-332-4

D2 Ashlesha Joshi ET AL: "Detecting Past and Present Intrusions through VulnerabilitySpecific Predicates",
, 26 October 2005 (2005-10-26), pages 1-14, XP55006679,
Brighton, United Kingdom
Retrieved from the Internet:
URL:http://www.cs.princeton.edu/courses/archive/spring06/cos592/bib/intrusions_sosp-joshi05.pdf
[retrieved on 2011-09-09]

D3 NIELS PROVOS: "A Virtual Honeypot Framework",
INTERNET CITATION, 21 October 2003 (2003-10-21), XP002285472,
Retrieved from the Internet:
URL:www.citi.umich.edu/techreports/reports/citi-tr-03-01.pdf
[retrieved on 2004-06-21]

D4 WO 2006/113781 A1 (UNIV COLUMBIA [US]; SIDIROGLOU STYLIANOS [US]; KEROMYTIS ANGELOS D [US) 26 October 2006 (2006-10-26)

1 The present application does not meet the criteria of Article 33(2) PCT, because the subject-matter of claim 1 is not new.

Document D1 discloses (the references in parentheses referring to that D1):

A computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network ("VMM-based intrusion detection and monitoring system for collecting information about attacks on honeypots, abstract"), wherein the decoy system (system running VMM, first page, right column, second paragraph) comprises:

one or more processors (implicit: VMMs such as Xen, see abstract, run on

a computer); and

memory storing (memory of computer running VMM):

a virtual machine (virtual machine instances, page 1, left column, last paragraph); and

a virtual machine monitor supervising the virtual machine ("While honeypots have traditionally employed VMMs for their ability to create and destroy virtual machine instances, as well as roll machines back to a clean state, we believe that VMMs are also ideal monitoring mechanisms.", page 1, left column, last paragraph), the method comprising, at the virtual machine monitor:

monitoring activity on the virtual machine (what a Virtual Machine Monitor does, see above);

identifying a plurality of activities being performed at the virtual machine ("In a three month period, we were able to detect five different attacks, as well as collect and try 46 more exploits on our honeypots", abstract), wherein each of the activities includes an activity source ("The invocation point of this sensor is in the sys bind handler, which is called whenever a process binds a socket to a local address.", page 4, left column, paragraph 4, the source being the process), an activity target ("The sensor's event handler determines the network port that is being bound.", the target being the port, page 4, left column, paragraph 4), and an association between the activity source and the activity target (logging of application identity and port number, page 4, left column, paragraph 4);

storing in the memory the activity sources, activity targets, and associations (logging, see above);

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine (the logfile created by the particular sensor is a fingerprint of similar or same attacks); and

transmitting the fingerprint (implicit, as the log-file is being analysed by the authors) to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (purpose of a honeypot).

2 The same reasoning applies, mutatis mutandis, to the subject-matter of the corresponding independent system and storage medium claims 19 and 20, which therefore are also considered not new.

3 Dependent claim 2-17 do not contain any features which, in combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty. In particular:

3.1 The additional subject-matter of claim 2 is disclosed in D1, because it is the definition of a honeypot machine to not be used for productive purposes and instead be monitored for activity, which can only be unauthorized.

3.2 The additional subject-matter of claim 3 is disclosed by D1, which monitors also files affected by the unauthorized activity and raises an alarm if a certain fingerprint of the activity is detected, see section 3.2 of the application.

3.3 The additional subject-matter of claim 4 is disclosed by D1, see point 1 above.

3.4 The additional subject-matter of claim 5 is disclosed by D1 as section 3.2 mentions detecting reading/writing of a file.

3.5 The additional subject-matter of claim 6 and 7 is disclosed by D1, see point 1 above.

3.6 The additional subject-matter of claims 8 to 10 is disclosed by D1, which graphically displays at least a subset of the stored activities in table 2 and visually distinguishes the activities (by using different Latin characters to describe them in that table). Also, the text "modifies xinetd to spawn shell", modifying being the first activity, spawning the second, xinetd the first target and that leading to the second activity discloses the subject-matter of claim 10.

3.7 The additional subject-matter of claim 11 and 12 is disclosed by D1, see point 3.6 above.

3.8 The additional subject-matter of claim 13 is discloses by D1, see point 1 above.

3.9 The additional subject-matter of claims 14, 15 and 16 is disclosed by D1, as D1 discloses detection of shellcode in a vulnerable buffer, buffers being not intended for execution, see page 9, left column, paragraph 2 (subject-matter of claim 14), leading network connections to execute shells (see msqlx exploit in table 1) and detected by identifying the data stream incoming (with the stream redirection sensor according to table 2).

3.10 Claim 17 is not clear, see Item VIII below.

3.11 The additional subject-matter of claim 18 is disclosed by D1, which discloses the number of attacks within a three months period, see abstract.

Re Item VIII

Certain observations on the international application

4 The application does not meet the requirements of Article 6 PCT, because claim 17 is not clear, the term "the stored events" lacking an antecedent in claim 1 to which claim 17 refers.

IPR2025-00069
CrowdStrike EX1002 Page 128

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information	For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.
Amending claims under Art. 19 PCT	Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.
Filing a demand for international preliminary examination	In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT). If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).
Filing informal comments	After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.
End of the international phase	At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).
Relevant PCT Rules and more information	Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

Bitte beachten Sie, dass angeführte Nichtpatentliteratur (wie z. B. wissenschaftliche oder technische Dokumente) je nach geltendem Recht dem Urheberrechtsschutz und/oder anderen Schutzarten für schriftliche Werke unterliegen könnte. Die Vervielfältigung urheberrechtlich geschützter Texte, ihre Verwendung in anderen elektronischen oder gedruckten Publikationen und ihre Weitergabe an Dritte ist ohne ausdrückliche Zustimmung des Rechtsinhabers nicht gestattet.

Veuillez noter que les ouvrages de la littérature non-brevets qui sont cités, par exemple les documents scientifiques ou techniques, etc., peuvent être protégés par des droits d'auteur et/ou toute autre protection des écrits prévue par les législations applicables. Les textes ainsi protégés ne peuvent être reproduits ni utilisés dans d'autres publications électroniques ou imprimées, ni rediffusés sans l'autorisation expresse du titulaire du droit d'auteur.

Please be aware that cited works of non-patent literature such as scientific or technical documents or the like may be subject to copyright protection and/or any other protection of written works as appropriate based on applicable laws. Copyrighted texts may not be copied or used in other electronic or printed publications or re-distributed without the express permission of the copyright holder.

XS CPRTENFRDE

Electronic Acknowledgement Receipt

EFS ID:	11329826
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Angela Hobson
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	03-NOV-2011
Filing Date:	17-JUN-2011
Time Stamp:	15:09:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292_5005US_IDS.pdf	252953 7c780823824786126ac50877542854c5d9da6298	yes	5

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
2	Foreign Reference	WO2006113781.pdf	1358386 a559847ffc087a1d6c367ebd05507ef60e678b5c	no	31
Warnings:					
Information:					
3	Non Patent Literature	Asrigo.pdf	1201589 63bb8355f62bf2ebe59a24ca6a26916d9b92331d	no	11
Warnings:					
Information:					
4	Non Patent Literature	DeBug.pdf	182180 e91e7a708cef9c1065949851dd982d6124178308	no	5
Warnings:					
Information:					
5	Non Patent Literature	Joshi.pdf	1534873 d3ff00d840ec6909c7cf1b924fc61887130aeeb4	no	14
Warnings:					
Information:					
6	Non Patent Literature	Krapf.pdf	238206 eabe3139207d38dd029cf3106c9d8dae257afe88	no	6
Warnings:					
Information:					
7	Non Patent Literature	Litty.pdf	1664257 4e3e1fef0dec6a9ac6f1f7f43e51f55130c4310c	no	16
Warnings:					
Information:					
8	Non Patent Literature	Provos.pdf	865537 2c7909dbebe503ce324ed9d2a5609ae570dbd273	no	11
Warnings:					
Information:					

9	Non Patent Literature	ISR_WO_5004.pdf	679393 41ca189400a20709a03b90de83b980d1aab0e00a	no	14
Warnings:					
Information:					
10	Non Patent Literature	ISR_WO_5005.pdf	594500 a661c9aa6268ad80e1137e97d82d23e16fe696dd	no	14
Warnings:					
Information:					
			Total Files Size (in bytes):	8571874	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed November 3, 2011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	CAPALIK et al.	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2431
Filed:	June 17, 2011	Examiner:	Not yet assigned
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☒ Each foreign patent;

☒ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☐ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☒ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☒ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a or 3b)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is:
☐ enclosed
☐ to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Item 3b to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a and 4b)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4.b ☐ The $180.00 fee set forth in 37 C.F.R. §1.17(p) is:
☐ enclosed.
☐ to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application,

and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

IPR2025-00069
CrowdStrike EX1002 Page 136

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: November 3, 2011

45,645
Dion M. Bregman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/163,590	06/17/2011	Alen Capalik	067292-5005-US

CONFIRMATION NO. 1008

24341
MORGAN, LEWIS & BOCKIUS, LLP. (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

PUBLICATION NOTICE



Title: System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

Publication No.US-2011-0321166-A1
Publication Date:12/29/2011

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

IPR2025-00069
CrowdStrike EX1002 Page 138

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	November 13, 2012
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	CAPALIK, Alen
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number - Kind Code[1]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	5,339,426	08-16-1994	Aoshima	
	A2	6,360,327 B1	03-19-2002	Hobson	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document Country Code[2] - Number[3] - Kind Code[4] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T Yes

OTHER NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	C1	Capalik, Notice of Allowance, U.S. Patent Application No. 11/488,743, 24 October 2012, 15 pgs
	C2	LIANG, Fast and Automated Generation of Attack Signatures: A Basis for Building Self-Protecting Servers, 7-11 November 2005
	C3	NeuralIQ, Office Action, Australian Patent Application No. 2008242296, 05 April 2012, 2 pgs

Examiner Signature		Date Considered	

DB2/ 23656556.1

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Electronic Acknowledgement Receipt

EFS ID:	14218816
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Meredith Ramirez
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	13-NOV-2012
Filing Date:	17-JUN-2011
Time Stamp:	17:45:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292_5005_US_IDS_11_13_2012.pdf	527916 af81d7858748c5c10409091e1652e281f2f078f8	yes	5

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
2	Non Patent Literature	Capalik_NOA_10_24_2012.pdf	661910 d4ca86bc3931e37123cadb7bb6eb3e027ea81ad7	no	15
Warnings:					
Information:					
3	Non Patent Literature	Liang.pdf	201807 2d3c05b3b57c3da1b646656a276a682bb44d3f8d	no	10
Warnings:					
Information:					
4	Non Patent Literature	Neuraliq_AU_OA_04_05_2012.pdf	55718 63b5b2a78ed087c672d6f7326b3be9a36103a9ea	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1447351		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

<u>New Applications Under 35 U.S.C. 111</u>
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

<u>National Stage of an International Application under 35 U.S.C. 371</u>
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

<u>New International Application Filed with the USPTO as a Receiving Office</u>
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed November 13, 2012

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al.	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☐ Each foreign patent;

☒ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language

IPR2025-00069
CrowdStrike EX1002 Page 142

abstracts of the non-English language publications.

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☒ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a or 3b)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is:
☐ enclosed
☐ to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Item 3b to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a and 4b)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4.b ☐ The $180.00 fee set forth in 37 C.F.R. §1.17(p) is:
☐ enclosed.
☐ to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

IPR2025-00069
CrowdStrike EX1002 Page 143

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

IPR2025-00069
CrowdStrike EX1002 Page 144

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: November 13, 2012

Dion M. Bregman (Reg. No. 45,645)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	**February 4, 2013**
				Application Number	**13/163,590**
				Filing Date	**June 17, 2011**
				First Named Inventor	**CAPALIK, Alen**
				Art Unit	**2453**
				Examiner Name	**Nguyen, Thu Ha T.**
Sheet	1	of	1	Attorney Docket Number	**067292-5005-US**

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number - Kind Code[1]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document Country Code[2] - Number[3] - Kind Code[4] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T Yes

OTHER NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		NeuralIQ, Office Action, CA 2,689,126, 15AUG2012, 3 pgs

Examiner Signature		Date Considered	

DB2/ 23862789.1

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Electronic Acknowledgement Receipt

EFS ID:	14870340
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Douglas James Crisman/Ramona J Zaya
Filer Authorized By:	Douglas James Crisman
Attorney Docket Number:	067292-5005-US
Receipt Date:	04-FEB-2013
Filing Date:	17-JUN-2011
Time Stamp:	17:15:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292-5005-US-IDS.pdf	225324 b4db43b8427e52dc242ad70e9aa0d89a3f4c8b33	yes	5

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	4
	Information Disclosure Statement (IDS) Form (SB08)	5	5

Warnings:					
Information:					
2	Non Patent Literature	NeuralIQ-OA-CA2689126-15AUG2012.pdf	170066 0fa76426301c40ba4be74f1ad531b63a00709631	no	3
Warnings:					
Information:					
		Total Files Size (in bytes):	395390		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed February 4, 2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik et al.	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language

IPR2025-00069
CrowdStrike EX1002 Page 149

abstracts of the non-English language publications.

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☒ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a or 3b)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is:
☐ enclosed
☐ to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Item 3b to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a and 4b)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4.b ☐ The $180.00 fee set forth in 37 C.F.R. §1.17(p) is:
☐ enclosed.
☐ to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this Information Disclosure Statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this Information Disclosure Statement.

IPR2025-00069
CrowdStrike EX1002 Page 150

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☐ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

IPR2025-00069
CrowdStrike EX1002 Page 151

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: February 1, 2013

Dion M. Bregman 45,645 (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed June 26, 2013	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T
Sheet	1	of	1	Attorney Docket Number	067292-5005US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2004/0025052 A1	02-05-2004	Dickenson	
		2005/0229250 A1	10-13-2005	Ring et al.	
		2007/0101431 A1	05-03-2007	Clift et al.	
		2007/0180529 A1	08-02-2007	Costea et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document Country Code[3] – Number[4] - Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		JP 2005-316779	11-10-2005	Intelligent Cosmos Research Institute		
		WO 2007/027739	03-08-2007	Microsoft Corp.		

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Office Action, US 13/759,335, 14 June 2013, 32 pgs
		NeuralIQ Inc., Notice of Reasons for Rejection, JP 2010-504185, 15 March 2013, 4 pgs

Examiner Signature		Date Considered	

DB2/24194294.1

No documents available for this priority number.

Espacenet

Bibliographic data: JP2005316779 (A) — 2005-11-10

UNAUTHORIZED ACCESS DETECTOR, DETECTION RULE GENERATION DEVICE, DETECTION RULE GENERATION METHOD, AND DETECTION RULE GENERATION PROGRAM

Inventor(s): IZUMI YUJI; KATO HIROYUKI; KATO YASUSHI; NEMOTO YOSHIAKI ± (IZUMI YUJI, ; KATO HIROYUKI, ; KATO YASUSHI, ; NEMOTO YOSHIAKI)

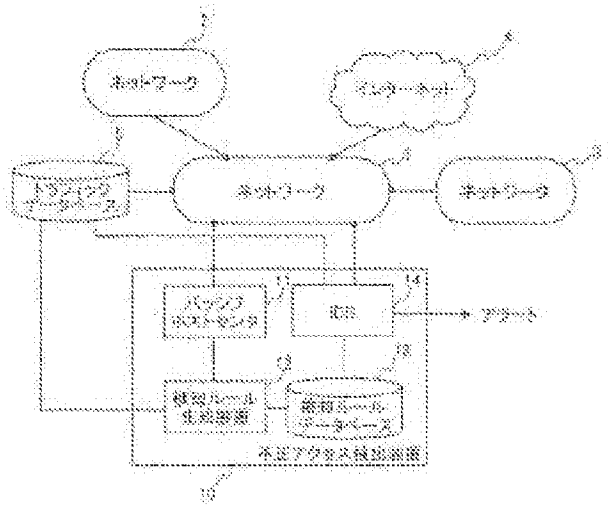
Applicant(s): INTELLIGENT COSMOS RES INST ± (INTELLIGENT COSMOS RESEARCH INSTITUTE)

Classification: **- international:** ***G06F15/00; G06F21/20;*** (IPC1-7): G06F15/00
- cooperative:

Application number: JP20040134668 20040428

Priority number (s): JP20040134668 20040428

Abstract of JP2005316779 (A)



PROBLEM TO BE SOLVED: To deal with new/unknown unauthorized access, for which a detection rule is not defined yet, and to quickly and automatically generate a detection rule for dealing with the new/unknown unauthorized access. ; SOLUTION: This unauthorized access detector detecting unauthorized access to a network is provided with a passive host sensor 11 detecting communication to itself without notifying own presence, a detection rule generation device 12 generating the detection rule characterizing the unauthorized access and outputting it, and a signature matching type IDS 14 determining an illegality degree of an observed access. The detection rule generation device 12 is provided with an automatic generation means automatically generating the detection rule based on an access log notified from the passive host sensor 11. ; COPYRIGHT: (C)2006,JPO&NCIPI

Last updated: 13.03.2013 Worldwide Database 5.8.6.6; 92p

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2005-316779
(P2005-316779A)
(43)公開日　平成17年11月10日(2005.11.10)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 15/00	G06F 15/00	330A	5B085

審査請求 未請求　請求項の数 27　ＯＬ　（全 22 頁）

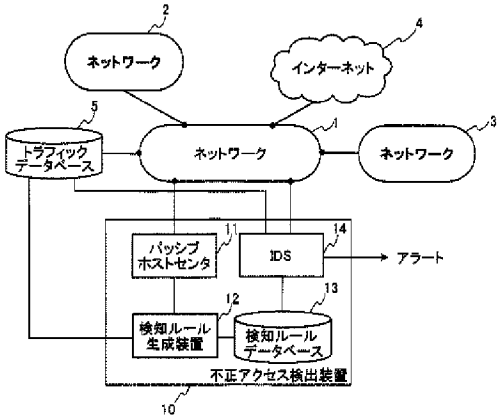
(21)出願番号　特願2004-134668 (P2004-134668)
(22)出願日　平成16年4月28日 (2004.4.28)

(71)出願人　503066952
株式会社インテリジェント・コスモス研究機構
宮城県仙台市青葉区南吉成六丁目６番地の３
(74)代理人　100088096
弁理士　福森　久夫
(72)発明者　和泉　勇治
宮城県仙台市青葉区荒巻字青葉５　東北大学大学院内
(72)発明者　加藤　弘之
宮城県仙台市青葉区荒巻字青葉５　東北大学大学院内

最終頁に続く

(54)【発明の名称】不正アクセス検出装置ならびに検知ルール生成装置、検知ルール生成方法および検知ルール生成プログラム

(57)【要約】
【課題】検知ルールが明らかでない新種や未知の不正アクセスに対処すること。また、新種や未知の不正アクセスに対処するための検知ルールの生成を迅速かつ自動的に行うこと。
【解決手段】ネットワークに対して行われる不正アクセスを検出する不正アクセス検出装置であって、自己の存在を知らせることなく自己宛の通信を検出するパッシブホストセンサ１１と、不正アクセスを特徴づける検知ルールを生成して出力する検知ルール生成装置１２と、観測されたアクセスの不正性を判定するシグネチャマッチング型ＩＤＳ１４とが備えられ、検知ルール生成装置１２は、パッシブホストセンサ１１から通知されたアクセスログに基づいて検知ルールを自動生成する自動生成手段を備える。
【選択図】　図１



IPR2025-00069
CrowdStrike EX1002 Page 156

【特許請求の範囲】
【請求項1】
ネットワークに対して行われる不正アクセスを検出する不正アクセス検出装置であって、
自己の存在を知らせることなく自己宛の通信を検出するパッシブホストセンサと、
不正アクセスを特徴づける検知ルールを生成して出力する検知ルール生成装置と、
観測されたアクセスの不正性を判定するシグネチャマッチング型のＩＤＳと、
を備え、
前記検知ルール生成装置は、
前記パッシブホストセンサから通知されたアクセスログに基づいて前記検知ルールを自動生成する自動生成手段を備えたことを特徴とする不正アクセス検出装置。
【請求項2】
前記自動生成手段は、前記アクセスログのプロトコルまたは当該アクセスログを構成するフィールドの特性に応じて検知ルールの自動生成処理を行わせるか否かを判定する第１の剪定手段を備えたことを特徴とする請求項１に記載の不正アクセス検出装置。
【請求項3】
前記自動生成手段は、前記アクセスログに基づいて仮の検知ルールを生成する仮の検知ルール生成手段と、該仮の検知ルールに対して所定の抽出処理を施して真の検知ルールを生成する抽出手段と、を具備する第２の剪定手段を備えたことを特徴とする請求項１または２に記載の不正アクセス検出装置。
【請求項4】
前記仮の検知ルール生成手段は、
前記アクセスログのメッセージ部を段階的に分割し、分割途中の段階を含め各段階で生成された文字列の全てを仮の検知ルールとして残しておくことを特徴とする請求項３に記載の不正アクセス検出装置。
【請求項5】
前記仮の検知ルール生成手段は、分割途中の各段階で検知ルールとして生成される文字列に対し、当該文字列の両端に分割時に付加されていた区切り文字を残しておくことを特徴とする請求項３または４に記載の不正アクセス検出装置。
【請求項6】
前記所定の抽出処理では、不正アクセスを含まないトラフィックデータである通常トラフィックデータに基づいて頻出文字列リストが生成され、前記仮の検知ルールから、当該頻出文字列リストの所定の順位以上に位置する頻出文字列が除去されることを特徴とする請求項１～５のいずれか一つに記載の不正アクセス検出装置。
【請求項7】
前記アクセスログのプロトコルがアプリケーション層の通信プロトコルであることを特徴とする請求項１～６のいずれか一つに記載の不正アクセス検出装置。
【請求項8】
前記第１の剪定手段は、
前記アプリケーション層の通信プロトコルで通信されたリクエストに含まれるメッセージヘッダを構成するフィールド名のセッションごとの出現頻度と、該フィールドの種類ごとに算出された所定の第１のしきい値と、に基づいて前記検知ルールの自動生成処理を行わせるか否かを判定することを特徴とする請求項７に記載の不正アクセス検出装置。
【請求項9】
前記第１の剪定手段は、
前記アプリケーション層の通信プロトコルで通信されたリクエストに含まれるメッセージヘッダのフィールド値を構成する文字列の任意の文字種間の遷移確率の平均値と、所定の第２のしきい値とに基づいて前記検知ルールの自動生成処理を行わせるか否かを判定することを特徴とする請求項７に記載の不正アクセス検出装置。

IPR2025-00069
CrowdStrike EX1002 Page 157

【請求項10】
観測された不正アクセスから生成される複数の検知ルールに対し、当該検知ルールの性能を表す重要度で重み付け処理した合計値である得点が所定値以上の場合にアラートを発生させることを特徴とする請求項１～９のいずれか一つに記載の不正アクセス検出装置。
【請求項11】
前記重要度は、過去のトラヒックデータに対する反応数に基づいて算出されることを特徴とする請求項１０に記載の不正アクセス検出装置。
【請求項12】
所定の許容Ｆ.Ｐ.数および検知ルールに反応したセッションごとの得点の傾向に基づいて判定しきい値が設定され、当該判定しきい値以上の得点を有する１以上のセッションが存在する場合に、アラートを発生させることを特徴とする請求項１～１１のいずれか一つに記載の不正アクセス検出装置。
【請求項13】
観測された不正アクセスが新種の不正アクセスの場合に、当該観測された不正アクセスに基づいて検知ルールを生成し、生成された検知ルールを所定のデータベースに追加する追加モードと、
登録済の検知ルールに基づいて観測されたアクセスが不正か否かを判定する判定モードと、
を有することを特徴とする請求項１～１２のいずれか一つに記載の不正アクセス検出装置。
【請求項14】
前記検知ルールを新規に構築するための生成モードを有することを特徴とする請求項１～１３のいずれか一つに記載の不正アクセス検出装置。
【請求項15】
検知ルールの追加および判定処理を同時に行う追加・判定モードを有することを特徴とする請求項１３または１４に記載の不正アクセス検出装置。
【請求項16】
ネットワークに対して行われる不正アクセスを検出するための検知ルールを生成する検知ルール生成装置であって、
入力されたアクセスログに基づいて不正アクセスを特徴づける検知ルールを自動生成する自動生成手段を備えたことを特徴とする検知ルール生成装置。
【請求項17】
前記自動生成手段は、前記アクセスログのプロトコルまたは当該アクセスログを構成するフィールドの特性に応じて検知ルールの自動生成処理を行わせるか否かを判定する第１の剪定手段を備えたことを特徴とする請求項１６に記載の検知ルール生成装置。
【請求項18】
前記自動生成手段は、前記アクセスログに基づいて仮の検知ルールを生成する仮の検知ルール生成手段と、該仮の検知ルールに対して所定の抽出処理を施して真の検知ルールを生成する抽出手段と、を具備する第２の剪定手段を備えたことを特徴とする請求項１６または１７に記載の検知ルール生成装置。
【請求項19】
前記仮の検知ルール生成手段は、
前記アクセスログのメッセージ部を段階的に分割し、分割途中の段階を含め各段階で生成された文字列の全てを仮の検知ルールとして残しておくことを特徴とする請求項１８に記載の検知ルール生成装置。
【請求項20】
前記仮の検知ルール生成手段は、分割途中の各段階で検知ルールとして生成される文字列に対し、当該文字列の両端に分割時に付加されていた区切り文字を残しておくことを特徴とする請求項１８または１９に記載の検知ルール生成装置。
【請求項21】

IPR2025-00069
CrowdStrike EX1002 Page 158

前記検知ルールを新規に構築するための生成モードを有することを特徴とする請求項１６～２０のいずれか一つに記載の検知ルール生成装置。
【請求項22】
仮の検知ルールデータから前記検知ルールが一括生成されることを特徴とする請求項２１に記載の検知ルール生成装置。
【請求項23】
ネットワークに対して行われる不正アクセスを検出するための検知ルールを生成する検知ルール生成方法であって、
入力されたアクセスログに基づいて不正アクセスを特徴づける検知ルールを自動生成する自動生成ステップと、
前記アクセスログのプロトコルまたは当該アクセスログを構成するフィールドの特性に応じて検知ルールの自動生成処理を行わせるか否かを判定する第１の剪定ステップと、
を含むことを特徴とする検知ルール生成方法。
【請求項24】
前記自動生成ステップは、前記アクセスログに基づいて仮の検知ルールを生成する仮の検知ルール生成ステップと、該仮の検知ルールに対して所定の抽出処理を施して真の検知ルールを生成する抽出ステップと、を具備する第２の剪定ステップを備えたことを特徴とする請求項２３に記載の検知ルール生成方法。
【請求項25】
前記仮の検知ルール生成ステップは、
前記アクセスログのメッセージ部を段階的に分割し、分割途中の段階を含め各段階で生成された文字列の全てを仮の検知ルールとして残しておくことを特徴とする請求項２４に記載の検知ルール生成方法。
【請求項26】
前記仮の検知ルール生成ステップは、分割途中の各段階で検知ルールとして生成される文字列に対し、当該文字列の両端に分割時に付加されていた区切り文字を残しておくことを特徴とする請求項２４または２５に記載の検知ルール生成方法。
【請求項27】
請求項２３～２６のいずれか一つに記載の方法を電子計算機に実行させることを特徴とする検知ルール生成プログラム。
【発明の詳細な説明】
【技術分野】
【0001】
この発明は、ネットワークに対して行われる不正アクセスの検出に関するものであり、特に、新種や未知の不正アクセスに対処可能な不正アクセス検出装置ならびに、これらの新種や未知の不正アクセスに迅速に対処するための検知ルールを自動生成可能な検知ルール生成装置、検知ルール生成方法および検知ルール生成プログラムに関するものである。
【背景技術】
【0002】
近年、インターネットが社会的に重要なメディアとなり、その上で様々なサービスが提供されている。例えば、従来から利用されているメール、ｗｅｂによるブラウジングや掲示板などに加え、オンラインショッピングや銀行決済、企業間の取引などにもインターネットが利用されるようになってきている。
【0003】
一方、これらへの利用に伴い、悪意のあるユーザによる不正アクセスによって、サービスの停止や、情報の改ざん、情報の漏洩などが起こった場合の社会的活動に与える影響が以前に比べて重大かつ深刻なものになってきている。そのため、不正アクセスをいち早く検出し対策をとることが求められている。
【0004】
上述のような不正アクセスを早期に検出するための検出手段の一つとして、侵入検知システム（ＩＤＳ：Ｉｎｔｒｕｓｉｏｎ　Ｄｅｔｅｃｔｉｏｎ　Ｓｙｓｔｅｍ）があり、そ

IPR2025-00069
CrowdStrike EX1002 Page 159

の中でも、“Ｓｎｏｒｔ”と呼ばれるシグネチャマッチング型のＩＤＳが実用化され、各所で使用されている。

【0005】

ところで、シグネチャマッチング型のＩＤＳは、既知の不正アクセスの通信内容に含まれる特徴的な文字列を予めデータベースとして保有するとともに、その文字列に一致するものが監視対象のネットワークで発見され場合に、管理者に対してアラートを通知するように動作する。したがって、この方式は、動作の高速性があり、誤検出が少ないといった利点を有している反面、対応する検知ルールが明らかでない新種や未知の不正アクセスについては、全く検知することはできないという問題点が存在しており、新種や未知の不正アクセスが発見されたときにいかにして、迅速に検知ルールを作成するかが重要な課題として残っている。

【0006】

このような状況下において、不正アクセスから自己のシステムを防御するための従来技術として、コンピュータネットワークのセキュリティサポート契約者に対し、不正侵入を検知した契約者のネットワーク機器からの情報により、不正侵入者をおとりサーバに誘導する手段を提供した管理システムが開示されている（例えば、特許文献１）。この特許文献１では、この管理システムを利用することの利点として、おとりサーバの設置やログ解析、応答パケットの作成といった対処を専門のサービス業者に委託することによりネットワーク管理のコストを軽減することができるという第１の利点と、サービス提供者側が、サービス利用者のネットワーク機器の状況を遠隔地から常時把握することができ、サービス利用者のところに出向かずとも迅速な対応が可能となるという第２の利点とが挙げられている。

【0007】

【特許文献1】特開２００２－３１８７３９号公報

【発明の開示】

【発明が解決しようとする課題】

【0008】

しかしながら、上述した従来のシグネチャマッチング型のＩＤＳや、上記特許文献１に開示された管理システムにおいては、根本的な問題点が内在しているという点で両者には共通点がある。すなわち、特許文献１の発明ではログ解析や不正アクセスに対する応答パケットの作成といった対処を専門のサービス業者に委託することが前提であり、従来のシグネチャマッチング型のＩＤＳに固有な「新種や未知の不正アクセスが発見されたときに迅速な対処ができない」という課題は依然として解決されていない。

【0009】

この発明は、上述した従来の欠点に鑑みてなされたものであり、検知ルールが明らかでない新種や未知の不正アクセスに対処することができる不正アクセス検出装置を提供することを目的とする。また、これらの新種や未知の不正アクセスに対処するための検知ルールの生成を迅速かつ自動的に行うことができる検知ルール生成装置、検知ルール生成方法および検知ルール生成プログラムを提供することを目的とする。

【課題を解決するための手段】

【0010】

上記目的を達成するため、請求項１にかかる不正アクセス検出装置は、ネットワークに対して行われる不正アクセスを検出する不正アクセス検出装置であって、自己の存在を知らせることなく自己宛の通信を検出するパッシブホストセンサと、不正アクセスを特徴づける検知ルールを生成して出力する検知ルール生成装置と、観測されたアクセスの不正性を判定するシグネチャマッチング型ＩＤＳと、を備え、前記検知ルール生成装置は、前記パッシブホストセンサから通知されたアクセスログに基づいて前記検知ルールを自動生成する自動生成手段を備えたことを特徴とする。

【0011】

また、請求項２にかかる不正アクセス検出装置は、上記の発明において、前記自動生成

IPR2025-00069
CrowdStrike EX1002 Page 160

手段は、前記アクセスログのプロトコルまたは当該アクセスログを構成するフィールドの特性に応じて検知ルールの自動生成処理を行わせるか否かを判定する第１の剪定手段を備えたことを特徴とする。

【0012】

また、請求項３にかかる不正アクセス検出装置は、上記の発明において、前記自動生成手段は、前記アクセスログに基づいて仮の検知ルールを生成する仮の検知ルール生成手段と、該仮の検知ルールに対して所定の抽出処理を施して真の検知ルールを生成する抽出手段と、を具備する第２の剪定手段を備えたことを特徴とする。

【0013】

また、請求項４にかかる不正アクセス検出装置は、上記の発明において、前記仮の検知ルール生成手段は、前記アクセスログのメッセージ部を段階的に分割し、分割途中の段階を含め各段階で生成された文字列の全てを仮の検知ルールとして残しておくことを特徴とする。

【0014】

また、請求項５にかかる不正アクセス検出装置は、上記の発明において、前記仮の検知ルール生成手段は、分割途中の各段階で検知ルールとして生成される文字列に対し、当該文字列の両端に分割時に付加されていた区切り文字を残しておくことを特徴とする。

【0015】

また、請求項６にかかる不正アクセス検出装置は、上記の発明において、前記所定の抽出処理では、不正アクセスを含まないトラフィックデータである通常トラフィックデータに基づいて頻出文字列リストが生成され、前記仮の検知ルールから、当該頻出文字列リストの所定の順位以上に位置する頻出文字列が除去されることを特徴とする。

【0016】

また、請求項７にかかる不正アクセス検出装置は、上記の発明において、前記アクセスログのプロトコルがアプリケーション層の通信プロトコルであることを特徴とする。

【0017】

また、請求項８にかかる不正アクセス検出装置は、上記の発明において、前記第１の剪定手段は、前記アプリケーション層の通信プロトコルで通信されたリクエストに含まれるメッセージヘッダを構成するフィールド名のセッションごとの出現頻度と、該フィールドの種類ごとに算出された所定の第１のしきい値と、に基づいて前記検知ルールの自動生成処理を行わせるか否かを判定することを特徴とする。

【0018】

また、請求項９にかかる不正アクセス検出装置は、上記の発明において、前記第１の剪定手段は、前記アプリケーション層の通信プロトコルで通信されたリクエストに含まれるメッセージヘッダのフィールド値を構成する文字列の任意の文字種間の遷移確率の平均値と、所定の第２のしきい値とに基づいて前記検知ルールの自動生成処理を行わせるか否かを判定することを特徴とする。

【0019】

また、請求項１０にかかる不正アクセス検出装置は、上記の発明において、観測された不正アクセスから生成される複数の検知ルールに対し、当該検知ルールの性能を表す重要度で重み付け処理した合計値である得点が所定値以上の場合にアラートを発生させることを特徴とする。

【0020】

また、請求項１１にかかる不正アクセス検出装置は、上記の発明において、前記重要度は、過去のトラヒックデータに対する反応数に基づいて算出されることを特徴とする。

【0021】

また、請求項１２にかかる不正アクセス検出装置は、上記の発明において、設定された許容Ｆ.Ｐ.数と、検知ルールごとの前記得点の傾向とに基づいて決定される判定しきい値が設定され、当該判定しきい値よりも上位順位にある検知ルールに反応したときにアラートを発生させることを特徴とする。

IPR2025-00069
CrowdStrike EX1002 Page 161

【0022】
　また、請求項１３にかかる不正アクセス検出装置は、上記の発明において、観測された不正アクセスが新種の不正アクセスの場合に、当該観測された不正アクセスに基づいて検知ルールを生成し、生成された検知ルールを所定のデータベースに追加する追加モードと、登録済の検知ルールに基づいて観測されたアクセスが不正か否かを判定する判定モードと、を有することを特徴とする。
【0023】
　また、請求項１４にかかる不正アクセス検出装置は、上記の発明において、前記検知ルールを新規に構築するための生成モードを有することを特徴とする。
【0024】
　また、請求項１５にかかる不正アクセス検出装置は、上記の発明において、検知ルールの追加および判定処理を同時に行う追加・判定モードを有することを特徴とする。
【0025】
　また、請求項１６にかかる検知ルール生成装置は、上記の発明において、ネットワークに対して行われる不正アクセスを検出するための検知ルールを生成する検知ルール生成装置であって、入力されたアクセスログに基づいて不正アクセスを特徴づける検知ルールを自動生成する自動生成手段を備えたことを特徴とする。
【0026】
　また、請求項１７にかかる検知ルール生成装置は、上記の発明において、前記自動生成手段は、前記アクセスログのプロトコルまたは当該アクセスログを構成するフィールドの特性に応じて検知ルールの自動生成処理を行わせるか否かを判定する第１の剪定手段を備えたことを特徴とする。
【0027】
　また、請求項１８にかかる検知ルール生成装置は、上記の発明において、前記自動生成手段は、前記アクセスログに基づいて仮の検知ルールを生成する仮の検知ルール生成手段と、該仮の検知ルールに対して所定の抽出処理を施して真の検知ルールを生成する抽出手段と、を具備する第２の剪定手段を備えたことを特徴とする。
【0028】
　また、請求項１９にかかる検知ルール生成装置は、上記の発明において、前記仮の検知ルール生成手段は、前記アクセスログのメッセージ部を段階的に分割し、分割途中の段階を含め各段階で生成された文字列の全てを仮の検知ルールとして残しておくことを特徴とする。
【0029】
　また、請求項２０にかかる検知ルール生成装置は、上記の発明において、前記仮の検知ルール生成手段は、分割途中の各段階で検知ルールとして生成される文字列に対し、当該文字列の両端に分割時に付加されていた区切り文字を残しておくことを特徴とする。
【0030】
　また、請求項２１にかかる検知ルール生成装置は、上記の発明において、前記検知ルールを新規に構築するための生成モードを有することを特徴とする。
【0031】
　また、請求項２２にかかる検知ルール生成装置は、上記の発明において、仮の検知ルールデータから前記検知ルールが一括生成されることを特徴とする。
【0032】
　また、請求項２３にかかる不正アクセス検出方法は、ネットワークに対して行われる不正アクセスを検出するための検知ルールを生成する検知ルール生成方法であって、入力されたアクセスログに基づいて不正アクセスを特徴づける検知ルールを自動生成する自動生成ステップと、前記アクセスログのプロトコルまたは当該アクセスログを構成するフィールドの特性に応じて検知ルールの自動生成処理を行わせるか否かを判定する第１の剪定ステップと、を含むことを特徴とする。
【0033】

IPR2025-00069
CrowdStrike EX1002 Page 162

また、請求項２４にかかる不正アクセス検出方法は、上記の発明において前記自動生成ステップは、前記アクセスログに基づいて仮の検知ルールを生成する仮の検知ルール生成ステップと、該仮の検知ルールに対して所定の抽出処理を施して真の検知ルールを生成する抽出ステップと、を具備する第２の剪定ステップを備えたことを特徴とする。

【0034】

また、請求項２５にかかる不正アクセス検出方法は、上記の発明において前記仮の検知ルール生成ステップは、前記アクセスログのメッセージ部を段階的に分割し、分割途中の段階を含め各段階で生成された文字列の全てを仮の検知ルールとして残しておくことを特徴とする。

【0035】

また、請求項２６にかかる不正アクセス検出方法は、上記の発明において前記仮の検知ルール生成ステップは、分割途中の各段階で検知ルールとして生成される文字列に対し、当該文字列の両端に分割時に付加されていた区切り文字を残しておくことを特徴とする。

【0036】

また、請求項２７にかかる検知ルール生成プログラムは、請求項２３～２６のいずれか一つに記載の方法を電子計算機に実行させることを特徴とする。

【発明の効果】

【0037】

この発明にかかる不正アクセス検出装置によれば、パッシブホストセンサから通知されたアクセスログに基づいて検知ルールを自動生成するようにしているので、検知ルールが明らかでない新種や未知の不正アクセスに対処することができる。

【0038】

また、この発明にかかる検知ルール生成装置によれば、入力されたアクセスログに基づいて不正アクセスを特徴づける検知ルールを自動生成するようにしているので、新種や未知の不正アクセスに対処するための検知ルールの生成を迅速かつ自動的に行うことができる。

【発明を実施するための最良の形態】

【0039】

以下、図面を参照して、この発明の実施の形態である不正アクセス検出装置ならびに検知ルール生成装置および検知ルール生成方法について説明する。なお、この実施の形態によりこの発明が限定されるものではない。

【0040】

（実施の形態１）

図１は、この発明の実施の形態１にかかる不正アクセス検出装置の構成を示すブロック図である。同図に示す接続構成は、不正アクセス検出装置１０が接続されるネットワークがインターネットや他のネットワークなどの任意のネットワークに接続されている状態を示すものである。

【0041】

図１において、不正アクセス検出装置１０は、ネットワーク２，３およびインターネット４に接続されたネットワーク１に接続されている。一方、ネットワーク１には、ネットワーク１の通信ログなどを常時記録するためのトラフィックデータベース５が接続されている。不正アクセス検出装置１０は、パッシブホストセンサ１１と、検知ルール生成装置１２と、検知ルールデータベース１３と、ＩＤＳ１４とを備えている。不正アクセス検出装置１０を構成する各構成部は、パッシブホストセンサ１１と、ＩＤＳ１４とがネットワーク１にそれぞれ接続され、パッシブホストセンサ１１に接続される検知ルール生成装置１２と、ＩＤＳ１４に接続される検知ルールデータベース１３とがそれぞれ接続されている。また、検知ルール生成装置１２およびＩＤＳ１４は、トラフィックデータベース５にも接続されている。

【0042】

例えば、パッシブホストセンサ１１、検知ルール生成装置１２およびＩＤＳ１４は、ワ

IPR2025-00069
CrowdStrike EX1002 Page 163

ークステーションまたはパーソナルコンピュータなどのプラットフォームと、このプラットフォームに搭載される処理ソフトウェアなどから構成される。また、検知ルールデータベース１３は磁気ディスク等の記憶装置から構成される。なお、これらの各構成部は、図１に示すようにそれぞれが異なるハードウェアで処理させる構成としてもよいし、また、それぞれの処理能力に応じて、各構成部で行われる幾つかの処理機能を統合して同一ハードウェア上で処理させる構成としてもよい。例えば、パッシブホストセンサ１１内に検知ルール生成装置１２の機能を組み込むように構成してもよい。また、検知ルール生成装置１２内に検知ルールの記憶領域を確保し、検知ルールデータベース１３の機能を組み込むように構成してもよい。

【0043】

つぎに、図１に示す不正アクセス検出装置１０の３つの処理モードについて説明する。不正アクセス検出装置１０は、つぎに示す３つの処理モードを有する。

（１）　検知ルールデータベース１３を新規に構築するための生成モード

（２）　観測された不正アクセスが新種の不正アクセスの場合に、この観測された不正アクセスに基づいて不正アクセス検知ルール（以下、単に「検知ルール」と呼称）を生成し、生成された検知ルールを検知ルールデータベース１３に追加する追加モード

（３）　登録済の検知ルールに基づいて観測されたアクセスが不正か否かを判定する判定モード

また、上記３つの処理モードの他に検知ルールの自動生成と、生成された検知ルールの登録を迅速に行うことができるという特徴を活用し、検知ルールの追加および判定処理を同時に行う追加・判定モードも存在するが、この追加・判定モードは、システムの運用上のモードであり機能的には追加モードおよび判定モードの機能を組み合わせたものに相当するので、上記３つの処理モードに含めて考えることにする。　なお、ここでいう検知ルールという用語は、一般的なＩＤＳなどに設定されている不正パケットの特徴情報を示すシグネチャと同義であると考えて差しつかえない。

【0044】

上述の３つの処理モードにおいて、以下のような処理が行われる。生成モードでは、予め記録されているアクセスログ（例えば、トラフィックデータベース５などに記録されているログデータ）に基づいて検知ルールが生成され、生成された検知ルールが検知ルールデータベース１３に登録される。なお、検知ルールの生成に際しては、上述したＳｎｏｒｔなどに記述されているルールセットなどを活用することができる。追加モードでは、パッシブホストセンサ１１において観測されたアクセスログに基づいて生成される検知ルールが検知ルールデータベース１３に追加される。判定モードでは、ＩＤＳ１４において観測されたアクセスの不正性が判定される。

【0045】

なお、パッシブホストセンサ１１は、一種のおとりシステムであり、故意に脆弱性を設けたホストセンサをおとりとしてネットワークに設置して不正アクセスの挙動を観測するためのものである。パッシブホストセンサ１１を用いる理由は、「通常、このおとりシステムであるパッシブホストセンサ１１をクライアントとして利用するユーザはなく、また、外部に対するアナウンスも行われていないので、パッシブホストセンサ１１に対して行われる通信は全て何らかの悪意を持って行われる」、という考え方に基づいている。

【0046】

また、パッシブホストセンサ１１を侵入検知システムとして見た場合にはつぎのような利点がある。すなわち、従来は実際に被害が出るか、もしくはネットワーク上の通信ログを詳細に解析しなければ不正アクセスが行われたか否かの判断を行うことができなかったが、その判断を即座に行うことができる。さらに、不正アクセスの解析に先立ち、必要な不正アクセスログの分離作業も必要なくなる。

【0047】

つぎに、上記３つの処理モードの各処理手順について各図面を参照しながら説明する。図２は、生成モード時の処理手順を示すフローチャートである。なお、同図に示すように

IPR2025-00069
CrowdStrike EX1002 Page 164

、アクセスログなどのトラフィックデータに基づいて仮の検知ルールデータ２１が生成されて記録されているものとする。例えば、仮の検知ルールデータ２１には、任意のトラフィックデータに対して上述のＳｎｏｒｔなどのルールセットを適用し、このルールセットに反応した複数のセッション（セッション群）などが記録されている。

【0048】

図２のフローに戻り、まず、仮の検知ルールデータ２１に記録されている仮の検知ルールデータが検知ルール生成装置１２に読み込まれる（ステップＳ１０１）。検知ルール生成装置１２は、不正アクセスを特徴づける検知ルールの自動生成処理（詳細は後述）を行う（ステップＳ１０２）。自動生成された検知ルールは、検知ルールデータベース１３に送信され（ステップＳ１０３）、登録される（ステップＳ１０４）。また、この検知ルールはＩＤＳ１４に送信され（ステップＳ１０５）、設定登録される（ステップＳ１０６）。ここで、自動生成された検知ルールを検知ルールデータベース１３に加えてＩＤＳ１４にも設定登録するようにしているが、この理由は不正アクセスの検出処理を迅速に行うためである。ただし、検出処理に対する時間的要求がさほど厳しくない場合には自動生成された検知ルールをＩＤＳ１４に設定登録しなくてもよい。この場合には、不正アクセスの判定処理を行う際に、ＩＤＳ１４側から検知ルールデータベース１３を参照するような処理方式を採用すればよい。

【0049】

ところで、上記でいうセッションという概念は、「接続要求」があった時点から「終了通知」または「タイムアウト」になった時点までの期間を意味するものである。例えば、ＴＣＰの場合では、ＳＹＮパケット（接続要求パケット）からＦＩＮ（終了通知）、または、ＲＳＴ（切断要求パケット）送信されるまでか、あるいは通信が途絶えて（通信相手からのパケット送信が途絶えて）から設定したタイムアウトになった時点までの期間を意味する。

【0050】

つぎに、追加モード時の処理手順について説明する。図3は、追加モード時の処理手順を示すフローチャートである。同図において、パッシブホストセンサ１１は、ネットワーク１から自身に対して行われたアクセスを検出する（ステップＳ１１１）。上述のように、「パッシブホストセンサ１１に対して行われる通信は全て何らかの悪意を持って行われる」ということを前提としているため、パッシブホストセンサ１１は、ステップＳ１１１で検出されたアクセスを不正アクセスと判定し、不正アクセスがあったことをトラフィックデータベース５に対して通知（ステップＳ１１２）するとともに、当該アクセスにかかるアクセスログを検知ルール生成装置１２に送信する（ステップＳ１１３）。

【0051】

トラフィックデータベース５は、ネットワーク１で行われているアクセスデータを、常時、所定の間隔で記録しているが、パッシブホストセンサ１１から不正アクセスが通知された場合には、通常トラフィックデータの更新処理を行う（ステップＳ１１４）。なお、ここでいう「通常トラフィックデータ」とは、不正アクセス以外のトラフィックデータのみで構成されたトラフィックデータのことを指しており、この更新処理では、トラフィックデータベース５に蓄積されているトラフィックデータ（通信ログデータ）の中から不正アクセスにかかるセッションのトラフィックデータが除去される。

【0052】

一方、検知ルール生成装置１２は、検知ルールの自動生成処理に先立ってトラフィックデータベース５から通常トラフィックデータを読み込み（ステップＳ１１５）、この通常トラフィックデータとパッシブホストセンサ１１から送信されたアクセスログとに基づいて検知ルールの自動生成処理を行う（ステップＳ１１６）。なお、ステップＳ１１６の処理は、「生成モード時における検知ルールの自動生成処理」である図２のステップＳ１０２の処理と同等である。その後のステップＳ１１７～Ｓ１２０処理、すなわち、検知ルール生成装置１２で自動生成された検知ルールが検知ルールデータベース１３や、ＩＤＳ１４に登録される処理については、生成モード時と同様な処理であり、その説明を省略する

IPR2025-00069
CrowdStrike EX1002 Page 165

。

【0053】

ところで、上記の処理では、通常トラフィックデータを生成する際には、パッシブホストセンサ１１からの不正アクセスの通知に基づいて、常時記録しているトラフィックデータからパッシブホストセンサ１１で観測されたセッション「のみ」を除去するようにしている。一方、このような除去処理とは異なるつぎのような処理を適用することも可能である。例えば、パッシブホストセンサで観測されたセッションだけでなく、同種と考えられる不正を含むセッションを除去するような処理を行う場合には、上記ステップＳ１１６の処理後に、不正アクセスを通知するとともに、生成された検知ルールセットをトラフィックデータベース５に対して通知することもできる。

【0054】

なお、図３に示す追加モード時の通常トラフィックデータの読込処理（ステップＳ１１５）では、通常トラフィックデータの全体を読み込む処理と、ステップＳ１１４の処理にて更新された通常トラフィックデータの更新分のデータ（差分データ）だけを読み込む処理とが考えられ、いずれの処理を適用してもよい。ただし、通常トラフィックデータは膨大な量のデータ群であり、検知ルールの生成の都度、通常トラフィックデータを読み込むことは得策ではなく、後者のように通常トラフィックデータの差分データだけを読み込むようにすれば、処理負荷の低減化や、処理時間の短縮化が可能となる。

【0055】

また、図２に示す生成モード時の処理手順の中では、頻出文字列リストの除外処理を行わない場合、あるいは予め検知ルール自動生成装置内に頻出文字列リストが保持されている場合を想定しているので、検知ルールの自動生成処理（ステップＳ１０２）において、通常トラフィックデータの読込処理を行ってはいない。しかしながら、生成モード時の処理手順においても、図３に示す追加モード時の処理手順のように、通常トラフィックデータを読み込んだ後に頻出文字列リストを生成するとともに、生成された頻出文字列を仮の検知ルールから除外する処理を行うようにしてもよい。

【0056】

つぎに、判定モード時の処理手順について説明する。図４は、判定モード時の処理手順を示すフローチャートである。同図において、ＩＤＳ１４は、ネットワーク１で行われたアクセスを検出し（ステップＳ１２１）、検出したアクセスが自身に設定登録されている検知ルールに反応するか否かを判定し（ステップＳ１２２）、検知ルールに反応した場合（ステップＳ１２２，Ｙｅｓ）にはアラートを出力する（ステップＳ１２５）。一方、全ての検知ルールに反応しない場合（ステップＳ１２２，Ｎｏ）にはアラートを出力しない。なお、検知ルールに反応した場合（ステップＳ１２２，Ｙｅｓ）には、不正アクセスがあったことをトラフィックデータベース５に対して通知する（ステップＳ１２３）。トラフィックデータベース５は、ＩＤＳ１４からの通知に基づいて、通常トラフィックデータの更新処理を行う（ステップＳ１２４）。

【0057】

つぎに、検知ルールの自動生成処理について説明する。図５は、図２に示すステップＳ１０２の処理や、図３に示すステップＳ１１６の処理に対応するものであり、自動生成処理の一例としてＨＴＴＰ（Ｈｙｐｅｒ　Ｔｅｘｔ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）通信に適用した検知ルール自動生成処理の処理手順を示すフローチャートである。図５に示すフローには、同一の不正行為だけでなく、同種の不正行為をも含んだリクエストを検出する一方で、不正でないものを不正と判断するフォールスポジティブ（以下「Ｆ.Ｐ.」と標記）や、不正なものを不正でないと判断するフォールスネガティブ（以下「Ｆ.Ｎ.」と標記）を極力少なくするための処理が含まれている。なお、このフローは、好適な一例としてＨＴＴＰ通信の場合について説明するものであり、必ずしもＨＴＴＰプロトコルに限定されるものではない。例えば、ＳＭＴＰプロトコルや、ＦＴＰプロトコルなどのアプリケーション層の通信プロトコルにも適用できる。この場合、ＨＴＴＰプロトコルのメッセージと同等の構造を有しているものに対して適用することができ、同等な構造がない

IPR2025-00069
CrowdStrike EX1002 Page 166

ものに対しては当該処理をスキップしてもよい。

【0058】

ここで、図５のフローチャートの説明に際し、以降の説明の理解を容易にするため、ＨＴＴＰリクエストメッセージの構造について説明する。図６は、ＨＴＴＰリクエストメッセージの構造を示す図である。ＨＴＴＰリクエストメッセージはＲＦＣ２６１６によって定義されており、同図に示すように、スタートライン、メッセージヘッダ部、メッセージボディの３つの部分から構成される。

【0059】

スタートラインには、主としてリクエストの動作および対象となるファイルが記述され、空白を区切り文字として、メソッド、ＵＲＩ、ＨＴＴＰバージョンの３つの部分に分けられる。ＵＲＩには、“？”に続けてクエリ文字列が続く場合がある。クエリ文字列はサーバ側で実行されるプログラムにデータを渡すために用いられる。なお、サーバ側のプログラムによって形式は異なるが、一般には、変数名と値が“＝”で結ばれ、それが複数個の“＆”を区切りとして連結したものである場合が多い。一方、メッセージヘッダ部は、クライアント側の情報をサーバ側に伝えるために用いられる。なお、メッセージヘッダ部では、一つの行に記述されるメッセージヘッダが複数記述され、各メッセージヘッダは“：”で区切られた“フィールド名”と“フィールド値”から構成される。また、メッセージボディは、サーバ側で実行されるプログラムにデータ渡す際に用いられるものであり、上記ＵＲＩのクエリ文字列と同様の形式である場合が多い。

【0060】

つぎに、図５に戻り、検知ルール生成装置１２で行われる検知ルールの自動生成処理について説明する。同図に示すように、この自動生成処理ステップは、ステップＳ２０１～Ｓ２０４の第１の剪定処理ステップと、ステップＳ２０５～Ｓ２０７の第２の剪定処理ステップとに分解することができる。ここで、第１の剪定処理ステップは、検知ルール自動生成の前処理に相当するものであり、処理対象の種類（通信プロトコル）や、処理対象を構成するメッセージフィールドの特性に応じて、後続の第２の剪定処理を行わせるか否かのフィルタリングを行うものである。一方、第２の剪定処理ステップは、検知ルール自動生成の本処理に相当するものであり、実際に検知ルールの自動生成処理を行うものである。ただし、後述のように、一旦、仮の検知ルールセットを生成し、生成された仮の検知ルールセットから所定の文字列を除外するようなフィルタリング処理を併用している。これらの第１、第２の剪定処理ステップを行うことで、単純に自動生成処理を行う場合に比べて、処理時間、処理負荷を大幅に低減させることができ、また、誤検知の確率を大幅に低下させることができるという利点がある。

【0061】

図５において、検知ルール生成装置１２は、パッシブホストセンサ１１から送信された不正アクセスログ（ＨＴＴＰリクエスト）に対して、その処理対象を特定する。例えば、“スタートライン”、“メッセージヘッダ”、“メッセージボディ”のいずれに該当するのかを特定する（ステップＳ２０１）。処理対象が“メッセージヘッダ”以外（ステップＳ２０２、Ｎｏ）ならば、第１の剪定処理ステップを抜けて第２の剪定処理ステップ（ステップＳ２０５）の処理に移行する。一方、処理対象が“メッセージヘッダ”の場合には（ステップＳ２０２、Ｙｅｓ）、メッセージヘッダを構成する“フィールド名”および“フィールド値”のそれぞれに対して、それぞれ異なる判定処理が行われる。まず、フィールド名に対しては、各セッションにおけるフィールド名の出現頻度と、ヘッダフィールドの種類（例えば、Ｃｏｏｋｉｅヘッダフィールド、Ｉｆ－Ｍｏｄｉｆｉｅｄ－Ｓｉｎｃｅヘッダフィールド）ごとに算出された所定のしきい値としての第１のしきい値との間で比較処理が行われる（ステップＳ２０３）。フィールド名の出現頻度が第１のしきい値以下の場合には（ステップＳ２０３、Ｎｏ）、第１の剪定処理ステップを抜けて第２の剪定処理ステップ（ステップＳ２０５）の処理に移行し、フィールド名の出現頻度が第１のしきい値よりも大きい場合には（ステップＳ２０３、Ｙｅｓ）、ステップＳ２０４に移行する。

IPR2025-00069
CrowdStrike EX1002 Page 167

【0062】
また、フィールド値に対しては、各セッションにおいて、フィールド値を構成する文字列の任意の文字種間の遷移確率の平均値と、所定のしきい値としての第２のしきい値との間で比較処理が行われる（ステップＳ２０３）。このフィールド値の遷移確率の平均値が第２のしきい値より大きい場合には（ステップＳ２０４、Ｎｏ）、第２の剪定処理ステップに移行することなく自動生成処理を終了し、フィールド値の遷移確率の平均値が第２のしきい値以下の場合には（ステップＳ２０４、Ｙｅｓ）、第２の剪定処理ステップのステップＳ２０５に移行する。なお、上記の説明の中で、ステップＳ２０４で行われる平均処理は、相乗平均、相加平均などの任意の平均処理を適用することができる。また、上記の説明の中の「文字種間の遷移確率」については、以下にその詳細について補足する。
【0063】
「文字種間の遷移確率」とは、メッセージヘッダなどに含まれる文字列の各文字の移り変わりを確率的に表したものである。通常、文字列は左から右へ向かって変化するという前提であり、文字列のある２文字に着目した場合、左側の文字種が観測された後、右側の文字種が出現する確率は、左側の文字種と、右側の文字種との関係で決定され、文字種ごとに異なる確率値をとる。この確率値を「文字種間の遷移確率」と定義している。例えば、日本語の場合、文末に「です。」という文字列が頻繁に出現するので、「で」という文字種のつぎに「す」という文字種に遷移する確率は高くなる。このように、ステップＳ２０３の処理では、メッセージヘッダに現れる文字を対象として、上記のように定義された文字種間の遷移確率を予め算出するようにしている。
【0064】
つぎに、図５のフローチャートに戻って、第２の剪定処理ステップについて説明する。検知ルール生成装置１２は、スタートライン、メッセージボディなどのリクエストデータや、第１の剪定処理ステップの処理でフィルタリングされたメッセージヘッダから不正アクセスを検出するための文字列を抽出した仮の検知ルールセットを生成し（ステップＳ２０５）、その一方で、通常トラフィックデータに基づいて頻出文字列リストを生成し、あるいは頻出文字列リストに新たな検知ルールを追加する（ステップＳ２０６）。検知ルール生成装置１２は、検知ルールセットから頻出文字列リストの上位に位置する所定の頻出文字列を除去した検知ルール（真の検知ルール）を生成して出力する（ステップＳ２０７）。なお、この検知ルールが、検知ルールデータベース１３に登録され、ＩＤＳ１４に反映されることは前述のとおりである。
【0065】
このように、図５に示す第１の剪定処理ステップおよび第２の剪定処理ステップの処理に基づいて、同種の不正行為を含んだリクエストの検出を可能とする一方で、Ｆ.Ｐ.数やＦ.Ｎ.数を局限可能な検知ルールを自動生成することができる。なお、上述の説明の中で、ステップＳ２０５の仮の検知ルールセットの生成処理、ステップＳ２０６の頻出文字列の生成処理およびステップＳ２０７の頻出文字列による除外処理の各説明が不足しているので、さらに説明を加える。
【0066】
図７および図８は、仮の検知ルールセットの生成処理について補足するための図であり、より詳細には、図７は、同種の不正アクセスを検出するための検知ルールの一例を示す説明図であり、図８は、プロトコル構文を考慮した階層的な分割手法の一例を示す説明図である。まず、図７において、上段部には、ＨＴＴＰプロトコルのリクエストメッセージ（Ａ）が示されている。中上段部には、リクエストメッセージ（Ａ）から抽出された３つの検知ルール（ａ），（ｂ），（ｃ）が示されている。このような検知ルールが生成されている場合に、例えば、中下段部に示される不正なリクエストメッセージ（Ｂ），（Ｃ）が検出された場合を考える。このとき、検知ルール（ａ）ではリクエストメッセージ（Ｂ），（Ｃ）ともに検知することができず、検知ルール（ｃ）ではリクエストメッセージ（Ｂ），（Ｃ）ともに検知することができるが、不正なアクセス以外にも反応する可能性がある。一方、検知ルール（ｂ）ではリクエストメッセージ（Ｂ），（Ｃ）ともに検知する

IPR2025-00069
CrowdStrike EX1002 Page 168

ことができ、また、不正なアクセス以外に反応する可能性は検知ルール（ｃ）よりも小さい。このように、検知ルール（ｂ）は不正な部分の特徴部分のみが適切に記述された例としての一例を示すものである。

【0067】

また、図８には、ＨＴＴＰプロトコルのスタートラインの記述例が示されている。例えば、スタートラインでは、空白によって、メソッド、ＵＲＩ、バージョンに分割し、ＵＲＩは“？”によってファイル指定部およびクエリ文字列に分割し、さらに、ファイル指定部は、“／”によって分割する。なお、分割途中の段階を含め、各段階で生成された文字列の全てを、仮の検知ルールとして残しておくことが重要なポイントである。このような分割途中の段階で生成された文字列を含めることで、同種の不正アクセスを検出する確率を増大させることができる。なお、同図には示していないが、メッセージヘッダや、メッセージボディについても同様な手法で分割することができる。

【0068】

分割に際して、他の考慮すべき事項として、生成した検知ルールが全く関係のない文字列や、当該文字列を部分的に含む文字列に偶然に一致することを避ける必要がある。このため、図８の下段部に示すように、一旦分割された文字列の両端に分割に用いた区切り文字を残すようにする。例えば、ＵＲＩ部分を分割した、“ａｒｃｈ”という文字列が生成された場合には、分割に用いた文字“／”を両端に残し、“／ａｒｃｈ／”を検知ルールとする。この処理により、“ｒｅｓｅａｒｃｈ”や、“ａｒｃｈｉｔｅｃｔｕｒｅ”などの文字列に偶然に一致するような状況が回避され、また、ＵＲＩから生成された検知ルールがＵＲＩ部分により限定的にマッチするようになり、Ｆ.Ｐ.数の増加防止に効果的である。

【0069】

一方、図９は、頻出文字列の生成処理および仮の検知ルールに対する頻出文字列の除外処理を補足するための図であり、より詳細には、通常トラフィックデータの中に含まれる文字列の出現頻度の一例を示す図である。同図に示すグラフは横軸が文字列を出現頻度順に並べたときの順位であり、縦軸は当該順位文字列の総リクエスト数に対する出現頻度である。例えば、同図の例では、縦軸上の切片に’；ｑ＝’という文字列の総リクエスト数に対する出現頻度である“２４６０４９”の値がプロットされ、以下、右隣の所定の位置に’ｉｍａｇｅ／’、’ｔｅｘｔ／’、・・・のそれぞれの値がプロットされる。同図では、好適な例として、面積の８０％を占めるまでの文字列を高頻度で出現する文字列（頻出文字列）として定義し、これらの文字列は不正の特徴を表していないものとして取り扱われる。すなわち、仮の検知ルールの中にこれらの文字列を含んでいる場合には、検知ルールから取り除かれる。

【0070】

先に述べたように、通常トラヒックデータの大部分は正規の通信によって占められている。したがって、不正な通信に特有の文字列は通常トラヒックデータ中には高頻度では存在しないはずである。そこで、通常トラヒックデータ中にあるしきい値以上で高頻度に出現する文字列は、通常の通信にも含まれる一般的な語と判断して検知ルールから除くという処理を行うことで、同種の不正行為を含んだリクエストの検出を可能とし、その一方で、不正でないものを不正と判定するＦ.Ｐ.数を局限することができる。

【0071】

なお、この実施の形態では、専用の装置を用いた構造について説明したが、本発明の適用対象は、必ずしも実施の形態に限定して解釈する必要はない。また、具体的構造についても、図１のブロック図に示されるものに限定して解釈する必要はなく、上記の手法を用いてネットワークの不正アクセスを検出できるものであればよい。

【0072】

（実施の形態２）

実施の形態２にかかる不正アクセス検出装置の構成は、図１に示す実施の形態１の構成と同一、あるいは同等である。一方、この実施の形態の処理は、実施の形態１の処理と比

IPR2025-00069
CrowdStrike EX1002 Page 169

較して以下のような特徴を有している。
（１）　実施の形態１の処理では、検知ルールに一つでも反応すればアラートを発生していたが、この実施の形態の判定処理では、反応した検知ルールに重要度を設定し、セッション単位での重要度の合計（以下「得点」と呼称）が所定値以上の場合にアラートを発生させる。
（２）　実施の形態１の処理では、許容Ｆ.Ｐ.数による制御という概念が存在しなかったが、この実施の形態では、許容Ｆ.Ｐ.数に基づいた制御を行う。
（３）　上記（２）に関連するが、設定された許容Ｆ.Ｐ.数と、検知ルールごとの得点の傾向とに基づいて決定される判定しきい値を設定し、当該判定しきい値よりも上位順位にある検知ルールに反応したときにアラートを発生させる。
【0073】
つぎに、上述した実施の形態２の特徴に含まれる「重要度」および「判定しきい値」の概念について説明する。実施の形態１のところで説明したように、パッシブホストセンサ１１が観測した１つの不正アクセスから複数個の検知ルールが生成される。これらの検知ルールには、リクエストメッセージ中の不正な部分を適切に記述しＦ.Ｐ.を発生させない理想的なものから、逆にＦ.Ｐ.を多く発生させるものまで、その性能にはばらつきがある。そこで、「重要度」という概念を導入し、検知ルールに対して、この「重要度」で重み付け処理を行うことを考える。具体的には、Ｆ.Ｐ.の発生具合によって検知ルールの性能を評価し、検知ルールが持つ情報量の観点から、Ｆ.Ｐ.の発生が少ない検知ルールの重要度は高く、逆にＦ.Ｐ.を多く発生させる検知ルールの重要度は低くなるように、それぞれの重要度に傾きを付けるように処理する。
【0074】
ここで、重要度は次式のように定義する。
重要度＝１／（過去のトラヒックデータに対する反応数）　・・・（１）
なお、過去のトラフィックデータとして上記で定義した通常トラフィックデータを用いるのが好適である。なぜなら、通常トラフィックデータ中には不正なトラフィック（セッション）の含まれる可能性が低いので、重要度の適正性を確保することができるからである。ところで、式（１）において、過去のトラヒックデータに対する反応数が０のときは、重要度の値が∞になってしまうので、適度な値を設定する必要がある。同式によれば、過去のトラヒックデータに対する反応数＝１のときに重要度＝１となるので、過去のトラヒックデータに対する反応数が０のときは、例えば、重要度＝２に設定することができる。なお、過去のトラヒックデータに反応する場合より反応しない場合の方が重要度を高く設定するという意味では、過去のトラヒックデータに対する反応数が０のときに、１を超える重要度が設定されていればよい。
【0075】
具体的には、検知ルールの１つを通常トラヒックデータに対して適用し、通常トラヒックデータに反応した数をフォールスポジティブと見なす。このようにして算出された検知ルールごとの反応数に基づき、反応数が少ない検知ルールは重要度を高く、反応数が多いものは重要度を低く設定するように処理する。なお、この重要度の設定処理は、予め実施しておくことができる。例えば、図２に示した検知ルールの自動生成処理（ステップＳ１０２）時に、仮の検知ルールデータ２１内に含ませた通常トラフィックデータに基づいて重要度を設定すればよい。また、図３に示した検知ルールの自動生成処理（ステップＳ１１６）時に、通常トラフィックデータに追加されたセッションに対する各検知ルールの重要度の更新処理を行うようにすればよい。
【0076】
つぎに、判定しきい値について説明する。この実施の形態では各検知ルールに上述のような重要度を導入したことにより、アラートを発生させる基準を、従来の、検知ルールが１つでも反応したセッションに対してアラートを発生させるという処理から、判定しきい値と呼ばれる基準を設定し、この判定しきい値を基準とした判定処理を導入する。
【0077】

IPR2025-00069
CrowdStrike EX1002 Page 170

判定しきい値の設定方法としては、例えば、以下の手順に示される。
（１）　許容Ｆ.Ｐ.数をＮに設定
（２）　通常トラフィックデータの各セッションに検知ルールを適用
（３）　各セッションごとに反応した検知ルールの重要度の合計（以下「得点」と呼称）を算出
（４）　得点を降順でソート
（５）　上位Ｎ番目のセッションとＮ＋１番目の間の所定の得点に判定しきい値を設定

【0078】
図１０は、判定しきい値の概念をさらに詳細に説明するための図である。同図の例では、１日以上（通常は、複数日分）の通常トラフィックデータに対して検知ルールを適用し、各セッションごとに反応した検知ルールの得点を算出し、得点の降順に整列させたものである。同図の例では、１日当たりの許容Ｆ.Ｐ.数が５に設定されるので、得点が２０９のセッションＳと、得点が１３４のセッションＬとの間に判定しきい値を設定するためのラインが引かれ、１３４以上で２０９以下の任意の値に判定しきい値が設定される。なお、判定しきい値を２０９に近い値に設定した場合と、１３４に近い値に設定した場合とでは、前者の方が、後者に比較して、Ｆ.Ｐ.数が減少する一方で、未検知数が増加する傾向になる。したがって、これらの判定しきい値や、許容Ｆ.Ｐ.数の設定については、管理者の判断に委ねられる部分となる。

【0079】
つぎに、上述のような「重要度」および「判定しきい値」の概念が導入された実施の形態２の不正アクセス検出装置の動作について説明する。図１１は、この発明の実施の形態２にかかる不正アクセス検出装置の判定モード時の処理手順を示すフローチャートである。なお、生成モード時および追加モード時の処理手順は、それぞれ図２および図４に示す実施の形態１の処理手順に上述の重要度の設定処理手順を含めたものと同一または同等であるので、説明を省略する。

【0080】
図１１において、ＩＤＳ１４は、ネットワーク１で行われたアクセスを検出し、検出したアクセスが自身に設定登録されている検知ルールに反応するか否かの判定処理を全ての検知ルールに対して行う（ステップＳ３０１）。つぎに、ＩＤＳ１４は、検出したアクセスが１以上の検知ルール反応したか否かを判定し（ステップＳ３０２）、全ての検知ルールに反応しない場合（ステップＳ３０２，Ｎｏ）にはアラートを出力せずにこの判定モードの処理から抜け出るが、１以上の検知ルールに反応した場合（ステップＳ３０２，Ｙｅｓ）には、通常トラフィックデータに基づいて予め算出されている重要度を参照して、各セッションごとの得点の算出処理を行う（ステップＳ３０４）。ＩＤＳ１４は、各セッションの得点と、上述した手順などにより予め設定された判定しきい値とをそれぞれ比較し（ステップＳ３０５）、全てのセッションが判定しきい値未満の場合（ステップＳ３０５，Ｎｏ）にはアラートを出力せずにこの判定モードの処理から抜け出るが、判定しきい値以上の得点を有する１以上のセッションが存在する場合（ステップＳ３０５，Ｙｅｓ）にはアラート（要すれば当該セッション番号や、当セッションの内容も含む）を出力する（ステップＳ３０６）。なお、アラートが出力された場合には、不正アクセスがトラフィックデータベース５に通知され（ステップＳ３０７）、爾後の判定処理に備えて通常トラフィックデータが更新される（ステップＳ３０８）。

【0081】
なお、上記の処理手順の中で、重要度の重み付けを行わず（すなわち、重要度は全て同一）、判定しきい値のみで判定してもよい。この場合、ステップＳ３０４の処理をバイパスすることができる。

【0082】
（実施の形態２の装置の評価）
図１２は、実施の形態２の不正アクセス検出装置の評価実験を行った結果を示す図である。図１２において、横軸を設定した１ルールセットあたりの許容Ｆ.Ｐ.数とし、縦軸を

IPR2025-00069
CrowdStrike EX1002 Page 171

検出率およびＦ.Ｐ.数とした。また、実線部分は重要度と判定しきい値の両者を導入した場合の波形であり、破線部分は判定しきい値のみを導入した場合の波形である。

【0083】

ここで、評価実験の環境を簡単に説明する。まず、１００台規模のホストが接続するＬＡＮを出入りする１日分のトラヒックデータにＳｎｏｒｔに付属のルールセットを適用し、反応したセッションを、パッシブホストセンサ１１で観測された新種の不正アクセス手法と想定し、反応しなかったトラヒックデータを通常トラヒックデータと想定してこれらをテストデータとした。つぎに、不正なリクエストデータの１つをパッシブホストセンサ１１で観測された未知の不正と想定し、本発明の処理手順に基づいて検知ルールを生成した。また、生成した検知ルールセットを不正アクセスのトラヒックに適用し、同種の不正リクエストを検知できるかどうかを調べた。さらに、通常トラヒックデータに適用にしたときのＦ.Ｐ.数についてもカウントした。

【0084】

図１２の結果に示されるように、重要度および判定しきい値を導入した場合、ならびに判定しきい値のみを導入した場合の両者ともに殆どの領域において９５％前後の良好な検出率が維持されている。また、許容Ｆ.Ｐ.数を５０から１０程度に軽減させた場合であっても、検出率の低下がほとんどなく、良好な検出性能が維持され、実運用に十分耐えうる検出性能が得られている。

【0085】

図１３は、実運用上のデータを用いて評価実験を行った結果を示す図表であり、より詳細には、ある年月の２１日～２８日までの８日間に観測されたＨＴＴＰリクエストに対する検知結果を示す図表である。図１２の実験結果はＳｎｏｒｔに付属の標準ルールセットを未知の不正と想定し、人為的に生成したテストデータを用いて行ったものであるが、図１３に示す実験結果は、この実施の形態の不正アクセス検出装置を実稼働のネットワーク上に実際に設置して評価したものである。このネットワークには１００台程度のホストが接続され、常時約３０のホストが外部のｗｅｂサーバにアクセスしている。また、ネットワーク内にはｗｅｂサーバが１０台稼働し、ネットワークの入口では全てのトラヒックが観測されダンプデータとして保存されている。なお、ネットワーク入口を出入りするトラヒックは、１日あたり約３０，０００セッションである。

【0086】

図１３に示すように、８日間の全てにおいて検知率が１００％であり、良好な結果が得られている。また、フォールスポジティブ数も平均して１日あたり９個に抑えられており、実運用に耐えられる値を示している。この結果により、この実施の形態の不正アクセス検出装置の有用性が十分に証明されているものと考える。

【産業上の利用可能性】

【0087】

以上のように、この発明にかかる不正アクセス検出装置は、シグネチャマッチング型のＩＤＳをベースとしているものの、検知ルールが明らかでない新種や未知の不正アクセスに対処することのできるＩＤＳとして有用である。

【図面の簡単な説明】

【0088】

【図1】この発明の実施の形態１にかかる不正アクセス検出装置の構成を示すブロック図である。

【図2】生成モード時の処理手順を示すフローチャートである。

【図3】追加モード時の処理手順を示すフローチャートである。

【図4】判定モード時の処理手順を示すフローチャートである。

【図5】自動生成処理の一例としてＨＴＴＰ通信に適用した検知ルール自動生成処理の処理手順を示すフローチャートである。

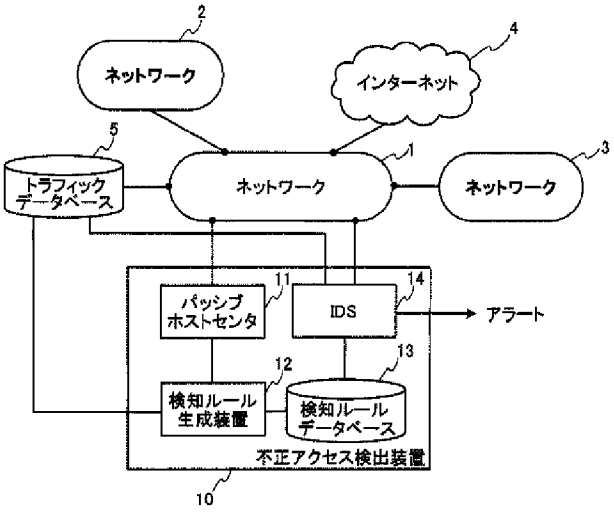
【図6】ＨＴＴＰリクエストメッセージの構造を示す図である。

【図7】同種の不正アクセスを検出するための検知ルールの一例を示す説明図である。

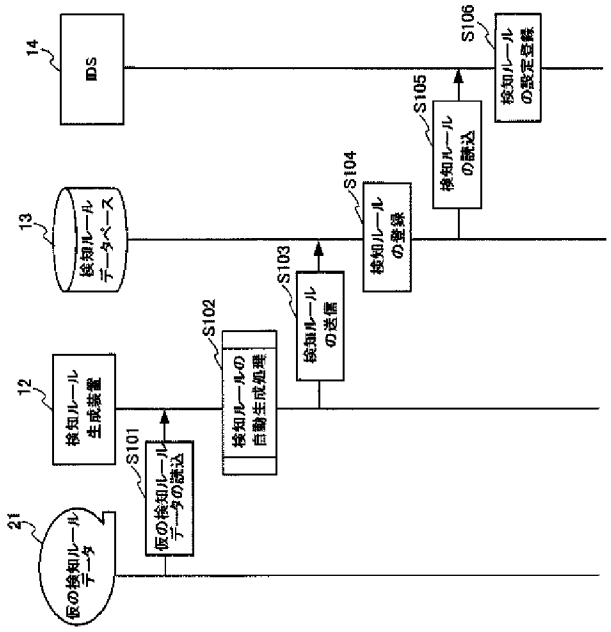
IPR2025-00069
CrowdStrike EX1002 Page 172

【図8】図８は、プロトコル構文を考慮した階層的な分割手法の一例を示す説明図である
。
【図9】通常トラフィックデータの中に含まれる文字列の出現頻度の一例を示す図である
。
【図10】判定しきい値の概念をさらに詳細に説明するための図である。
【図11】この発明の実施の形態２にかかる不正アクセス検出装置の判定モード時の処理手順を示すフローチャートである。
【図12】実施の形態２の不正アクセス検出装置の評価実験を行った結果を示す図である。
【図13】実運用上のデータを用いて評価実験を行った結果を示す図表である。
【符号の説明】
【0089】
１，２，３　ネットワーク
４　インターネット
５　トラフィックデータベース
１０　不正アクセス検出装置
１１　パッシブホストセンサ
１２　検知ルール生成装置
１３　検知ルールデータベース
２１　仮の検知ルールデータ

【図1】

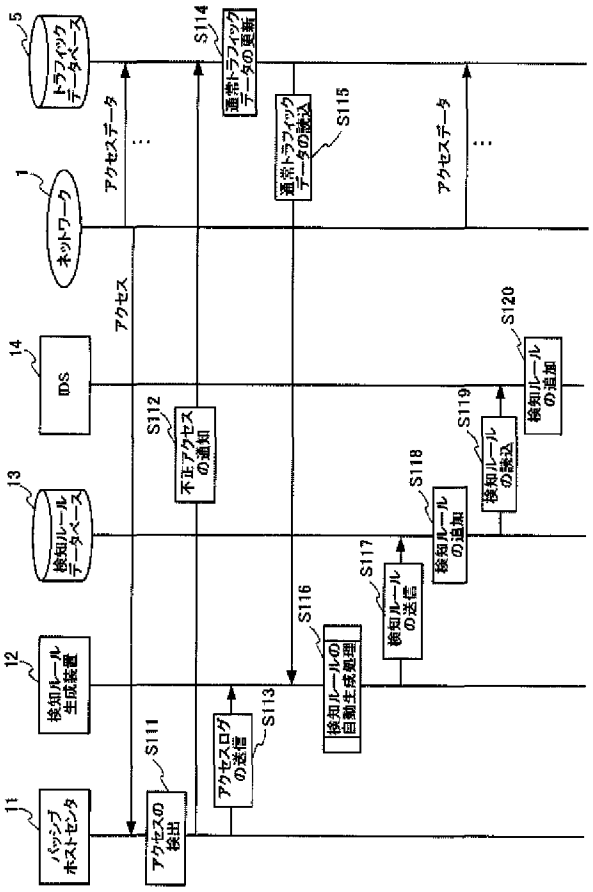


【図2】

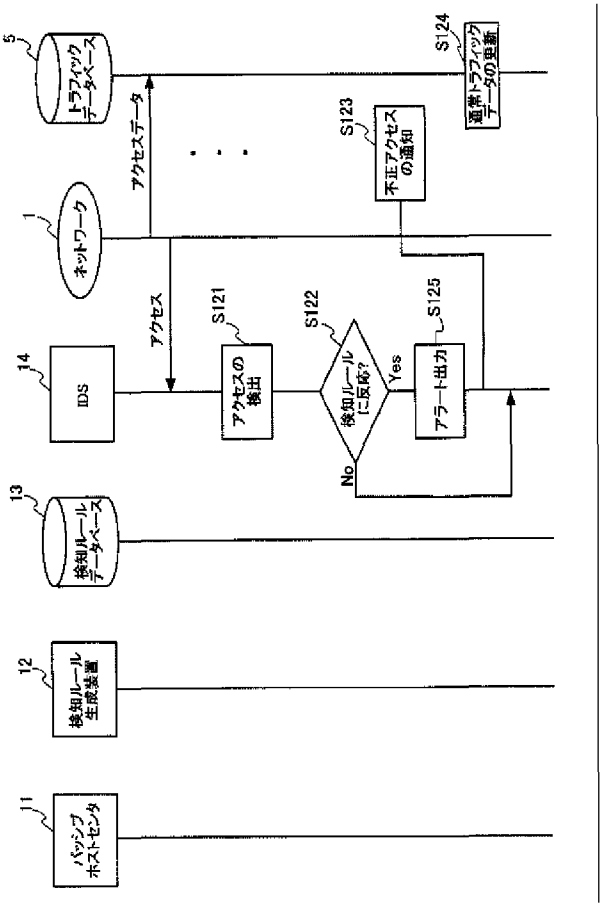


IPR2025-00069
CrowdStrike EX1002 Page 174

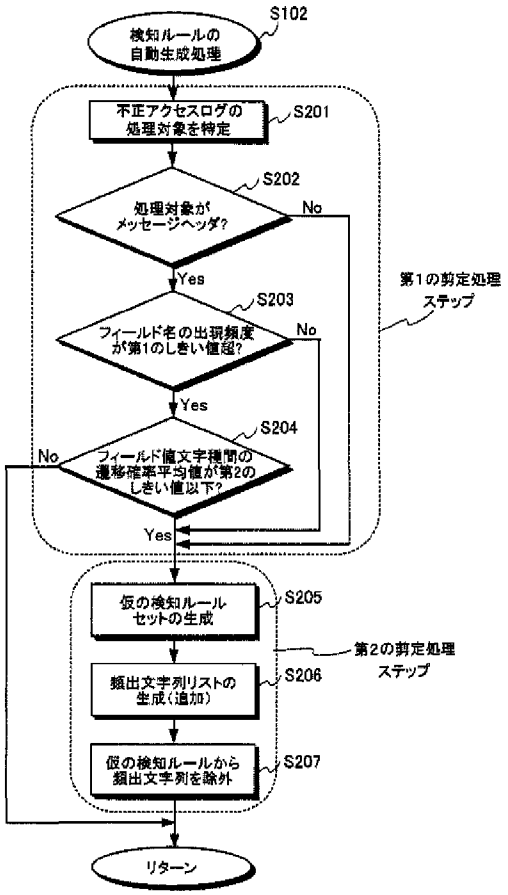
【図3】



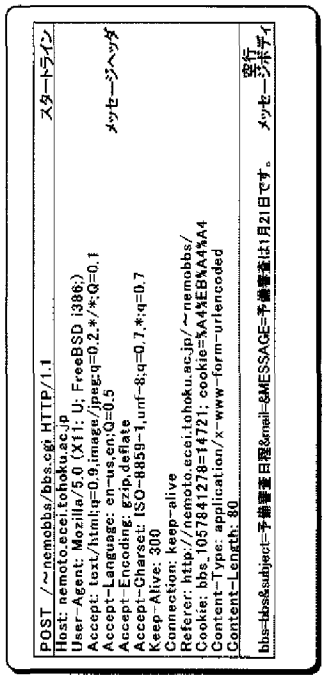
【図4】



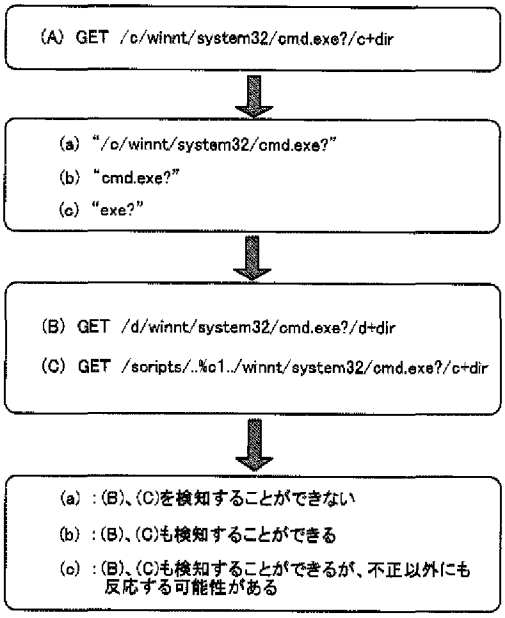
【図5】



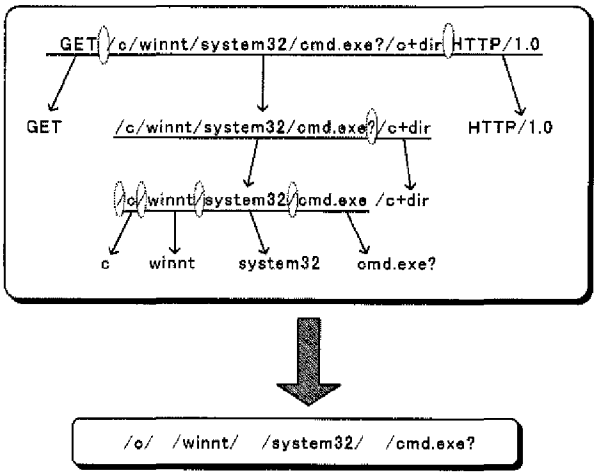
【図6】



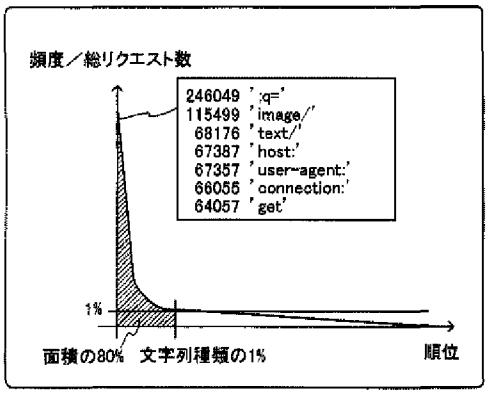
【図7】



【図8】



【図9】



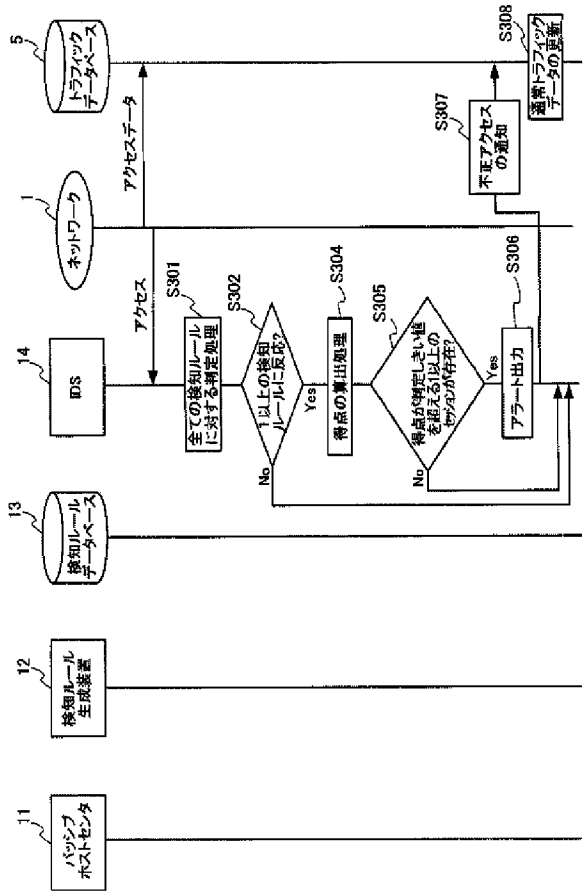
【図10】

判定しきい値の設定例
(N=5)の場合

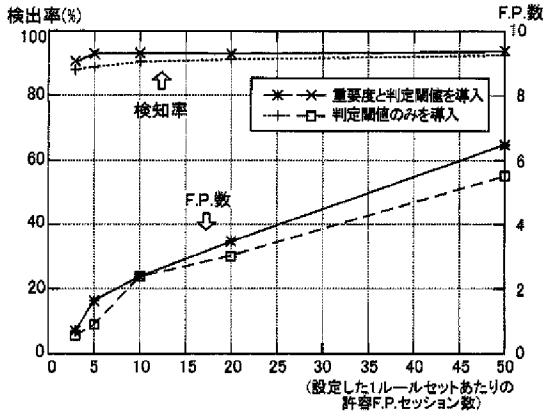
順位	セッション名	得点
1	セッションB	1034
2	セッションF	509
3	セッションA	243
4	セッションC	214
5	セッションS	209
6	セッションL	134
7	セッションH	124
8	セッションP	115
⋮	⋮	⋮

判定しきい値

【図11】



【図12】



【図13】

	21	22	23	24	25	26	27	28	平均
検知すべきセッション数	48	65	52	8	46	1486	2771	965	
検知できた数	48	65	52	8	46	1486	2771	965	
フォールスネガティブ数	0	0	0	0	0	0	0	0	
検知率(%)	100	100	100	100	100	100	100	100	100
フォールスポジティブ数	3	5	8	26	12	8	7	3	9

(72)発明者　加藤　寧
宮城県仙台市青葉区荒巻字青葉５　東北大学大学院内
(72)発明者　根元　義章
宮城県仙台市青葉区荒巻字青葉５　東北大学大学院内
Ｆターム(参考) 5B085 AE00

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 March 2007 (08.03.2007)

PCT

(10) International Publication Number
WO 2007/027739 A1

(51) International Patent Classification:
G06F 9/455 (2006.01) *G06F 9/00* (2006.01)
G06F 9/06 (2006.01) *G06F 12/00* (2006.01)

(21) International Application Number:
PCT/US2006/033815

(22) International Filing Date: 29 August 2006 (29.08.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/215,380 30 August 2005 (30.08.2005) US

(71) Applicant *(for all designated States except US)*: **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(72) Inventor: **TRAUT, Eric, P.**; One Microsoft Way, Redmond, Washington 98052-6399 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

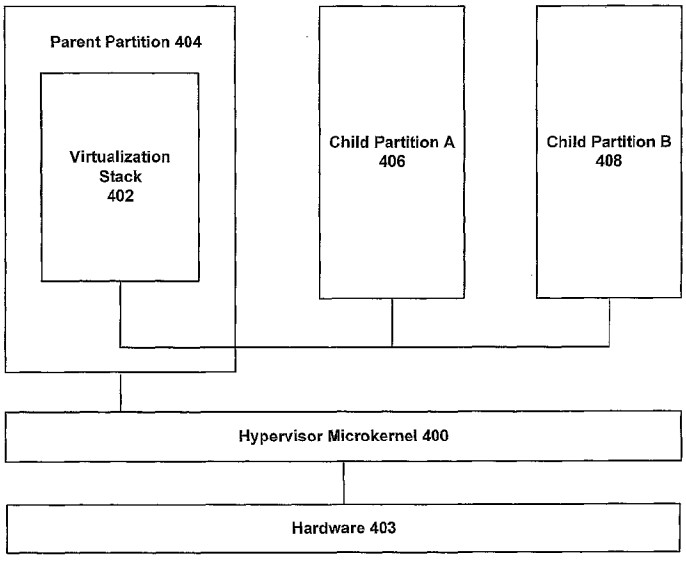
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: HIERARCHICAL VIRTUALIZATION WITH A MULTI-LEVEL VIRTUALIZATION MECHANISM



(57) Abstract: Hierarchical virtualization is disclosed, where such virtualization can be accomplished with a multi-level mechanism. The hierarchical virtualization includes using a hypervisor that maintains a first partition and using a virtualization stack within the first partition to create and control a second partition. Multiple virtualization stacks can subsist within the first partition, and each such virtualization stack can create and control multiple partitions. In one particular implementation, a child partition can have exclusive control over a portion or all of its resources with respect to a parent partition. The hypervisor as the ultimate arbiter in such a virtualized environment enforces such a setup and is able to communicate directly within any partition within the virtualized hierarchy.

WO 2007/027739 A1

IPR2025-00069
CrowdStrike EX1002 Page 178

HIERARCHICAL VIRTUALIZATION WITH A MULTI-LEVEL VIRTUALIZATION MECHANISM

TECHINICAL FIELD

[0001] The present disclosure generally relates to the field computing. More specifically, it relates to computer virtualization.

BACKGROUND

[0002] The notion of virtualization entails the virtualizing of computer hardware such that multiple operating systems, each of which may be contained in a separate partition, can run on a single piece of hardware. Virtualizing software abstracts the hardware in various ways such that diverse operating systems interact with the software, and the software in turn interacts with the hardware.

[0003] Most virtualization systems contain a single Virtual Machine Monitor (VMM) software. In some arrangements, this VMM is called a "hypervisor." A hypervisor is designed to run directly on hardware. As such, it is the ultimate arbiter of how the hardware is used. For this reason, in the general case, there can be only one hypervisor on a machine (on one set of hardware). A hypervisor allows multiple "guest" operating systems (OSs) or "guests" for short, to run on a system concurrently.

[0004] A VMM or hypervisor can be designed with certain goals in mind. Engineers must make trade-offs between security, complexity, flexibility, performance, and so on. Some VMMs or hypervisors allow interaction with the guests through a programmatic interface. As with any interface, versioning becomes important. A guest written for one version of a hypervisor may be incompatible with a different version of the hypervisor.

[0005] Thus, there are situations where it would be useful to run multiple copies of a hypervisor on a single machine. One version, for example, could be extremely simple and provide high security guarantees, and another version could provide more complex and intricate features. Such multiple versions could run side-by-side.

[0006] Unfortunately, this is not feasible with today's designs because there can be only one hypervisor on the machine. One traditional approach to this problem is to use recursive virtualization whereby hypervisors are "nested." A single "real" hypervisor sits at the base, and one or more second-level hypervisors run above it. This arrangement has the disadvantage of poor performance. Because the second-level hypervisors were written

IPR2025-00069
CrowdStrike EX1002 Page 179

assuming they have direct access to the hardware, they will not perform as well. In short, with each additional level of nested hypervisors, the performance of the overall virtualized system becomes geometrically worse off.

[0007] Also, many processors provide hardware support for one level of virtualization, but they rarely provide support for more than one. Thus, from a hardware point of view, it becomes difficult to implement multiple hypervisors on a single physical machine. Thus, it would be advantageous to provide mechanisms for running virtualizing software directly on hardware such that multiple versions of the software are running directly on the hardware at the same time.

SUMMARY

[0008] The subject matter disclosed in the present application concerns hierarchical virtualization with a multi-level virtualization mechanism. In one example, a method for providing such virtualization is used, where a first partition is maintained with a hypervisor. A first virtualization stack within the first partition interacts with a second partition, for instance, by creating the second partition in the first place and allocating its resources. The hypervisor in such a hierarchical arrangement of the partitions, where a virtualization stack in one partition controls another partition, is actually aware of each partition and can directly communicate with each partition. Because it can communicate with each partition, the hypervisor can also enumerate any resources within any given partition.

[0009] Furthermore, the second partition can add on to the hierarchical relationship of the partitions by creating a third partition using its own second virtualization stack. Additionally, a third virtualization stack within the first partition can co-exist side-by-side with the first virtualization stack, where this latter third virtualization stack can create a fourth partition that is independent from the previously mentioned first, second, and third partitions. Alternatively, the first virtualization stack can create the fourth partition since a virtualization stack can create and control more than one partition at any given time.

[0010] In another example of the disclosure, security of the hierarchical virtualization is discussed. Thus, a parent partition is provided, and this parent partition has a virtualization stack. A child partition is created by the virtualization stack within the parent partition, however, the child partition is not completely under the control of the parent because it has at least one resource (or portion thereof) exclusively under its own control. For security reasons, a child partition may not trust its parent partition, and if that is the case, certain resources in the child are not attainable by the parent. In order to implement this

IPR2025-00069
CrowdStrike EX1002 Page 180

emancipation of the child from the parent partition, the child partition asks the parent partition for exclusive control of resources and other objects, and the hypervisor, as the ultimate arbiter in this virtualized environment, makes sure the parent partition complies with the child partition's requests.

[0011] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The foregoing Summary, as well as the following Detailed Description, is better understood when read in conjunction with the appended drawings. In order to illustrate the present disclosure, various aspects of the disclosure are shown. However, the disclosure is not limited to the specific aspects discussed. The following figures are included:

[0013] **Figure 1** is a block diagram representing the logical layering of the hardware and software architecture for virtualized operating environment in a computer system;

[0014] **Figure 2A** is a block diagram representing a virtualized computing system wherein the virtualization is performed by the host operating system (either directly or via a hypervisor);

[0015] **Figure 2B** is a block diagram representing an alternative virtualized computing system wherein the virtualization is performed by a virtual machine monitor running side-by-side with a host operating system;

[0016] **Figure 3** illustrates one type of virtualization with nested hypervisors and partitions;

[0017] **Figure 4A** illustrates hierarchical virtualization with a multi-level virtualization mechanism which obviates the need for using nested hypervisors;

[0018] **Figure 4B** provides a bird's eye view of how the microkernelized hypervisor and virtualization stack fit within an exemplary implementation;

[0019] **Figure 4C** illustrates a scenario where a child partition asks a parent partition for exclusive control of its own resources;

[0020] **Figure 5** illustrates the notion that multiple virtualization stacks can reside in one partition;

[0021] **Figure 6** illustrates the arrangement of virtualization stacks and their corresponding partitions in hierarchical fashion;

IPR2025-00069
CrowdStrike EX1002 Page 181

[0022] **Figure** 7 illustrates the relationship between a hypervisor microkernel and a virtualization stack that provides virtualization services for hierarchical virtualization; and

[0023] **Figure 8** shows the various components that make up the virtualization stack and their relationship to each other.

DETAILED DESCRIPTION

Overview

[0024] The description provided below first starts off with a general and brief discussion of virtual machines. Next, it shifts its focus to a discussion of hierarchical virtualization with a multi-level virtualization mechanism. Relevant aspects of hierarchical virtualization are discussed, where one partition maintained by a hypervisor and a virtualization stack contained therein can create and control another partition; or alternatively, it can have more than one virtualization stack that can create and control further partitions. In either case, the hypervisor can directly communicate with each partition in the hierarchy because it is aware of each partition in the first place. Lastly, the mechanism that allows for hierarchical virtualization is discussed piece-by-piece, by first breaking it up into a hypervisor microkernel and a virtualization stack. Each of the elements and components of these two pieces, in turn, is further discussed in more detail.

Virtual Machines

[0025] Figure 1 is a diagram representing the logical layering of the hardware and software architecture for a virtualized environment in a computer system. In the figure, a virtualization program 110 runs directly or indirectly on the physical hardware architecture 112. The virtualization program 110 may be (a) a virtual machine monitor that runs alongside a host operating system or a host operating system with a hypervisor component wherein the hypervisor component performs the virtualization. The virtualization program 110 virtualizes a guest hardware architecture 108 (shown as dashed lines to illustrate the fact that this component is a partition or a "virtual machine"), that is, hardware that does not actually exist but is instead virtualized by the virtualizing program 110. A guest operating system 106 executes on the guest hardware architecture 108, and a software application 104 runs on the guest operating system 106. In the virtualized operating environment of Fig. 1, the software application 104 can run in a computer system 102 even if the software application 104 is designed to run on an operating system that is generally incompatible with a host operating system and the hardware architecture 112.

IPR2025-00069
CrowdStrike EX1002 Page 182

[0026] Figure 2A illustrates a virtualized computing system comprising a host operating system (host OS) software layer 204 running directly above physical computer hardware 202, where the host OS 204 provides access to the resources of the physical computer hardware 202 by exposing interfaces to partitions A 208 and B 210 for the use by operating systems 212 and 214, respectively. This enables the host OS 204 to go unnoticed by operating system layers 212 and 214 running above it. Again, to perform the virtualization, the host OS 204 may be a specially designed operating system with native virtualization capabilities or, alternately, it may be a standard operating system with an incorporated hypervisor component for performing the virtualization (not shown).

[0027] Referring again to Fig. 2A, above the host OS 204 are two partitions, partition A 208, which may be, for example, a virtualized Intel 386 processor, and partition B 210, which may be, for example, a virtualized version of one of the Motorola 680X0 family of processors. Within each partition 208 and 210 are guest operating systems (guest OSs) A 212 and B 214, respectively. Running on top of guest OS A 212 are two applications, application A1 216 and application A2 218, and running on top of guest OS B 214 is application B1 220.

[0028] In regard to Fig. 2A, it is important to note that partition A 208 and partition B 214 (which are shown in dashed lines) are virtualized computer hardware representations that exist only as software constructions. They are made possible due to the execution of specialized virtualization software(s) that not only presents partition A 208 and partition B 210 to Guest OS A 212 and Guest OS B 214, respectively, but which also performs all of the software steps necessary for Guest OS A 212 and Guest OS B 214 to indirectly interact with the real physical computer hardware 202.

[0029] Figure 2B illustrates an alternative virtualized computing system wherein the virtualization is performed by a virtual machine monitor (VMM) 204' running alongside the host operating system 204". In certain cases, the VMM 204' may be an application running above the host operating system 204'' and interacting with the computer hardware 202 only through the host operating system 204''. In other cases, as shown in Fig. 2B, the VMM 204'may instead comprise a partially independent software system that on some levels interacts indirectly with the computer hardware 202 via the host operating system 204'' but on other levels the VMM 204' interacts directly with the computer hardware 202 (similar to the way the host operating system interacts directly with the computer hardware). And yet in other cases, the VMM 204' may comprise a fully independent software system that on all levels interacts directly with the computer hardware 202 (similar to the way the host

IPR2025-00069
CrowdStrike EX1002 Page 183

operating system interacts directly with the computer hardware) without utilizing the host operating system 204'' (although still interacting with the host operating system 204'' in order to coordinate use of the computer hardware 202 and avoid conflicts and the like).

[0030] All of these variations for implementing the above mentioned partitions are just exemplary implementations, and nothing herein should be interpreted as limiting the disclosure to any particular virtualization aspect.

Hierarchical Virtualization with a Multi-Level Virtual Machine Monitor

[0031] Hierarchical virtualization can be accomplished with a multi-level virtualization mechanism in the form of a virtual machine monitor (VMM) or a hypervisor. For example, the functionality provided traditionally through the use of a monlithic hypervisor can be split into a microkernel that runs directly on hardware and a virtualization stack that operates within a partition. This kind of multi-level architecture allows for hierarchical virtualization in that a virtualization stack within a partition can create and control (or "maintain," in short) other partitions, and these partitions can in turn contain other virtualization stacks that can maintain still other partitions. Importantly, this kind of architecture is distinct from a typical "nested" recursive virtualization and improves on the performance thereof.

[0032] Figure 3 illustrates, by way of contrast to hierarchical virtualization with a multi-level virtualization mechanism, recursive virtualization. In recursive virtualization, hypervisors are "nested". A single "real" hypervisor sits at the base, and one or more second-level hypervisors run above it. For example, in Fig. 3, a "real" hypervisor A 301 sits on top of the hardware 300 of a machine. Hypervisors B 302 and C 308 are nested within guest partitions B 314 and C 316, where the guest partitions B 314 and C 316 are maintained by the "real" hypervisor A 301.

[0033] The nested hypervisors B 302 and C 308 can each maintain their own guest partitions. For instance, hypervisor B 302 maintains a guest partition B.1 304 and guest partition B.2 306. Likewise, hypervisor C 308 maintains a guest partition C.1 310 and guest partition C.2 312. Although it is not illustrated so in Fig. 3, it is understood by those skilled in the art, that guest partitions B.1 304, B.2 306, C.1 310 and C.2 312, within guest partitions B 314 and B 316, can host further nested hypervisors. And these further nested hypervisors can maintain further nested partitions, and so on.

[0034] This recursive arrangement, however, has the disadvantage of poor performance. Because the second-level (and all higher level) hypervisors were written

IPR2025-00069
CrowdStrike EX1002 Page 184

assuming they have direct access to the hardware, they will not perform well. Also, many processors provide hardware support for one level of virtualization, but they rarely provide support for more than one. Lastly, in such a nested set-up, no hypervisor is aware of all the partitions nor can it communicate directly (e.g. via hypercalls) with all the partitions. For example, if hypervisor A 301 wants to communicate with guest B.1 304, it must go through hypervisor B 302, which is very inefficient.

[0035] In contrast to Fig. 3, Figs. 4A and 4B illustrate hierarchical virtualization with a multi-level virtualization mechanism which obviates the need for using nested hypervisors. Thus, Fig. 4A depicts a hypervisor with split functionality (operating on multiple levels) vis-à-vis a traditional hypervisor. On the left of Fig. 4A is a traditional hypervisor 405 setup, and on the right is the setup disclosed herein, where a hypervisor is split into a virtualization stack 402 and a hypervisor microkernel 400.

[0036] The microkernel 400 is very small and simple and it interacts with the hardware 403. It only provides the most basic services required to partition a machine's resources. The more complex portions of the hypervisor 401 are "pushed out" to any selected guest partition 405 in the form of a virtualization stack 402. The virtualization stack 402 deals with behavior like device virtualization, paging, partition creation, configuration, and so on.

[0037] Fig. 4B provides a bird's eye view of how the microkernelized hypervisor and virtualization stack fit in a typical virtualization environment. Thus, in one aspect of the present disclosure, the hypervisor microkernel 400 sits directly on top of physical machine hardware 403, and the associated virtualization stack 1 402 of the hypervisor microkernel 400 is pushed out to a parent partition 404. The virtualization stack 402, in turn, is capable of maintaining its own partitions. In Fig. 4B, the virtualization stack 402 maintains child partition A 406 and a child partition B 408.

[0038] Interestingly, from a security point of view, child partitions may actually distrust their parent partitions even though parent partitions typically control child partitions. Because a parent partition by default has control of a child partition, it can manage the resources within a child partition. If malicious software ever infiltrated a parent partition, the child partition would be susceptible to the malicious software. For this reason, in another aspect of the present disclosure, a child partition can ask its parent partition to be emancipated or set free from the control of a parent partition. Such emancipation entails the parent partition relinquishing control over the child partition's resources (such as memory

IPR2025-00069
CrowdStrike EX1002 Page 185

pages) and having the parent partition uninstall any of its intercepts (which may provide the parent partition with information related to content within the child partition).

[0039] Thus, Fig. 4C illustrates a scenario where a child partition A 406 asks 410 a parent partition 404 to be emancipated. A designated component within the virtualization stack processes this request. Typically, what may happen is that the request is made by an operating system (i.e., the kernel of the OS) in the child partition A 406 or some kind of a driver in the child partition A 406, and this request may be made to a boot loader within the parent partition 404. The boot loader may be an enlightened boot loader (i.e., a boot loader aware of virtualization). In this way, the parent partition 404 may close the door on any tampering with the child partition A 406, since when the child partition A 406 becomes emancipated it cannot be hacked via the parent partition 404.

[0040] The hypervisor 400 actually enforces 412 this request, since it is the ultimate arbiter in any virtualized system. In Fig. 4C, by way of example, a portion of the memory of the child partition A 406 is not accessible 414 by the parent partition 404. Thus, the parent partition 404 cannot access the resources of the child partition A 406. Yet, the parent partition 404 may have access 416 to other portions of the child partition A 406.

[0041] In the same vein, the entire child partition B 408 is not accessible 414 by the parent partition 404, and therefore the parent partition 404 is fully distrusted, thereby making the child partition B 408 very secure. This means that the parent partition 404 cannot know anything about the child partition B 408. Interestingly enough, in some aspects of the present disclosure, the parent partition 404 despite it's limited (or non-existent) control over a fully emancipated partition, such as partition B 408, still has the ability as a parent partition 404 to terminate the child partition B 408 if the child partition behaves in an inappropriate or unexpected manner.

[0042] In yet another aspect of the present disclosure, Fig. 5 illustrates the notion that multiple virtualization stacks can reside in one partition. For example, a first virtualization stack 1 502 can reside in a parent partition 508 alongside a second virtualization stack 2 503. The first virtualization stack 1 502 is capable of maintaining multiple child partitions (with respect to the parent partition that it is residing in). Thus, virtualization stack 1 502 maintains child partition 1A 504 and child partition 1B 506. Likewise, virtualization stack 2 503 maintains child partition 2A 505 and child partition 2B. Although only two virtualization stacks are illustrated, any number of virtualization stacks can reside in a given partition, and each of these virtualization stacks can maintain any given number of child partitions.

IPR2025-00069
CrowdStrike EX1002 Page 186

[0043] One reason for having multiple virtualization stacks alongside each other in one partition is that, for example, one virtualization stack 502 could specialize in supporting stripped-down secure partitions while another virtualization stack 503 could specialize in providing full-blown support of all kinds of resources. Naturally, the former virtualization stack 502 would be a lot more secure (and hence so would its partitions) because it would be proportionately less complex than the latter virtualization stack 503. Security and complexity would be trade-offs in this context. Thus, for instance, the latter virtualization stack 503 could provide IDE (Integrated Device Electronics) and SCSI (Small Computer System Interface) support, while the former stripped-down version 502 would not.

[0044] In yet another aspect of the disclosure, as is illustrated in Fig. 6, the aforementioned virtualization stacks and their corresponding partitions can be arranged in a hierarchical fashion. Thus, a hypervisor microkernel 600 maintains a parent partition 608, and the corresponding virtualization stack 1 602 to the hypervisor microkernel 600 is located in the parent partition 608. This virtualization stack 1 602 maintain a first child partition 1A 604 and a second child partition 1B 606. A second virtualization stack 2 610 resides in the second child partition 1B 606, and this virtualization stack 2 610 maintain two other child partitions (or grand child partitions with respect to the original partition 608): child partition 2A 605 and child partition 2B 607.

[0045] Although it is not so illustrated in Fig. 6, it is understood that each of the child partitions 605 and 607 maintained by the second virtualization stack 2 610 could in turn maintain one or more tertiary virtualization stacks, and these stacks in turn could maintain further child partitions. In short, Fig. 6 attempts to illustrate the notion that the hypervisor microkernel-cum-virtualization stack architecture allows for hierarchical virtualization. Partitions can hold multiple virtualization stacks and such virtualization stacks can maintain multiple partitions, and such multiple partitions can maintain further virtualization stacks, and so on.

[0046] One benefit of this type of hierarchical arrangement is that it supports multi-level administration of large machines. For example, a "machine administrator" can control the virtualization stack within a "root partition" (i.e. the top-most parent partition). This administrator can then create sub-partitions that have virtualization stacks of their own and assign each of these a set of machine resources (memory, processors, NICs, disk drives, and so on). This administrator can then allow other administrators (e.g. team-level administrators) to further partition the resources they were assigned. In such a scenario, the second-level virtualization stack is constrained to use the resources provided by the first-level

IPR2025-00069
CrowdStrike EX1002 Page 187

(i.e. root-level) virtualization stack, but then those assigned resources can be used in any way fit. A virtual machine management system that knows about the hierarchy can present it as such, allowing an administrator at each level to reallocate resources among the partitions they control.

[0047] This kind of hierarchical scenario should be distinguished from the nested scenario discussed with reference to Fig. 3. Unlike in the nested case that has multiple hypervisors running in nested partitions, where each hypervisor is not aware of base partitions (below it) or derivative partitions (above it), in the hierarchical scenario there is a single hypervisor that is aware of all the partitions. In this case, the multiple virtualization stacks allow for the creation of various hierarchical relationships between partitions. Interestingly, unlike anything that came before, the present hypervisor can directly communicate (i.e. obviating the need to go through any other hypervisors or virtualization software) with any partition even when such partitions are maintained in a hierarchical relationship by the various corresponding virtualization stacks. Such direct communication can be accomplished through direct hypercalls from the hypervisor to any given partition.

Microkernelized Hypervisor and Virtualization Services

[0048] As mentioned above, hierarchical virtualization is supported by the microkernelized hypervisor-cum-virtualization stack architecture. Figure 7 focuses on hypervisor components which includes the hypervisor microkernel 702 and virtualization services 704 within the hypervisor (Fig. 8, below, focuses on the virtualization stack architecture).

[0049] With specific reference to Fig. 7, in the microkernel 702, the bottom-most layer is the hardware abstraction layer 706 and it is responsible for abstracting platform-specific aspects of the microkernel 702. Other modules within this layer and the layer discussed below may be employed, as those skilled in the art will readily appreciate. These layers and modules therein are merely exemplary, presented here for the sake of discussion – they are not limiting or dispositive in any way.

[0050] On top of this layer is the memory management layer 710. This layer has a memory manager module that provides primitive internal memory management for the hypervisor 700 and a resource manager module that stores the resource policies for a given CPU and memory usage. Higher-level components are responsible for enforcing these policies.

IPR2025-00069
CrowdStrike EX1002 Page 188

[0051] Finally, the third kernel layer 712 contains at least four exemplary modules: First, a security access manager module manages access right for partitions and resources that can be shared or moved between partitions; second, a thread manager manages threads internal to the hypervisor 700; third, a timer manager manages timer queues and timer interrupts; and fourth, a scheduler implements the hypervisor's 700 scheduler.

[0052] Similarly, in the virtualization services 704, four layers may also be used. The first layer is the virtualization abstraction layer 714 and it contains a virtualization abstraction layer module that abstracts the virtualization extensions provided by a processor.

[0053] Next, a partition layer 716 contains at least three of the following modules: a partition manager module that manages partition objects and related data structures; a virtual manager processor module that manages one or more virtual processors associated with each partition—in this setup, each virtual processor has its own processor state and runs on its own hypervisor stack; and a synthetic interrupt controller that implements an interrupt controller similar to an x86 advanced programmable interrupt controller.

[0054] The next layer concerns the address space. This layer can have an address manager module that manages the definition of a guest's physical address space and its mapping to underlying physical memory resources. Of course, other modules may be used that help to manipulate address space mechanisms and this is just an exemplary module.

[0055] Lastly, the virtualization services 704 contains four modules: first, a dispatch manager handles incoming events and dispatches them accordingly; second, a hypercall manager module dispatches hypervisor calls from a guest; third, an intercept manager module handles the dispatching and routing of intercepts (e.g. accesses to model-specific registers, execution of certain instructions, and so on); and fourth, an instruction completion module handles completion of certain instructions during virtualization.

Virtualization Stack Components

[0056] In another aspect of the disclosure, Fig. 8 shows the various components that make up the virtualization stack and their relationship to each other. Any related components not disclosed herein can be examined in a related application titled: "SYSTEMS AND METHODS FOR MULTI-LEVEL INTERCEPT PROCESSING IN A VIRTUAL MACHINE ENVIRONMENT," Serial No. 11/078,141, filed March 11, 2005. The "external monitor" disclosed in this latter application is a sub-component of the virtualization stack discussed in the present application.

IPR2025-00069
CrowdStrike EX1002 Page 189

[0057] A given virtualization stack 800 can be implemented in user mode 802 and kernel mode 804. Furthermore, the kernel mode 804 can have components such as a hypervisor API and hypervisor message handler library 806 and a virtualization infrastructure driver 810. The user-mode 802 can have components such as a virtual machine service 812 and a virtual machine worker process 814.

[0058] Each of these components may have a specifically defined task. For example, the hypervisor API library 806 exposes the hypervisor API to higher-level components, allowing them to call the hypervisor using normal operating system calling conventions. This library can be found in all partitions that contain enlightened code (i.e. code aware of virtualization) – whether or not they host a virtualization stack. Moreover, the hypervisor message handler library 806 allows callers to register kernel-level call-backs for messages received from the hypervisor or from other partitions. Such messages are delivered as inter-partition interrupts with message payloads. This interface allows a single partition to host multiple parallel virtualization stacks. For example, a third party could implement a virtualization stack that resides in the same parent partition as the original-party virtualization stack. Or multiple versions of the original-party virtualization stack could run side by side.

[0059] Next, the Virtualization Infrastructure Driver (VID) 810 encapsulates the bulk of the virtualization stack's kernel-mode functionality. It contains several subcomponents. For example, it contains the Virtualization Stack Memory Manager. This subcomponent is responsible for managing a pool of system physical pages that are "owned" by the virtualization stack and used to back the guest physical memory of the child partitions managed by that virtualization stack. This sub-component supports memory over-commit and cross-partition page sharing (for pages with identical contents). It also exposes a set of interfaces that allow user-mode components to define the layout of a virtual machine's guest physical address (GPA) space and to place read & write intercepts on page ranges (e.g. for use during snapshotting or live migration).

[0060] Furthermore, the VID 810 also contains Complex Instruction Completion. This subcomponent is able to perform the interpretation of complex instructions that touch memory and are not handled directly by the hypervisor. This support is required for certain device emulation scenarios (e.g. accesses to planar VGA memory, writes to ROM, or accesses to memory-mapped registers of an emulated device).

[0061] The VID 810 also contains Processor Intercepts. This subcomponent allows user-mode components to specify virtual processor intercepts. For example, an emulated device module may want to receive an intercept notification when a particular I/O port range

IPR2025-00069
CrowdStrike EX1002 Page 190

is accessed via an IN or OUT instruction. Other examples of processor intercepts include: MSR access, CPUID, exceptions, and HLT. This component tracks the installed intercepts and routes the intercept notification as appropriate.

[0062] Lastly, the VID 810 may contain Partition Creation & Control subcomponent. This subcomponent allows user-level components to create, delete, and manage partitions and specify partition-wide resources and quotas, defining scheduling and access control policies. For example, the creation of a new partition might be implemented by first making a hypercall to a module within the hypervisor (e.g. HvCreatePartition). Next, one or more virtual processors are created by invoking a hypercall HvCreateVp. Memory is assigned to the guest physical address space of the newly-created partition by invoking another hypercall, e.g. HvMapGpaPages. Intercepts are requested for certain processor action by invoking the hypercall HvInstallIntercept. Various scheduling and security policies are set by invoking the hypercall HvSetPartitionProperty. Initialization code (e.g. an OS loader or a system BIOS) is copied into the memory of the newly-created virtual machine. Execution within the virtual machine begins when a hypercall HvResumePartition is invoked. These hypercalls are merely exemplary and those skilled in the art would appreciate that other and equivalent methods could be implemented to achieve partition creation. Likewise, methods concerning partition deletion (removing virtual processors, guest physical addresses, etc.) are readily appreciated by those skilled in the art, as are methods for managing partition resources.

[0063] As mentioned above, the VID 810 and HV API 806 subsist in kernel mode 804. However, other components of the virtualization stack 800 subsist in user mode 802. For example, Virtual Machine Management Service 812 manages a set of VM configurations and exposes a set of WMI-based APIs for managing and controlling VMs. It is responsible for spawning a new VM worker process when a virtual machine is started. This service can be restartable without affecting any of the VM worker processes (making the system more resilient if the service crashes).

[0064] Another user-mode 802 component is the Virtual Machine Worker Process 814. Each virtual machine has an associated worker process. If a component within the worker process crashes, the damage can be contained to a single virtual machine. In the Worker Process 814 there is a Virtualized Device Framework. A virtual machine is composed of a set of virtual devices. Each device has its own settings and parameters, many of which can be adjusted by the user. The device framework is responsible for instantiating virtual device modules and "wiring up" these devices to form a functional virtual machine.

IPR2025-00069
CrowdStrike EX1002 Page 191

The devices that make up a virtual machine are defined in a device manifest, part of the VM's configuration file.

[0065] Within the aforementioned framework, is the Virtual Device Modules (VDEVs): These plug-in modules contain the logic required to instantiate, initialize, save, restore, reset, and tear down a virtual device. Some virtual devices implement the full emulation of legacy hardware devices. These virtual devices are referred to as emulated device modules and make use of I/O and memory intercepts to respond to guest accesses.

[0066] Within the worker process 814 there may also resides a Virtual Machine Creator. This component is responsible for creating and managing a running virtual machine. It handles VM-wide policies, responds to dynamic resource change requests, and is responsible for pausing & resuming, saving & restoring, snapshotting, and live migration of the VM.

[0067] While the present disclosure has been described in connection with the preferred aspects, as illustrated in the various figures, it is understood that other similar aspects may be used or modifications and additions may be made to the described aspects for performing the same function of the present disclosure without deviating therefrom. For example, in one aspect of the disclosure, hierarchical virtualization was discussed that was made possible by using a multi-level virtualization mechanism. However, other equivalent mechanisms to these described aspects are also contemplated by the teachings herein. Therefore, the present disclosure should not be limited to any single aspect, but rather construed in breadth and scope in accordance with the appended claims.

IPR2025-00069
CrowdStrike EX1002 Page 192

What is Claimed:

1. A method for providing hierarchical virtualization, comprising:

maintaining a first partition 608 with a hypervisor 600; and

interacting with a second partition 606 using a first virtualization stack 602 within the first partition 608, wherein the hypervisor 600 is aware of the first partition 608 and the second partition 606.

2. The method according to claim 1, wherein the hypervisor 400 is further aware of at least one resource 416 within the first partition 406 and the second partition 414, and wherein the hypervisor 400 is configured to enumerate the at least one resource 416 upon a request.

3. The method according to claim 1, wherein the second partition 606 communicates directly with the hypervisor 600.

4. The method according to claim 1, wherein the first virtualization stack 602 creates the second partition 606.

5. The method according to claim 4, wherein the second partition 606 contains a second virtualization 610 stack that is configured to create and interact with a third partition 605.

6. The method according to claim 1, wherein the first partition 508 contains the first virtualization stack 502 and also contains a second virtualization stack 503, wherein the first virtualization stack 502 and the second virtualization 503 stack are contained in the first partition 508 simultaneously at least for a given period of time.

7. The method according to claim 1, wherein the first virtualization stack 508 creates the second partition 504 and a third partition 506.

8. A method for providing secured hierarchical virtualization, comprising:

providing a parent partition 404, wherein the parent partition 404 has a virtualization stack 402; and

providing a child partition 406, wherein the child partition 406 is created by the

IPR2025-00069
CrowdStrike EX1002 Page 193

virtualization stack 402 within the parent partition 404, and wherein the child partition 406 has at least a resource 414 that is exclusively controlled by the child partition 406.

9. The method according to claim 8, wherein the resource 414 includes at least one memory page.

10. The method according to claim 8, wherein the child partition 406 obtains exclusive control of the resource 414 by making a request 410 to the parent partition 404.

11. The method according to claim 10, wherein a hypervisor 400 validates 412 that the parent partition 404 has complied with the request 410 made by the child partition 406.

12. The method according to claim 10, wherein the request 410 made by the child partition 406 is made by an operating system kernel within the child partition 406.

13. The method according to claim 10, wherein the request 410 made by the child partition 406 is made by a driver within the child partition 406.

14. The method according to claim 10, wherein the request 410 made by the child partition 406 is made to a boot loader within the parent partition 404.

15. A computer readable medium bearing computer executable instructions providing hierarchical virtualization, comprising:

using a first partition 608 to create a second partition 604, wherein the second partition 604 is created by a virtualization stack 602 in the first partition 608; and

providing a microkeralized hypervisor 600 configured to interact directly with the first partition 608 and the second partition 604;

16. The computer readable medium according to claim 15, wherein the virtualization stack 602 in the first partition 608 further creates a third partition 606.

17. The computer readable medium according to claim 15, further comprising a second virtualization stack 503 located in the first partition 508, wherein the second virtualization stack 503 creates a third partition 505.

IPR2025-00069
CrowdStrike EX1002 Page 194

18. The computer readable medium according to claim 15, wherein the second partition 606 has its own virtualization stack 610.

19. The computer readable medium according to claim 18, wherein the virtualization stack 610 in the second partition 606 creates a third partition 605.

20. The computer readable medium according to claim 18, wherein the virtualization stack 602 in the first partition 608 and a virtualization stack 610 in the second partition 606 coexist substantially at least for a given period of time.

IPR2025-00069
CrowdStrike EX1002 Page 195

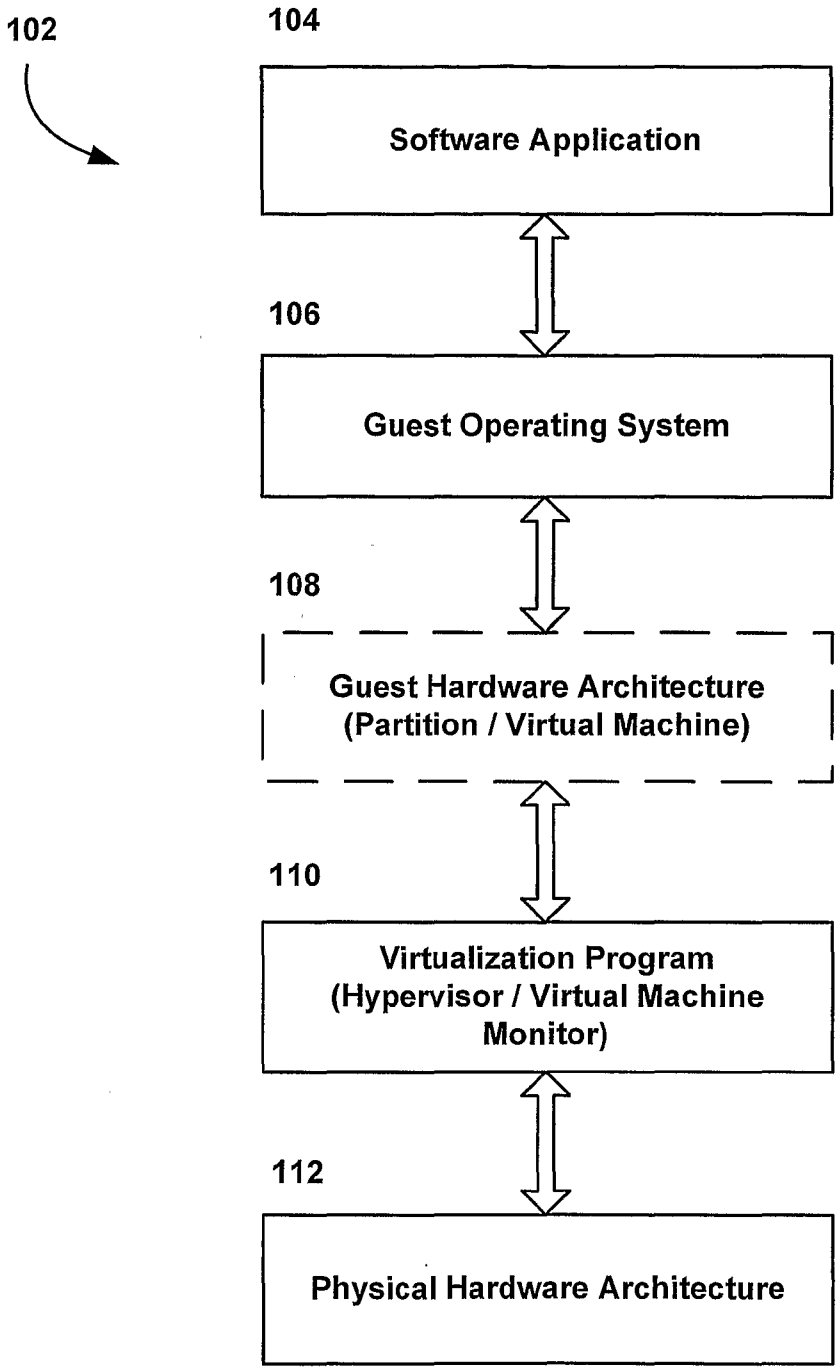

102
104
Software Application
106
Guest Operating System
108
Guest Hardware Architecture
(Partition / Virtual Machine)
110
Virtualization Program
(Hypervisor / Virtual Machine
Monitor)
112
Physical Hardware Architecture

Fig. 1

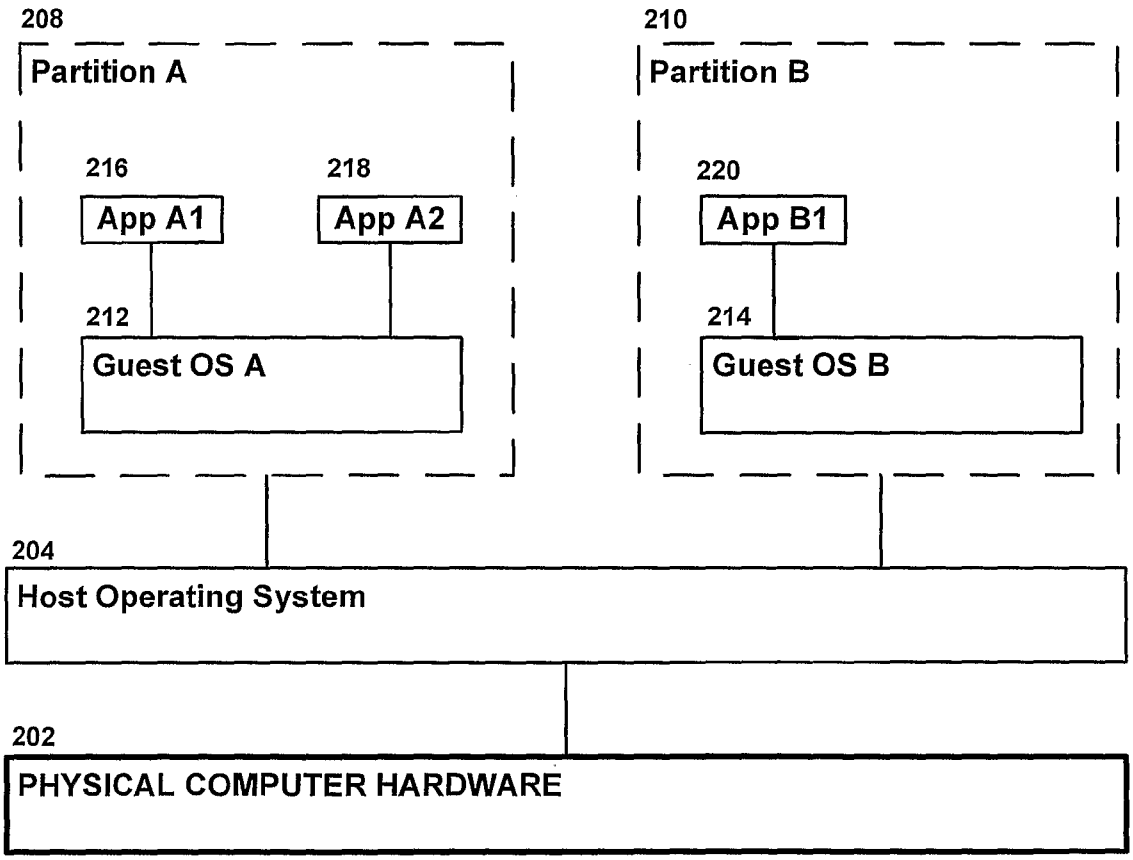

208
Partition A
216
App A1
218
App A2
212
Guest OS A
210
Partition B
220
App B1
214
Guest OS B
204
Host Operating System
202
PHYSICAL COMPUTER HARDWARE

Fig. 2A

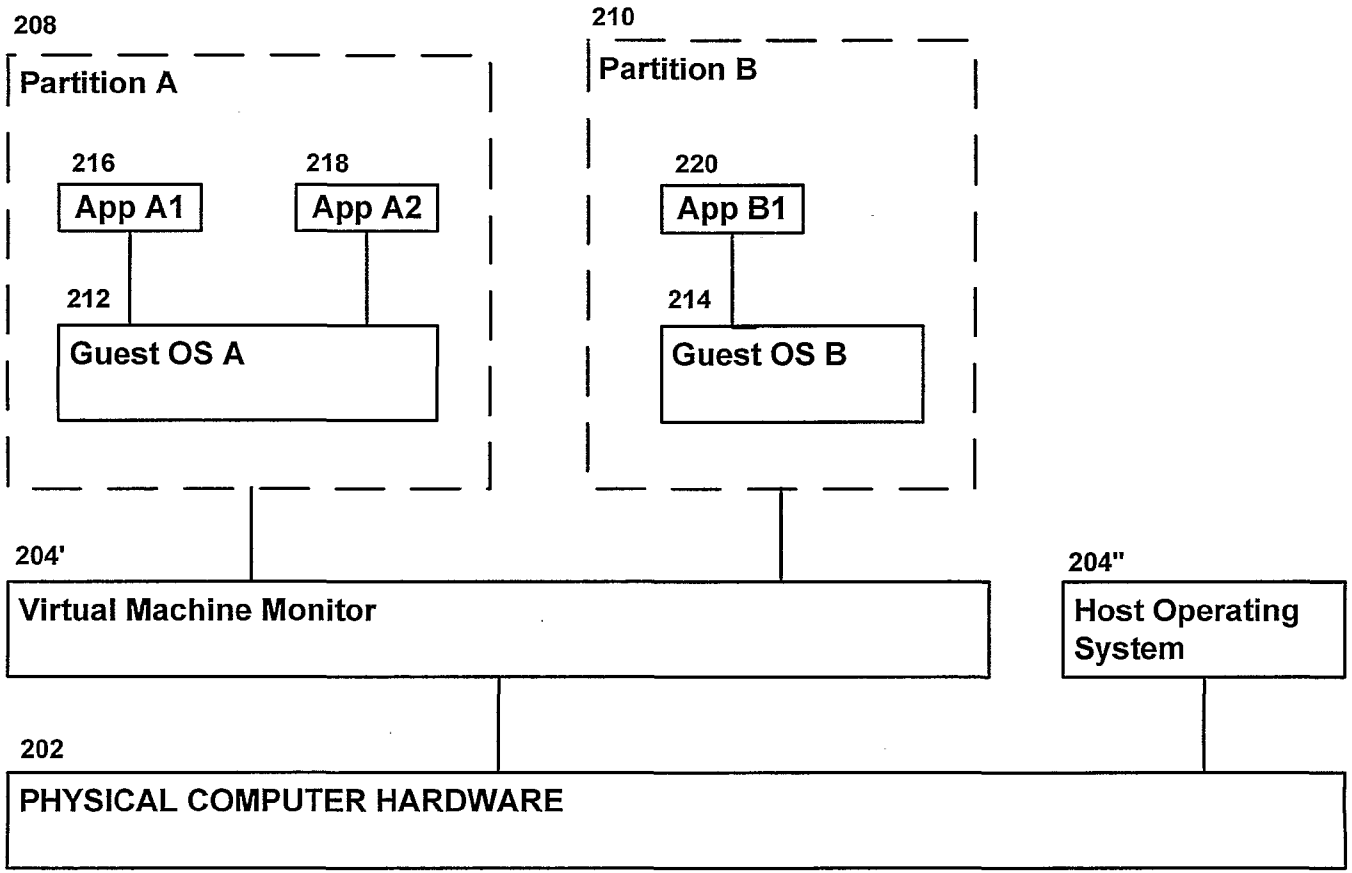


Fig. 2B

IPR2025-00069
CrowdStrike EX1002 Page 198

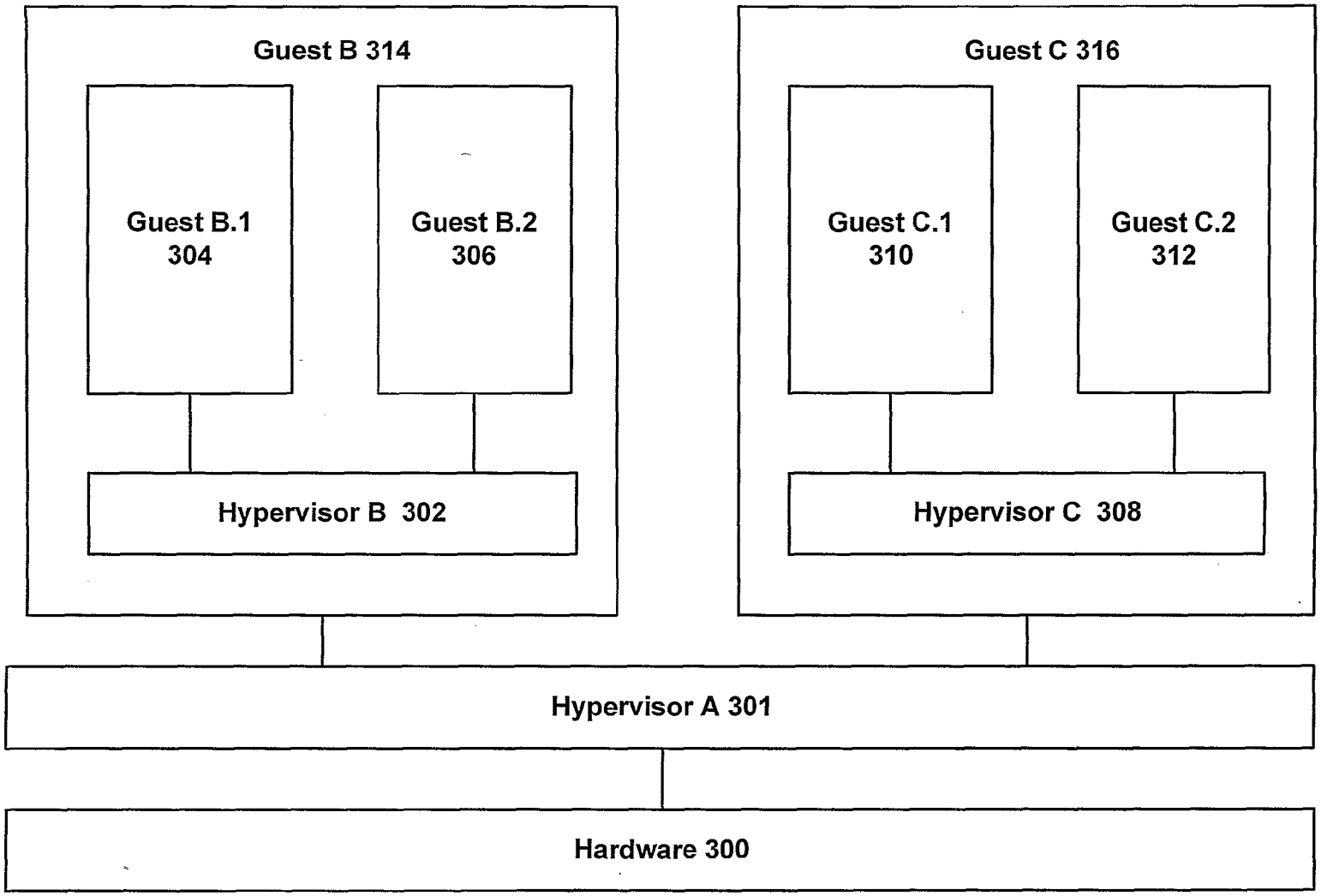

Guest B 314
Guest B.1
304
Guest B.2
306
Guest C 316
Guest C.1
310
Guest C.2
312
Hypervisor B 302
Hypervisor C 308
Hypervisor A 301
Hardware 300

Fig. 3

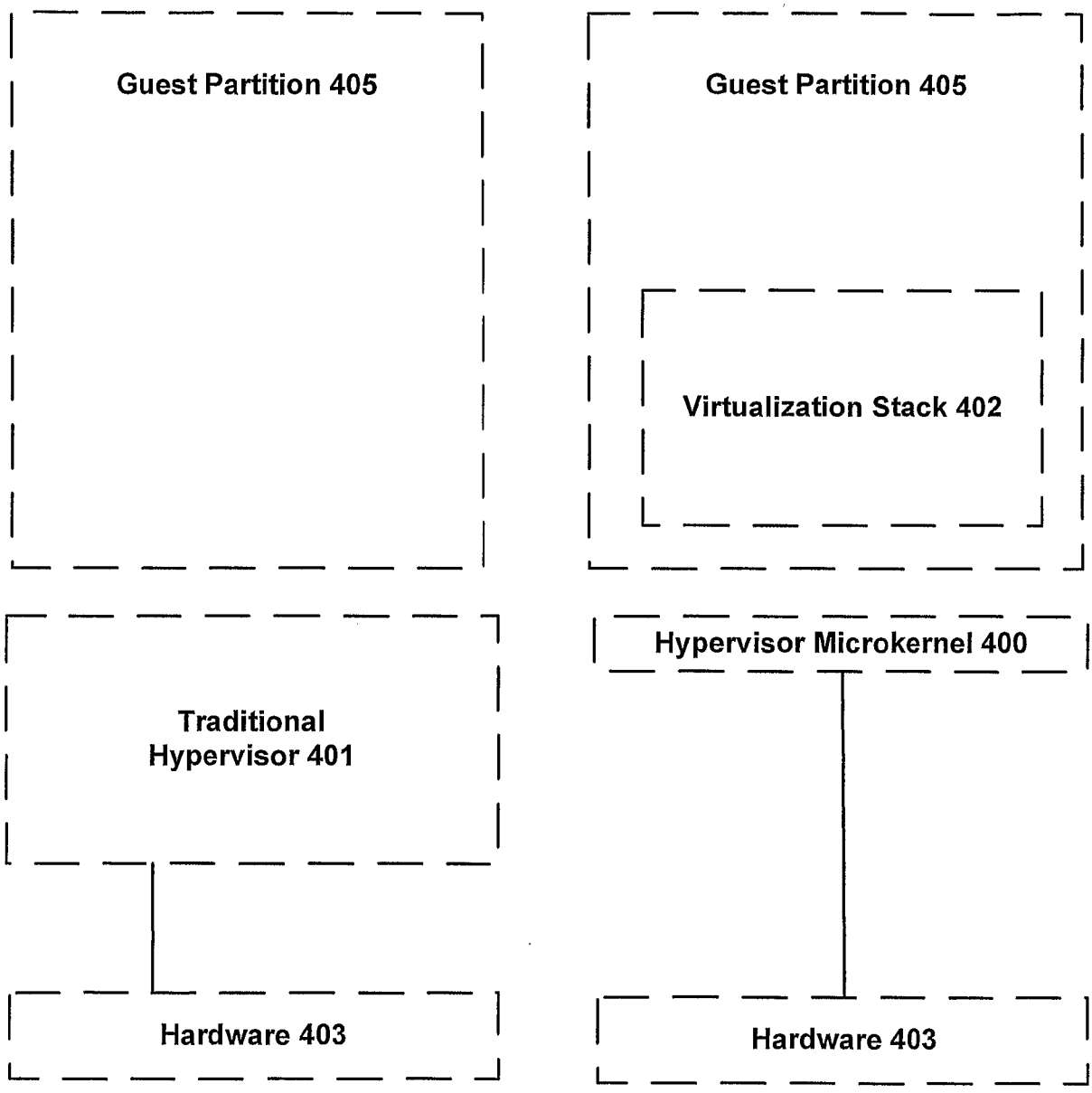

Guest Partition 405
Guest Partition 405
Virtualization Stack 402
Traditional Hypervisor 401
Hypervisor Microkernel 400
Hardware 403
Hardware 403

Fig. 4A

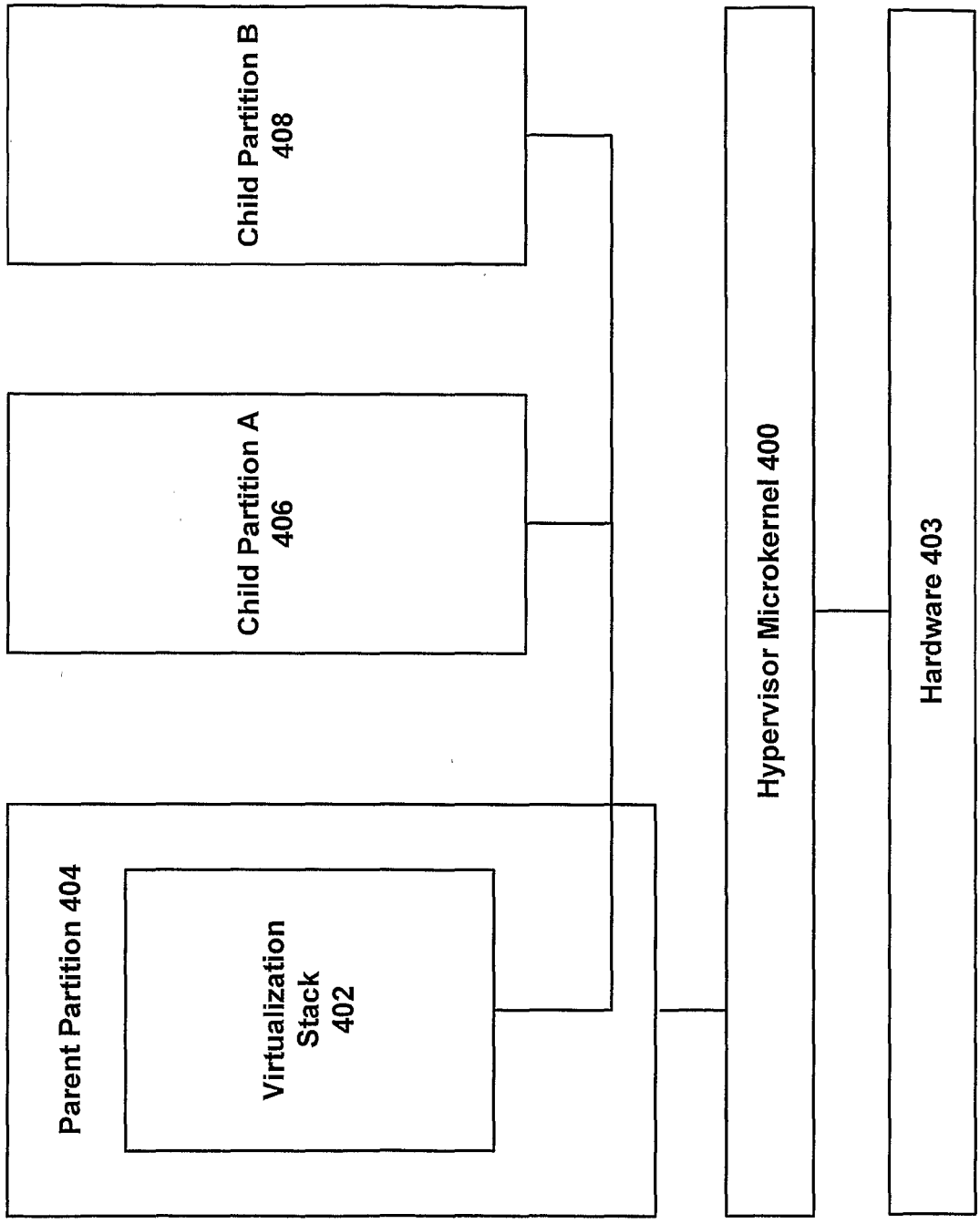


Fig. 4B

IPR2025-00069
CrowdStrike EX1002 Page 201

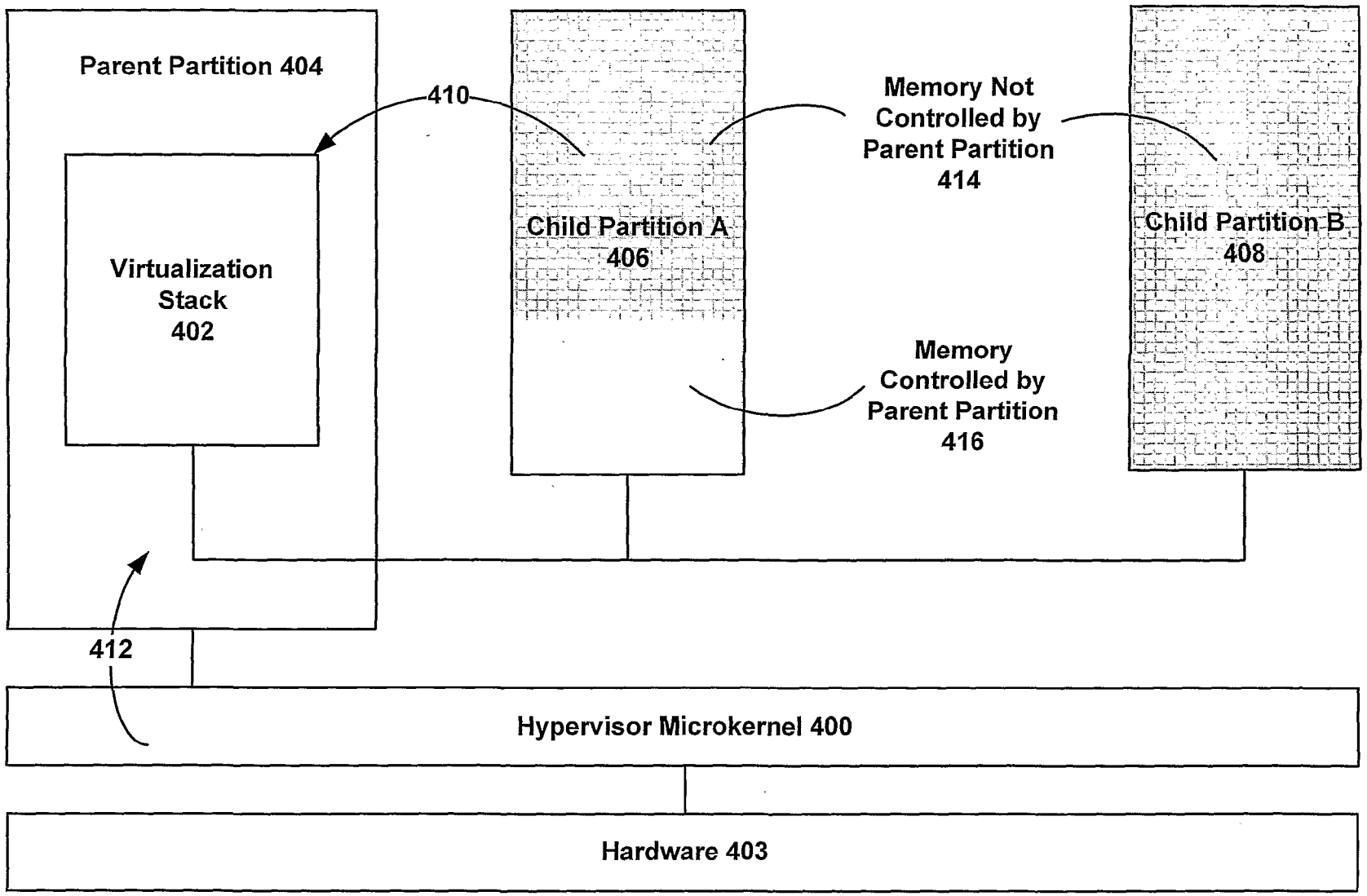


Fig. 4C

IPR2025-00069
CrowdStrike EX1002 Page 202

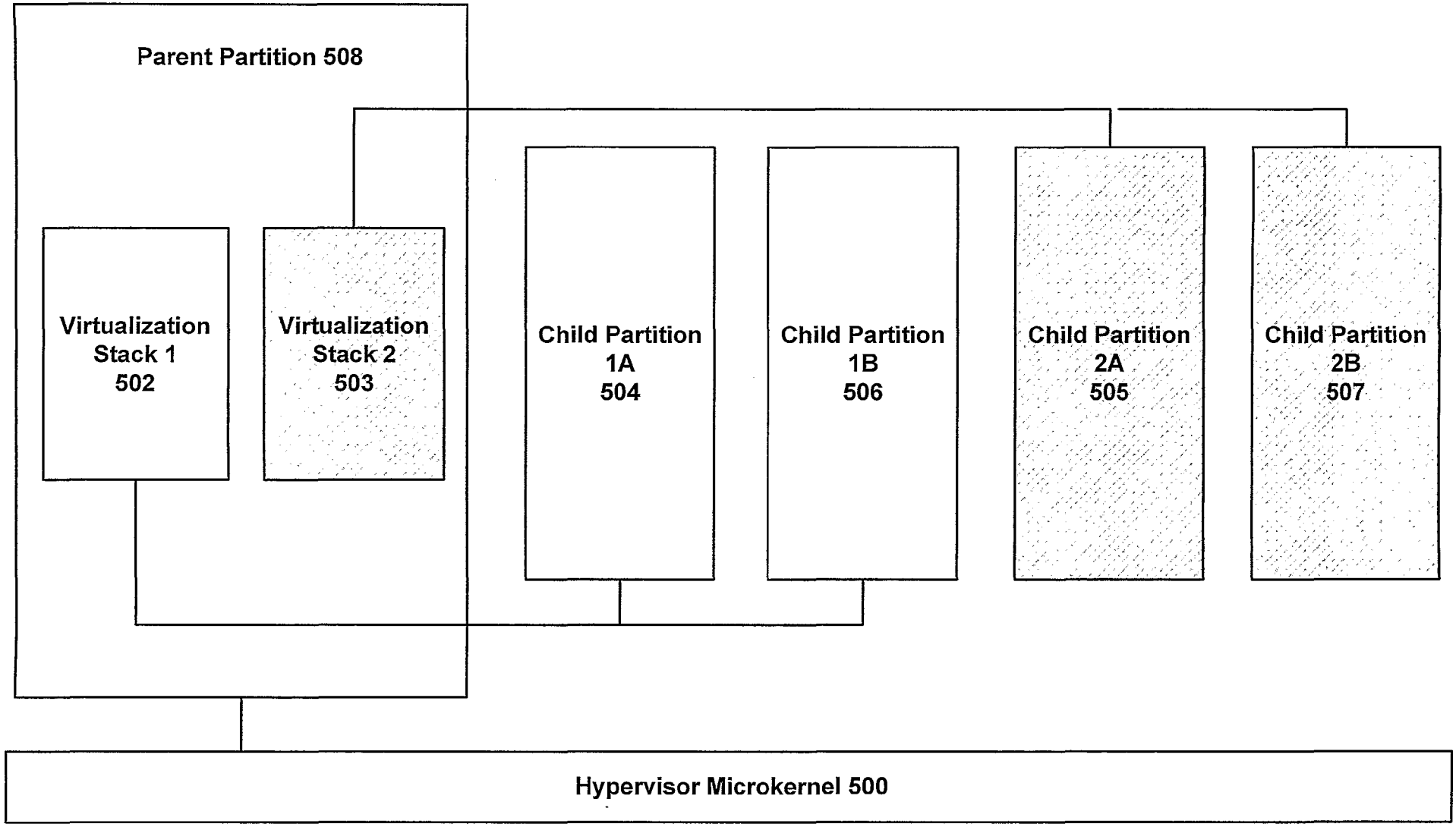

Parent Partition 508
Virtualization Stack 1 502
Virtualization Stack 2 503
Child Partition 1A 504
Child Partition 1B 506
Child Partition 2A 505
Child Partition 2B 507
Hypervisor Microkernel 500

Fig. 5

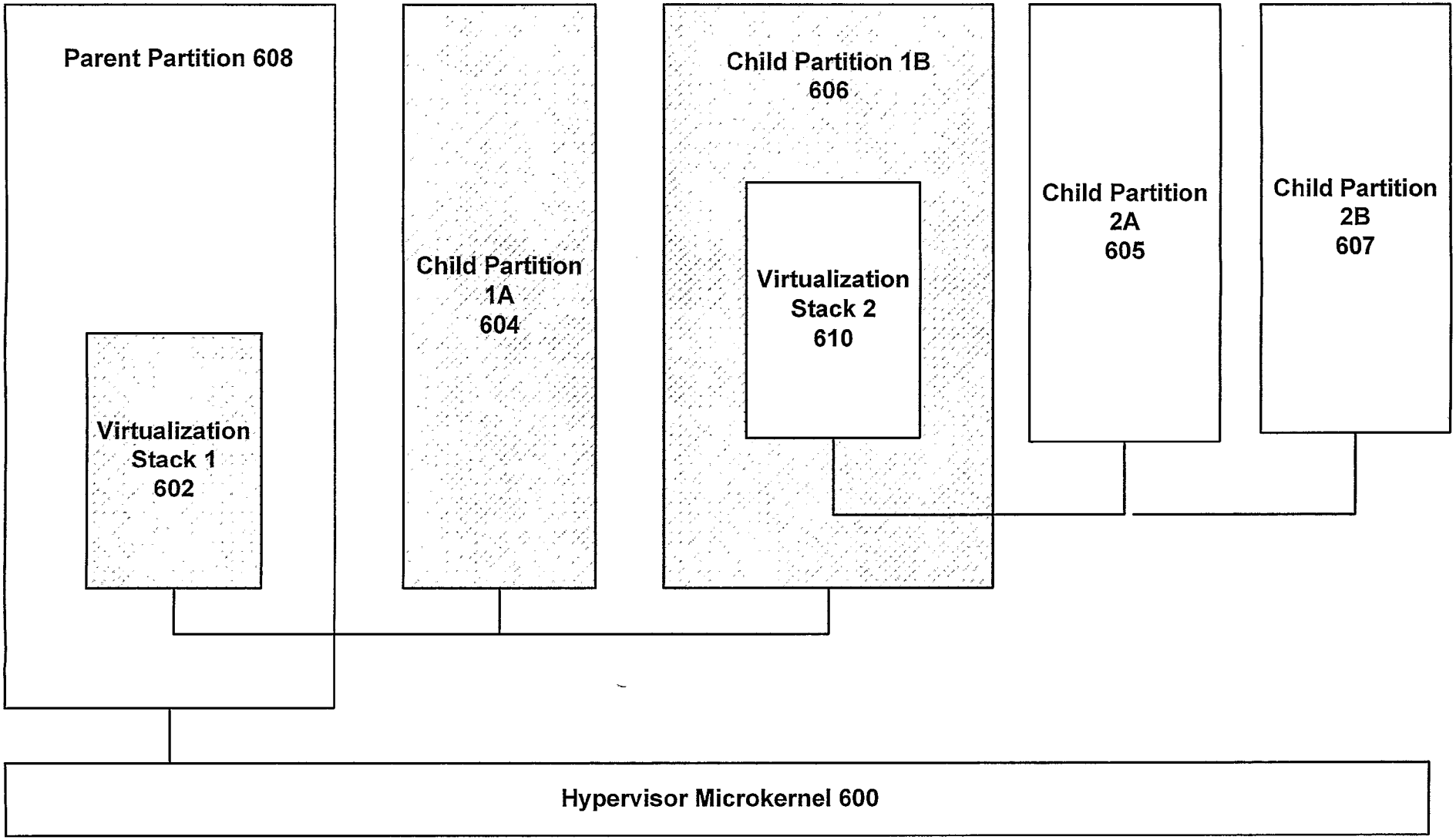

Parent Partition 608
Virtualization Stack 1 602
Child Partition 1A 604
Child Partition 1B 606
Virtualization Stack 2 610
Child Partition 2A 605
Child Partition 2B 607
Hypervisor Microkernel 600

Fig. 6

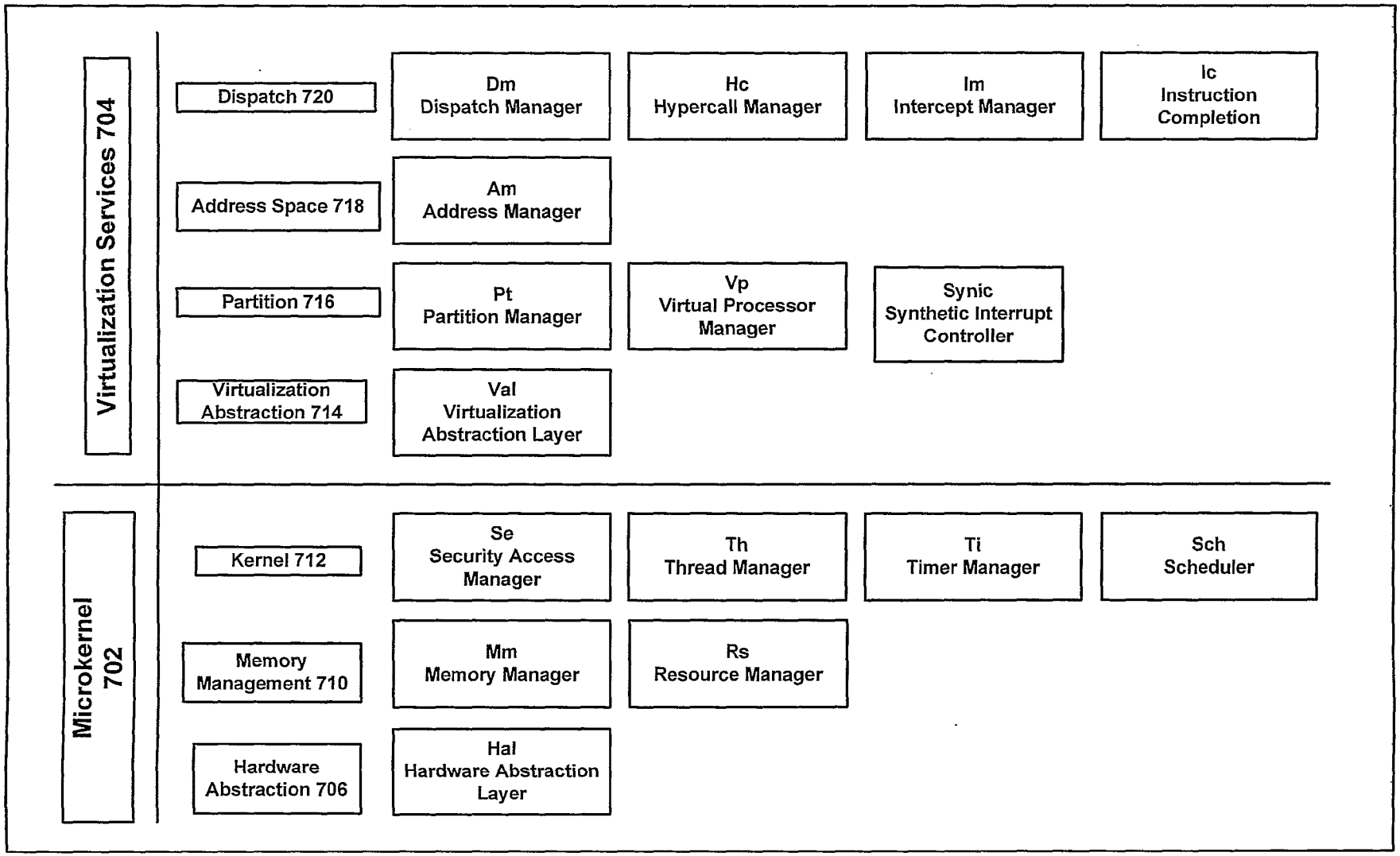


Fig. 7

IPR2025-00069
CrowdStrike EX1002 Page 205

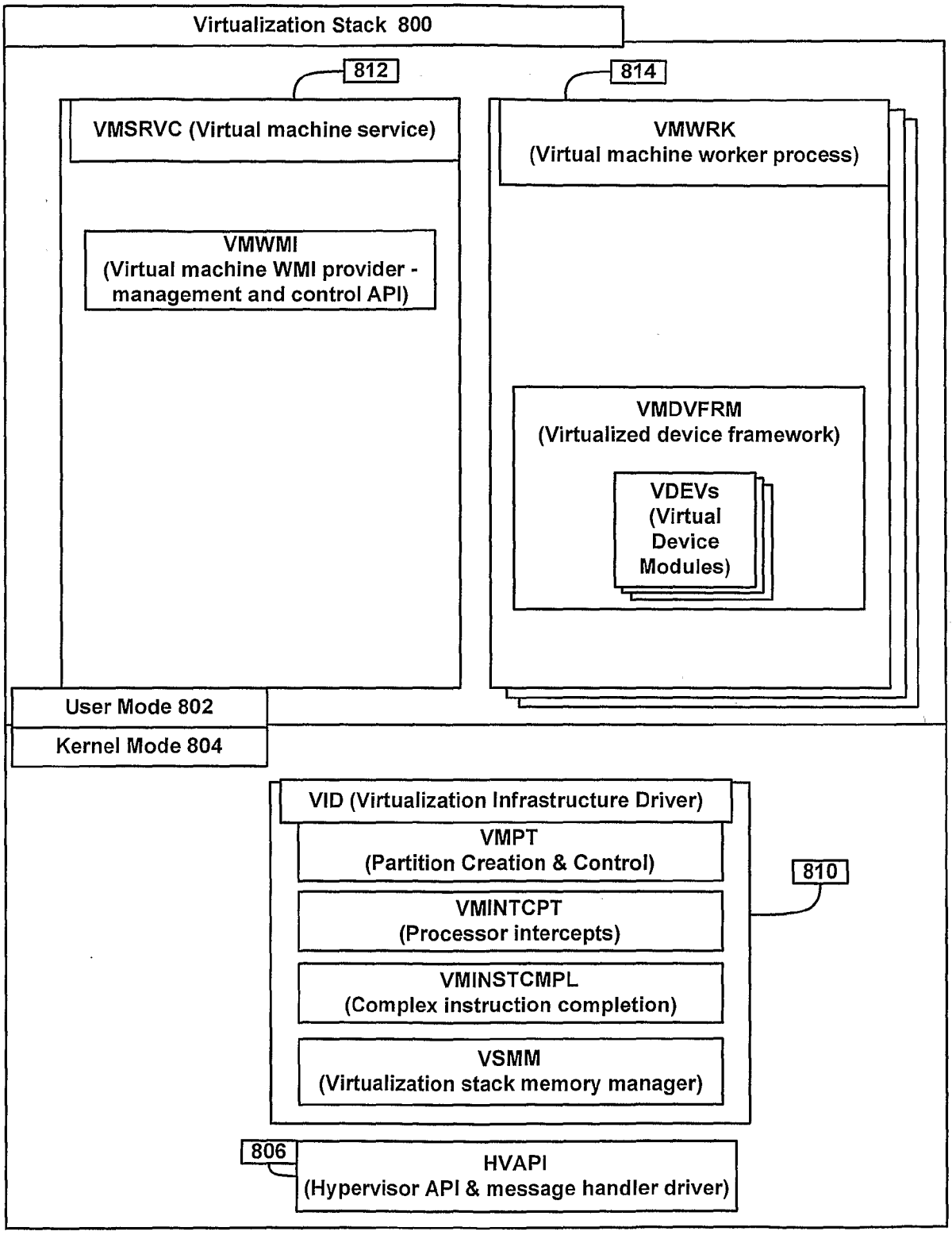

Virtualization Stack 800
812
VMSRVC (Virtual machine service)
VMWMI
(Virtual machine WMI provider - management and control API)
814
VMWRK
(Virtual machine worker process)
VMDVFRM
(Virtualized device framework)
VDEVs
(Virtual Device Modules)
User Mode 802
Kernel Mode 804
VID (Virtualization Infrastructure Driver)
VMPT
(Partition Creation & Control)
VMINTCPT
(Processor intercepts)
VMINSTCMPL
(Complex instruction completion)
VSMM
(Virtualization stack memory manager)
810
806
HVAPI
(Hypervisor API & message handler driver)

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2006/033815

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/455(2006.01)i, G06F 9/06(2006.01)i, G06F 9/00(2006.01)i, G06F 12/00(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 8 : G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

KR, JP IPC as above

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search terms used)

eKIPASS (KIPO internal) "hierarchical", "virtualization", "partition", "hypervisor"

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US6633916 B2 (Hewlett-Packard Development Company) 14 Oct. 2003 See the abstract; claims 1-22; figure3	1-20
Y	US6934888 B2 (International Business Machines Corporation) 23 Aug. 2005 See the abstract; claims 1-22; figure2	1-20
A	US2004/0205272 A1 (International Business Machines Corporation) 14 Oct. 2004 See the abstract; claims 1-25; figure2	1-20

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 JANUARY 2007 (12.01.2007)	**12 JANUARY 2007 (12.01.2007)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office 920 Dunsan-dong, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	JEONG, Hae Kon Telephone No. 82-42-481-5986

IPR2025-00069
CrowdStrike EX1002 Page 207

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/US2006/033815

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US06633916 B2	14.10.2003	EP00917056A2	19.05.1999
		EP00917056A3	09.08.2000
		JP2000132530A2	12.05.2000
		US20020032850A1	14.03.2002
US06934888 B2	23.08.2005	US2003172323A1	11.09.2003
US20040205272A1	14.10.2004	JP2004303237A2	28.10.2004
		KR2004086167A	08.10.2004
		US7000051BB	14.02.2006

IPR2025-00069
CrowdStrike EX1002 Page 208

Electronic Acknowledgement Receipt

EFS ID:	16165191
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Lamesha Robertson
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	26-JUN-2013
Filing Date:	17-JUN-2011
Time Stamp:	19:20:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292_5005US_IDS.pdf	239310 f44d83acccd8d91d8dac458dafc2543bbfacdc89	yes	5

	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
2	Foreign Reference	Intelligent_Cosmos_JP_2005_316779.pdf	1294621 e1d094dcba048eacaa2d9a406f5418279bfa422d	no	24
Warnings:					
Information:					
3	Foreign Reference	Microsoft_WO_2007_027739.pdf	1301986 56b3faf73f0cd9290c4af71a80b06dd474b7a904	no	31
Warnings:					
Information:					
4	Non Patent Literature	Capalik_OA_13_759_335_14_June_2013.pdf	1131937 2f0a2797d03ee65bd9fbe1b9b72f7a4eb903b833	no	32
Warnings:					
Information:					
5	Non Patent Literature	NeuralIQ_Notice_of_Reasons_JP_2010_504185_15_March_2013.pdf	151233 7553f9c7acd8b0e5a7cea5d1a99d49739b398119	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	4119087		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed June 26, 2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☒ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

IPR2025-00069
CrowdStrike EX1002 Page 212

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☒ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application

not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: June 26, 2013

45,645
Dion M. Bregman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

24341 7590 10/25/2013

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
10/25/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Office Action Summary	Application No. 13/163,590	Applicant(s) CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06/17/11*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/03/11, 11/03/11, 11/13/12, 02/04/13, 06/26/13*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

IPR2025-00069
CrowdStrike EX1002 Page 217

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

1. Claims **1-20** are presented for examination.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claim 20 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Examiner notes that Applicant's specification fails to disclose explicit examples or provide support for a suggestion of the particular forms of media which constitute the claimed "A computer readable storage medium". Thus, Examiner applies the broadest reasonable interpretation to the aforementioned claimed "medium" and considers the claims to intend to cover both transitory and non-transitory media. As a result, the transitory media (i.e. propagating signal for transmission of software) which is not patentable subject matter causes the claims to be rejected under 35 USC §101, as non-statutory.

Claim Rejections - 35 USC § 103

3. The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-20 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Jiang** U.S. Pub. No. **2008/0320594**, in view of **Aziz et al.,** U.S. Pub. No. **2012/0331553**.

4. As to claim 1, 20, **Jiang** teaches the invention as claimed, including a computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises: one or more processors; and memory storing:

a virtual machine (fig. 3, virtual machine 310); and

a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor (fig. 3, VM monitor 370):

monitoring activity on the virtual machine (par. 0039-0061);

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061).

Jiang does not explicitly teach storing in the memory the activity sources, activity targets, and associations; creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and transmitting the fingerprint to

prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

Aziz teaches storing in the memory the activity sources, activity targets, and associations (par. 0019, 0159-0161, 0179, 0190-0193);

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine (abstract, par. 0165-0166); and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (abstract, 0175-0180).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of **Jiang and Aziz** in order to preventing the spread of malware.

5. As to claim 2, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized (par. 0064-0067, 0212).

6. As to claim 3, **Aziz** teaches the invention as claimed, including the method of claim 1, wherein the fingerprint includes files that are affected by the unauthorized activities on the virtual machine (par. 0022, 0165-0166).

7. As to claim 4, **Aziz** teaches the invention as claimed, including the method of claim 1, wherein the fingerprint includes processes that are affected by the unauthorized activities on the virtual machine (par. 0022, 0165-0166).

8. As to claim 5, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network (abstract, par. 0102-0107).

9. As to claim 6, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections (par. 0032-0044).

10. As to claim 7, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections (par. 0032-0064, 0074-0077).

11. As to claim 8, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising graphically displaying at least a subset of the stored activities (par. 0090).

12. As to claim 9, **Jiang** teaches the invention as claimed, including the method of claim 8, wherein the displaying includes visually distinguishing at least a subset of the associations (par. 0032-0033, 0044, 0077).

13. As to claim 10, **Jiang** teaches the invention as claimed, including the method of claim 8, wherein the subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity (par. 0074-0075, 0077).

14. As to claim 11, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target (par. 0022, 0165-0166).

15. As to claim 12, **Aziz** teaches the invention as claimed, including the method of claim 11, further comprising tracking a transfer of malicious associations over time (par. 0098, 0101-0103, 0127, 0249).

16. As to claim 13, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising identifying activity sources that are affected by unauthorized activities (par. 0022, 0165-0166).

17. As to claim 14, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable (par. 0022, 0165-0166).

18. As to claim 15, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein: instructions executed by the one or more processors have respective privilege levels; respective activity sources have respective privilege levels; and the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions (par. 0102).

19. As to claim 16, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system (abstract, par. 0029-0030, 0033-0043).

20. As to claim 17, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising determining an activity status for the stored events, the activity status comprising one of: a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored

activities is associated with the source through one or more associations; and an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations (par. 0022, 0165-0166).

21. As to claim 18, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval (par. 0119-0120).

22. As to claim 19, **Jiang** teaches the invention as claimed, including a system, comprising:

one or more processors (par. 0043); and

memory storing: a virtual machine (fig. 3);

a virtual machine monitor supervising the virtual machine (fig. 3); and

one or more programs, the one or more programs including instructions for: monitoring activity on the virtual machine (par. 0039-0061);

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061).

Jiang does not explicitly teach storing in the memory the activity sources, activity targets, and associations; creating, from the stored activities, a fingerprint indicative of

the activity on the virtual machine; and transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

Aziz teaches storing in the memory the activity sources, activity targets, and associations (par. 0019, 0159-0161, 0179, 0190-0193);

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine (abstract, par. 0165-0166); and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (abstract, 0175-0180).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of **Jiang and Aziz** in order to preventing the spread of malware.

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thu Ha Nguyen, whose telephone number is (571) 272-3989. The examiner can normally be reached Monday through Friday from 8:30 AM to 5:00 PM.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele can be reached on 571-272-7288. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THUHA T. NGUYEN/

Primary Examiner, Art Unit 2453

Notice of References Cited	Application/Control No. 13/163,590	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0136720 A1	06-2006	Armstrong et al.	713/164
*	B	US-2006/0294592 A1	12-2006	Polyakov et al.	726/024
*	C	US-2007/0180450 A1	08-2007	CROFT et al.	718/001
*	D	US-2007/0250930 A1	10-2007	Aziz et al.	726/24
*	E	US-2008/0005782 A1	01-2008	Aziz, Ashar	726/003
*	F	US-2008/0177994 A1	07-2008	Mayer, Yaron	713/2
*	G	US-2008/0320594 A1	12-2008	Jiang, Xuxian	726/24
*	H	US-2009/0307273 A1	12-2009	Johnson et al.	707/200
*	I	US-2010/0042632 A1	02-2010	Johnson et al.	707/100
*	J	US-2011/0179136 A1	07-2011	Twitchell, JR., Robert W.	709/217
*	K	US-2011/0239291 A1	09-2011	SOTKA, SCOTT	726/14
*	L	US-2012/0174186 A1	07-2012	Aziz et al.	726/1
*	M	US-2012/0179904 A1	07-2012	Dunn et al.	713/155

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Notice of References Cited	Application/Control No. 13/163,590	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2012/0331553 A1	12-2012	Aziz et al.	726/23
*	B	US-8,539,582 B1	09-2013	Aziz et al.	726/24
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed June 26, 2013	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T
Sheet	1	of	1	Attorney Docket Number	067292-5005US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2004/0025052 A1	02-05-2004	Dickenson	
		2005/0229250 A1	10-13-2005	Ring et al.	
/Thu Ha Nguyen/		2007/0101431 A1	05-03-2007	Clift et al.	
		2007/0180529 A1	08-02-2007	Costea et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document Country Code[3] – Number[4] - Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		JP 2005-316779	11-10-2005	Intelligent Cosmos Research Institute		
		WO 2007/027739	03-08-2007	Microsoft Corp.		

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Office Action, US 13/759,335, 14 June 2013, 32 pgs
		NeuralIQ Inc., Notice of Reasons for Rejection, JP 2010-504185, 15 March 2013, 4 pgs

Examiner Signature	/Thu Ha Nguyen/	Date Considered	09/26/2013

DB2/24194294.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

IPR2025-00069

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L3	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 12:49
L4	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 12:50
L5	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 12:51
L6	50	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 12:51
L7	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 12:51
L8	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 12:51
S1	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/18 22:51
S2	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/18 22:52
S3	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/18 22:52
S4	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/18 22:53
S5	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2013/09/18 22:53

			DERWENT			
S6	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/18 22:53
S7	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/18 22:54
S8	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 11:28
S9	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 11:30
S10	70	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 11:30
S11	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 11:31
S12	10	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 11:34
S13	2	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/09/19 11:34

EAST Search History (Interference)

<This search history is empty>

9/19/2013 12:58:45 PM
C:\Users\tnguyen39\Documents\EAST\Workspaces\13163590.wsp

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed October 3, 2011*	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Capalik, Alen
				Art Unit	2431
				Examiner Name	Not yet assigned
Sheet	1	of	2	**Attorney Docket Number**	067292-5005-US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	1.	6,009,274	12-28-1999	Fletcher et al.	
	2.	6,279,113 B1	08-21-2001	Vaidya	
	3.	7,222,366 B2	05-22-2007	Bruton, III et al.	
	4.	7,392,543 B2	06-24-2008	Szor	
	5.	7,464,407 B2	12-09-2008	Nakae et al.	
	6.	US 2002/0099752 A1	07-25-2002	Markos et al.	
	7.	US 2002/0166063 A1	11-07-2002	Lachman, III et al.	
	8.	US 2003/0120935 A1	06-26-2003	Teal et al.	
	9.	US 2004/0225877 A1	11-11-2004	Huang	
	10.	US 2006/0018466 A1	01-26-2006	Adelstein et al.	
	11.	US 2006/0031673 A1	02-09-2006	Beck et al.	
	12.	US 2006/0136720 A1	06-22-2006	Armstrong et al.	
	13.	US 2006/0242703 A1	10-26-2006	Abeni	
	14.	US 2006/0288414 A1	12-21-2006	Kuroda	
	15.	US 2006/0294592 A1	12-28-2006	Polyakov et al.	
	16.	US 2007/0002689 A1	01-04-2007	Mateescu et al.	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document Country Code[3] – Number[4] - Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	1.	European Network of Affined Honeypots, "D1.2 Attack Detection and Signature Generation," May 11, 2006, 79 pgs.

Examiner Signature	/Thu Ha Nguyen/	Date Considered	09/26/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

IPR2025-00069
CrowdStrike EX1002 Page 232

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed October 3, 2011*	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Capalik, Alen
				Art Unit	2431
				Examiner Name	Not yet assigned
Sheet	2	of	2	**Attorney Docket Number**	067292-5005-US

	2.	SHIBUYA et al., "A Study for Some Experiences of the Operation of Highly Interactive Decoy System," Information Processing Society of Japan, Volume 45, No. 8, August 2004, 34 pgs.
	3.	Honeypot (computing)-Wikipedia, the free encyclopedia, downloaded July 17, 2006, 4 pgs., http://en.wikipedia.or/wiki/Honeypot_(computing)
	4.	Intrusion-detection system-Wikipedia, the free encyclopedia, downloaded July 17, 2006, 3 pgs., http://en.wikipedia.or/wiki/Intrusion_detection_system
	5.	International Search Report and Written Opinion for PCT/US08/60336 dated August 11, 2008, 9 pgs.
	6.	Office Action for 11/488,743 dated July 30, 2009, 21 pgs.
	7.	Office Action for 11/488,743 dated February 16, 2010, 23 pgs.
	8.	Office Action for 11/488,743 dated August 4, 2010, 21 pgs.
	9.	Office Action for 11/488,743 dated January 18, 2011, 23 pgs.
	10.	Office Action for 11/488,795 dated June 9, 2010, 13 pgs.
	11.	Office Action for 11/488, 795 dated December 1, 2010, 18 pgs.
	12.	Examiner's Answer for 11/488,795 dated May 31, 2011, 19 pgs.

Examiner Signature	/Thu Ha Nguyen/	Date Considered	10/22/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

IPR2025-00069
CrowdStrike EX1002 Page 233

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	Art Unit
	THU HA NGUYEN	2453

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	155, 164	09/14/13	THN
726	3, 14, 24	09/14/13	THN

SEARCH NOTES		
Search Notes	Date	Examiner
East, Derwent, JPO, EPO, USPG-Pub search	09/14/13	THN
Inventor name, assignee name search	09/14/13	THN

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

IPR2025-00069
CrowdStrike EX1002 Page 234

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/14/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

IPR2025-00069
CrowdStrike EX1002 Page 235

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	November 13, 2012
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	CAPALIK, Alen
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number - Kind Code[1]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	5,339,426	08-16-1994	Aoshima	
	A2	6,360,327 B1	03-19-2002	Hobson	

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document Country Code[2] - Number[3] - Kind Code[4] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T Yes

OTHER NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	C1	Capalik, Notice of Allowance, U.S. Patent Application No. 11/488,743, 24 October 2012, 15 pgs
	C2	LIANG, Fast and Automated Generation of Attack Signatures: A Basis for Building Self-Protecting Servers, 7-11 November 2005
	C3	NeuralIQ, Office Action, Australian Patent Application No. 2008242296, 05 April 2012, 2 pgs

Examiner Signature	/Thu Ha Nguyen/	Date Considered	09/26/2013

DB2/ 23656556.1

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed November 3, 2011*	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Capalik, Alen
				Art Unit	2431
				Examiner Name	Not yet assigned
Sheet	1	of	1	Attorney Docket Number	067292-5005-US

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	5,664,159	09-02-1997	Richter et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document Country Code[3] – Number[4] - Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
	B1	WO 2006/113781 A1	10-26-2006	The Trustees of Columbia University in the City of New York		

NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
	C1	ASRIGO et al., "Using VMM-Based Sensors to Monitor Honeypots," Department of Electrical and Computer Engineering, VEE'06, June 14-16, 2006, pgs. 13-23.
	C2	Debug Register, "Aus Lowlevel," March 22, 2010, 5 pgs.
	C3	JOSHI et al., "Detecting Past and Present Intrusions Through Vulnerability-Specific Predicates," Department of Electrical Engineering and Computer Science, SOSP'05, October 23-26, 2005, 14 pgs.
	C4	KRAPF et al., "XEN Memory Management (Intel IA-32)," October 30, 2007, 6 pgs.
	C5	LITTY et al., "Hypervisor Support for Identifying Covertly Executing Binaries," SS'08 Proceedings of the 17th Conference on Security Symposium, December 31, 2008, 1-16 pgs.
	C6	PROVOS, "A Virtual Honeypot Framework," October 21, 2003, 11pgs.
	C7	NEURALIQ, Inc., PCT/US2011/041122, June 20, 2011, International Search Report and Written Opinion mailed September 21, 2011, 14 pgs.
	C8	NEURALIQ, Inc., PCT/US2011/041119, June 20, 2011, International Search Report and Written Opinion mailed October 4, 2011, 14 pgs.

Examiner Signature	/Thu Ha Nguyen/	Date Considered	09/26/2013

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

DB2/ 22754118.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

IPR2025-00069
CrowdStrike EX1002 Page 237

INFORMATION DISCLOSURE CITATION IN A PATENT PTO 1449				Electronically filed	February 4, 2013
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	CAPALIK, Alen
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.	Document Number Number - Kind Code[1]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear

FOREIGN PATENT DOCUMENTS						
Examiner Initials	Cite No.	Foreign Patent Document Country Code[2] - Number[3] - Kind Code[4] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pgs, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T Yes

OTHER NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		NeuralIQ, Office Action, CA 2,689,126, 15AUG2012, 3 pgs

Examiner Signature	/Thu Ha Nguyen/	Date Considered	09/26/2013

DB2/ 23862789.1

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

IPR2025-00069
CrowdStrike EX1002 Page 238

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed November 18, 2013**	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2001/0011254 A1	08-02-2001	Clark	
		2002/0194437 A1	12-19-2002	Kapoor et al.	
		2004/0153672 A1	08-05-2004	Watt et al.	
		2004/0177269 A1	09-09-2004	Belnet et al.	
		2007/0240221 A1	10-11-2007	Tuvell et al.	
		2008/0127114 A1	05-29-2008	Vasudevan	
		2010/0095281 A1	04-15-2010	Raber	
		5,621,886	04-15-1997	Alpert et al.	
		5,740,413	04-14-1998	Alpert et al.	
		6,343,280 B2	01-29-2002	Clark	
		6,446,062 B1	09-03-2002	Levine et al.	
		7,996,836 B1	08-09-2011	McCorkendale et al.	

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Notice of Allowance, US 13/759,335, 09 October 2013, 10 pgs
		NeuralIQ Inc., Decision to Grant a Patent, JP 2010-504185, 26 July 2013, 1 pg
		Capalik, Office Action, US 13/163,578, 01 November 2013, 15 pgs

Examiner Signature		Date Considered	

Electronic Patent Application Fee Transmittal

Application Number:	13163590
Filing Date:	17-Jun-2011
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Dion M. Bregman/Lamesha Robertson
Attorney Docket Number:	067292-5005-US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	17427666
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Lamesha Robertson
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	18-NOV-2013
Filing Date:	17-JUN-2011
Time Stamp:	18:04:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	6146
Deposit Account	500310
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

IPR2025-00069
CrowdStrike EX1002 Page 242

1	Non Patent Literature	Capalik_NOA_13_759_335_09_October_2013.pdf	447000 cfdd8d6730195e24bcd19e58d04714d7db50f7b0	no	10
Warnings:					
Information:					
2	Non Patent Literature	Neural_Decision_to_Grant_JP_2010_504_185_26_July_2013.pdf	69262 d505163880000dcc231ff78fcfb97c5d9ec0b207	no	1
Warnings:					
Information:					
3	Non Patent Literature	Capalik_OA_13_163_578_01_November_2013.pdf	513813 c832dce2a9af978b8ba150aab99f488e88ada34d	no	15
Warnings:					
Information:					
4		067292_5005_US_IDS.pdf	243193 ae76e99df801f30280fb3ffca7318408f7c1a1d0	yes	5

Multipart Description/PDF files in .zip description

Document Description	Start	End
Transmittal Letter	1	4
Information Disclosure Statement (IDS) Form (SB08)	5	5

Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30272 427e1f0805bdddc97f352a3b0fe528901d2ae7e2	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1303540		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed November 18, 2013

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

IPR2025-00069
CrowdStrike EX1002 Page 245

2. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☒ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005US).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application

not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☒ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: November 15, 2013

59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

Electronically filed: January 27, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This response is in reply to the Office Action from the U.S. Patent and Trademark Office dated October 25, 2013. Please enter the following amendments and remarks into the file of the above identified application.

The Commissioner has been authorized through the electronic filing system to charge any additional fees or credit any overpayment associated with this communication to Deposit Account No. 50-0310 (order No. 067292-5005-US).

Amendments to the Claims begin on page 2.

Remarks begin on page 6.

IPR2025-00069
CrowdStrike EX1002 Page 249

CLAIM AMENDMENTS

The following listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Original) A computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises:

one or more processors; and

memory storing:

a virtual machine; and

a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

2. (Original) The method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.

3. (Original) The method of claim 1, wherein the fingerprint includes files that are affected by the unauthorized activities on the virtual machine.

4. (Original) The method of claim 1, wherein the fingerprint includes processes that are affected by the unauthorized activities on the virtual machine.

IPR2025-00069
CrowdStrike EX1002 Page 250

5. (Original) The method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

6. (Original) The method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

7. (Original) The method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

8. (Original) The method of claim 1, further comprising graphically displaying at least a subset of the stored activities.

9. (Original) The method of claim 8, wherein the displaying includes visually distinguishing at least a subset of the associations.

10. (Original) The method of claim 8, wherein the subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity.

11. (Original) The method of claim 1, further comprising identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.

12. (Original) The method of claim 11, further comprising tracking a transfer of malicious associations over time.

13. (Original) The method of claim 1, further comprising identifying activity sources that are affected by unauthorized activities.

14. (Original) The method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.

15. (Original) The method of claim 13, wherein:

instructions executed by the one or more processors have respective privilege levels;

IPR2025-00069
CrowdStrike EX1002 Page 251

respective activity sources have respective privilege levels; and

the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions.

16. (Original) The method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system.

17. (Original) The method of claim 1, further comprising determining an activity status for the stored events, the activity status comprising one of:

a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and

an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.

18. (Original) The method of claim 1, further comprising determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval.

19. (Original) A system, comprising:

one or more processors; and

memory storing:

a virtual machine;

a virtual machine monitor supervising the virtual machine; and

one or more programs, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

IPR2025-00069
CrowdStrike EX1002 Page 252

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

20. (Currently amended) A non-transitory computer readable storage medium, including one or more programs for execution by one or more processors of a computer system, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

IPR2025-00069
CrowdStrike EX1002 Page 253

REMARKS

This amendment responds to the office action mailed October 25, 2013. In the office action, the Examiner rejected:

A. claim 20 under 35 U.S.C. 101; and

B. claims 1-20 under pre-AIA 35 U.S.C. 103(a) over Jiang (US Pub. No. 2008/0320594) and Aziz (U.S. Pub. No. 2012/0331553).

INTERVIEW SUMMARY

Applicants' attorneys thank Examiner Nguyen for her comments during a telephone interview on January 23, 2014 with Applicants' attorneys, Dion Bregman and Tae-Woong Koo. In the interview, the Examiner agreed to consider Applicants' arguments once filed and indicated that the pending claims would likely require a new search. The Examiner also agreed to call Applicants' attorneys to schedule another interview if the application is not in condition for allowance.

OVERVIEW OF CHANGES TO THE CLAIMS

Claim 20 has been revised to insert "non-transitory" pursuant to 1351 Off. Gaz. Pat. Office 212 (February 23, 2010). Pursuant to the Official Gazette, such an amendment would not raise the issue of new matter. No new matter has been added.

With respect to all amendments, Applicants have not dedicated or abandoned any unclaimed subject matter. Moreover, Applicants have not acquiesced to any characterizations of the invention, nor any rejections or objections of the claims, made by the Examiner.

After entry of this amendment, the pending claims are: claims 1-20.

ARGUMENT

Applicants have not amended any of the claims substantively, and instead present arguments for their allowability. Applicants have not dedicated or abandoned any unclaimed subject matter. Applicants do not acquiesce to any characterizations of the invention, nor any rejections or objections of the claims, made by the Examiner.

IPR2025-00069
CrowdStrike EX1002 Page 254

Claim Rejections - 35 U.S.C. § 101

A. Rejection of claim 20 under 35 U.S.C. 101

Claim 20 has been amended to clarify that the computer readable storage medium is a "non-transitory" computer readable storage medium. As such, Applicants respectfully request that this rejection be withdrawn.

Claim Rejections - 35 U.S.C. § 103

The Examiner has rejected claims 1-20 under 35 U.S.C. 103(a) over Jiang and Aziz. This set of claims contains 3 independent claims, namely claims 1, 19 and 20.

To establish prima facie obviousness of a claimed invention, all the claim elements must be taught or suggested by the prior art. *In re Royka,* 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Indeed, the Board of Patent Appeal and Interferences confirmed that a proper obviousness determination requires an Examiner to make "a searching comparison of the claimed invention - including all its limitations - with the teaching of the prior art." See *In re Wada and Murphy,* Appeal 2007-3733, citing *In re Ochiai,* 71 F.3d 1565, 1572 (Fed. cir. 1995) (emphasis in original). Finding all the claim elements in the prior art is necessary, but not sufficient. *KSR Intern. Co. v. Teleflex Inc.,* 127 S.Ct. 1727, 1741 (2007) ("a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art"). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson,* 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, and (3) the level of skill in the art. *Graham v. John Deere Co.,* 383 U.S. 1, 17-18 (1966); *see also KSR Int'l Co. V. Teleflex Inc.,* 550 U.S. 398, 399 (2007). "Section 103 forbids issuance of a patent when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR,* at 2 (internal quotations omitted). Thus, to be patentable, the differences between the claimed subject matter and the prior art must be substantial enough to not be obvious to a person of ordinary skill in the art.

IPR2025-00069
CrowdStrike EX1002 Page 255

B. Rejection of claims 1-20 under 35 U.S.C. 103(a) over Jiang and Aziz

(a) The combination of Jiang and Aziz does not teach or suggest "identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target" as recited in claims 1 and 19-20

Independent claims 1 and 19-20 recite:

> identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an **activity source**, an **activity target**, and an **association between the activity source and the activity target**.

As explained in paragraphs [0007] and [0013] of this application, zero-day attacks are a critical threat to computer networks, and the above-recited features are important in dealing with such zero-day attacks.

> [0007] A critical threat to computer networks is the so-called zero-day attack that exploits security vulnerabilities previously unknown to software developers or system operators. Because the security vulnerabilities are unknown to the software developers or system operators, often the fingerprints of such zero-day attacks are unavailable for comparison. Until the fingerprints are identified, attacks exploiting the same security vulnerabilities continue without detection by the network security systems. However, identifying the fingerprints of malicious activities in the middle of numerous other non-malicious processes is not a trivial task.
>
> [0013] These embodiments identify unauthorized activities by monitoring and identifying associations between activity sources and activity targets without using pre-determined fingerprints. The data collected by these embodiments can be used to generate fingerprint data in response to the zero-day attacks.

Following the guidelines set by the Supreme Court in *KSR,* one first determines the scope and content of the prior art. Jiang teaches a malware detector, while Aziz teaches a dynamic signature creation and enforcement system configured to analyze network data. However, neither Jiang nor Aziz, either alone or in combination, teach or suggest "identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an **activity source**, an **activity target**, and an **association between the activity source and the activity target**," as required by claims 1 and 19-20.

With respect to the above-recited features, the Examiner states:

> Jiang teaches ... identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity

IPR2025-00069
CrowdStrike EX1002 Page 256

> source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061).[1]

However, paragraphs [0035], [0048]-[0050] and [0059]-[0061] of Jiang, cited by the Examiner, state (emphasis added):

> [0035] ... The open-source VMMs (QEMU, Xen, and UML) allow full access to low-level VM states and events. ...
>
> [0048] ... the instructions may further include, as shown in FIG. 2, retrieving for inspection virtual machine internal system events from the virtual resources S210. ... The virtual machine internal system events may comprise virtual memory events and/or virtual disk events.
>
> [0049] ... the instructions further include interpreting the **virtual memory events** and/or **virtual disk events** S220. After interpretation, the instructions may further include transparently encapsulating and presenting the interpreted virtual memory events and/or the interpreted virtual disk events to the anti-malware software S230.
>
> [0050] Interpreting either or both these types of events also help enable guest function extrapolation. Just as with the virtual machine internal system states, extrapolation can aid in extracting semantic-rich data ... from the virtual machine internal system events.
>
> [0059] Not only can the malware detection system 305 retrieve, interpret, and transparently encapsulate and present virtual machine internal system states, but it can also do the same for **virtual machine internal system events**. Such events can be retrieved from the virtual resources 340 for inspection. Retrieval of these events is also based on non-intrusive virtual machine introspection without perturbing their execution. The **virtual machine internal system events** may comprise **virtual memory events** ... and **virtual disk events** ....
>
> [0060] The malware detection system 305 may use the virtual machine inspector 362 may be configured to retrieve the virtual memory events from a virtual machine monitor .... Generally running between the host operating system ... and the virtual machine ..., the virtual machine monitor ... may be configured to intercept the virtual memory events. Upon interception, the guest function extrapolator 364 may extract semantic-rich data by interpreting the virtual memory events. Afterwards, the transparent presenter 366 may encapsulate and present the interpreted virtual memory events to the anti-malware software. Like above, the anti-malware software ... may be configured to use the virtual memory events to detect system compromises.
>
> [0061] Similarly, the malware detection system 305 may also use the virtual machine inspector 362 to retrieve the virtual disk events from a virtual machine monitor .... The virtual machine monitor ..., running between the host operating system ... and the virtual machine ... may

[1] Office action dated 10-25-2013, p. 3.

IPR2025-00069
CrowdStrike EX1002 Page 257

> be configured to intercept the virtual disk events. After interception, the guest function extrapolator 364 may extract semantic-rich data by interpreting the virtual disk events. Then, the transparent presenter 366 may encapsulate and present the interpreted virtual disk events to the anti-malware software ... for detecting any system comprise.

As shown above, paragraphs [0035], [0048]-[0050] and [0059]-[0061] of Jiang describe a malware detection system that detects virtual memory events and virtual disk events. These detected events in Jiang are interrupt, memory, and I/O access events.[2] Even if these events were targets, which they are not, Jiang simply does not disclose all of "an activity **source**, an activity **target**, and an **association between the activity source and the activity target**." As such, Jiang does not teach or suggest the above-recited features. Aziz is not cited for, nor does it teach or suggest the above-recited features.

Claims 2-18 depends on independent claim 1 and thus include all the limitations in claim 1. As discussed above, Jiang and Aziz do not teach or suggest every limitation of independent claim 1. Because Jiang and Aziz, either alone or in combination, do not teach or suggest each and every claim limitation, it is respectfully submitted that independent claims 1, 19, and 20, and associated dependent claims 2-18, are patentable over the cited references.

CONCLUSION

In view of the foregoing, it is respectfully submitted that the application is now in a condition for allowance. However, should the Examiner believe that the claims are not in condition for allowance, the Applicants request an Examiner Interview. The Examiner may contact the undersigned attorney at dbregman@morganlewis.com or 650.843.7519 to arrange a suitable time for the interview.

Respectfully submitted,

Date: January 27, 2014

45,645

Dion M. Bregman (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, California 94306
(650) 843-4000

[2] *See* paragraph [0067] of Jiang.

IPR2025-00069
CrowdStrike EX1002 Page 258

Electronic Acknowledgement Receipt

EFS ID:	18039671
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Sherri Ballbach
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	27-JAN-2014
Filing Date:	17-JUN-2011
Time Stamp:	19:54:52
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292-5005-US_ResponseToOfficeActionWithInterviewSummary.pdf	499136 3e9ea4e523ce349d29584cae83a1946290457974	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	5
	Applicant Arguments/Remarks Made in an Amendment	6	10
Warnings:			
Information:			
	Total Files Size (in bytes):	499136	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/163,590	Filing Date 06/17/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
	01/27/2014	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $40 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)		
		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/TARA WITCHER/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

24341 7590 01/29/2014

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
01/29/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/163,590	CAPALIK ET AL.	
	Examiner	Art Unit	
	THU HA NGUYEN	2453	

All participants (applicant, applicant's representative, PTO personnel):

(1) *THU HA NGUYEN*.

(3) *Dion Bregman (Reg. No. 45,645)*.

(2) *Tae-Woong Koo (Reg. No. 59,649)*.

(4)_____.

Date of Interview: *23 January 2014*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Jiang (USPN 2008/0320594) and Aziz (USPN 2012/0331553)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representatives discussed the different between the prior arts and the claimed invention and pointed out that Jiang does not teach or disclose the activity source, activity target and an association between the activity source and activity target. The examiner will reconsider and/or update search upon receiving the formal response.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/THU HA NGUYEN/ Primary Examiner, Art Unit 2453	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 05/01/2014

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER
NGUYEN, THU HA T

ART UNIT	PAPER NUMBER
2453	

DATE MAILED: 05/01/2014

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

TITLE OF INVENTION: System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	08/01/2014

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

IPR2025-00069
CrowdStrike EX1002 Page 265

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 05/01/2014
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

TITLE OF INVENTION: System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	08/01/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
NGUYEN, THU HA T	2453	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

IPR2025-00069
CrowdStrike EX1002 Page 266

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

24341 7590 05/01/2014

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER	
NGUYEN, THU HA T	
ART UNIT	**PAPER NUMBER**
2453	

DATE MAILED: 05/01/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

IPR2025-00069
CrowdStrike EX1002 Page 267

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/163,590	Applicant(s) CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *01/27/14*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-20*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 11/18/13
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/THU HA NGUYEN/
Primary Examiner, Art Unit 2453

Notice of References Cited	Application/Control No. 13/163,590	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2003/0023656 A1	01-2003	Hutchison et al.	709/100
*	B	US-7,581,219 B2	08-2009	Neiger et al.	718/1
*	C	US-7,596,654 B1	09-2009	Wong, Kai C.	711/6
*	D	US-2011/0060947 A1	03-2011	Song et al.	714/37
*	E	US-8,365,180 B2	01-2013	Kawasaki et al.	718/104
*	F	US-8,448,170 B2	05-2013	Wipfel et al.	718/1
*	G	US-2013/0238785 A1	09-2013	Hawk et al.	709/224
*	H	US-8,539,582 B1	09-2013	Aziz et al.	726/24
*	I	US-2013/0254870 A1	09-2013	Sotka, Scott	726/11
*	J	US-8,572,613 B1	10-2013	Brandwine, Eric J.	718/100
*	K	US-2013/0304903 A1	11-2013	Mick et al.	709/224
*	L	US-2014/0026121 A1	01-2014	Jackson et al.	717/124
*	M	US-8,683,548 B1	03-2014	Curry et al.	726/1

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1008

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/163,590	06/17/2011	726	2453	067292-5005-US

APPLICANTS

INVENTORS

Alen Capalik, Pacific Palisades, CA;
David Andrews, Los angeles, CA;
Ben Becker, Santa Monica, CA;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/358,367 06/24/2010

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **

06/29/2011

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /THU HA T NGUYEN/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	17	20	3

ADDRESS

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306
UNITED STATES

TITLE

System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

FILING FEE RECEIVED		
462	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

IPR2025-00069
CrowdStrike EX1002 Page 271

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	23	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:08
L2	7	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN. and (virtual adj machine$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:09
L3	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L4	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L5	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L6	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L7	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L8	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L9	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L10	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L11	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L12	83	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4)	US-PGPUB; USPAT;	OR	OFF	2014/04/07 10:21

		and source and target$4 and fingerprint$4	EPO; JPO; DERWENT			
L13	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L14	12	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L15	2	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L16	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L17	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L18	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L19	59	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L20	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L21	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:21
L22	18	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:27
L26	6388	718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:27
L27	1	22 and 26	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:27
L28	5390	718/100.ccls.	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/04/07 10:28

			DERWENT			
L29	0	22 and 28	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:28
L30	0	19 and 28	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:28
L31	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "7263".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:33
L32	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "726/3".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:33
L33	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/3.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:33
L34	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/14-15.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:33
L35	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/24-26.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:33
L36	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/22.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:33
L37	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/11.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:33
L38	162	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:34
L39	9	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:34
L40	66	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:35
L41	6388	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2014/04/07 10:36

		same auth$7 same fingerprint$4 718/1.ccls.	DERWENT			
L42	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:47
L43	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:48
L44	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:48
L45	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 10:48
L47	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/04/07 12:36

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L23	18	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 10:27
L24	4872	718/1.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 10:27
L25	4568	718/100.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 10:27
L46	9	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 11:37
L48	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 12:38
L49	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/155.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 12:44
L50	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/164-165.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 12:44
L51	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and	US-PGPUB; USPAT;	OR	OFF	2014/04/07 12:45

		prevent$4 same attack$4	UPAD			
L52	66	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 12:45
L53	84	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; UPAD	OR	OFF	2014/04/07 12:45

4/ 7/ 2014 1:05:41 PM
C:\ Users\ tnguyen39\ Documents\ EAST\ Workspaces\ 13163590.wsp

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

CPC						
Symbol					**Type**	**Version**
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets						
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	20	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2453	04/16/14	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION										
CLASS	SUBCLASS	CLAIMED					NON-CLAIMED					
726	25	G	0	6	F	11 / 00 (2006.01.01)						

CROSS REFERENCE(S)					
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	3	14	15	24	25
709	223	224			
713	155	164	165		
718	1	100			

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2453	04/16/14	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

IPR2025-00069
CrowdStrike EX1002 Page 278

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

☒ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☐ **T.D.** ☐ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17												
	2		18												
	3		19												
	4		20												
	5														
	6														
	7														
	8														
	9														
	10														
	11														
	12														
	13														
	14														
	15														
	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 20	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2453 (Primary Examiner)	04/16/14 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed November 18, 2013	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005US

U.S. PATENT DOCUMENTS					
Examiner Initials	Cite No.[1]	Document Number Number - Kind Code[2]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		2001/0011254 A1	08-02-2001	Clark	
		2002/0194437 A1	12-19-2002	Kapoor et al.	
		2004/0153672 A1	08-05-2004	Watt et al.	
		2004/0177269 A1	09-09-2004	Belnet et al.	
		2007/0240221 A1	10-11-2007	Tuvell et al.	
		2008/0127114 A1	05-29-2008	Vasudevan	
		2010/0095281 A1	04-15-2010	Raber	
		5,621,886	04-15-1997	Alpert et al.	
		5,740,413	04-14-1998	Alpert et al.	
		6,343,280 B2	01-29-2002	Clark	
		6,446,062 B1	09-03-2002	Levine et al.	
		7,996,836 B1	08-09-2011	McCorkendale et al.	

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Notice of Allowance, US 13/759,335, 09 October 2013, 10 pgs
		NeuralIQ Inc., Decision to Grant a Patent, JP 2010-504185, 26 July 2013, 1 pg
		Capalik, Office Action, US 13/163,578, 01 November 2013, 15 pgs

Examiner Signature	/Thu Ha Nguyen/	Date Considered	04/07/2014

DB2/ 24519607.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

IPR2025-00069
CrowdStrike EX1002 Page 280

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	Art Unit
	THU HA NGUYEN	2453

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	155, 164	09/14/13	THN
726	3, 14, 24	09/14/13	THN
Update search		04/06/14	THN
709	223, 224	04/06/14	THN
726	3, 14-15, 22, 24-26	04/06/14	THN
718	1, 100	04/06/14	THN
713	155, 164, 165	04/06/14	THN

SEARCH NOTES		
Search Notes	Date	Examiner
East, Derwent, JPO, EPO, USPG-Pub search	09/14/13	THN
Inventor name, assignee name search	09/14/13	THN
Update search	04/06/14	THN
East, Derwent, JPO, EPO, USPG-Pub search	04/06/14	THN
Inventor name, assignee name search	04/06/14	THN
NPL, Google search	04/06/14	THN

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

IPR2025-00069
CrowdStrike EX1002 Page 281

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
726	3, 14, 15, 24, 25	04/06/14	THN
709	223, 224	04/06/14	THN
713	155, 164, 165	04/06/14	THN
718	1, 100	04/06/14	THN

IPR2025-00069
CrowdStrike EX1002 Page 282

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

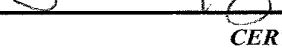
Address to:
Mail Stop RCE
Commissioner of Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Electronically filed	June 17, 2014
Application Number	13/163,590
Filing Date	June 17, 2011
First Named Inventor	Capalik
Art Unit	2453
Examiner Name	Nguyen, Thu Ha T.
Attorney Docket No.	067292-5005-US

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application. Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application.

1. Submission required under 37 C.F.R. § 1.114
   - a. ☐ Previously submitted
     - i. ☐ Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on _____ (Any unentered amendment(s) referred to above will be entered).
     - ii. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed _____
     - iii. ☐ Other _____
   - b. ☒ Enclosed
     - i. ☐ Amendment/Reply
     - ii. ☐ Affidavit(s)/Declaration(s)
     - iii. ☒ Information Disclosure Statement (IDS)
     - iv. ☒ Other Cited References
2. Miscellaneous
   - a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 C.F.R. § 1.17(i) required)
   - b. ☐ Other _____
3. Fees — The RCE fee under 37 C.F.R. § 1.17(e) is required by 37 C.F.R. § 1.114 when the RCE is filed
   - a. ☒ The Director is hereby authorized to charge the following fees, any underpayment of fees, or credit any overpayments, to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US).
     - i. ☒ (1st request) RCE fee required under 37 C.F.R. § 1.17(e)(1), estimated to be **$600 (small entity)**
     - ii. ☐ (2nd or subsequent request) RCE fee required under 37 C.F.R. § 1.17(e)(2), estimated to be $ 1700 (large entity) or $850 (small entity)
     - iii. ☐ Extension of time fee required under 37 C.F.R. §§ 1.136 and 1.17, estimated to be $ for a month(s) extension, the request for which is being made herewith
     - iv. ☐ Other _____
   - b. ☐ Check in the amount of $ _____ enclosed
   - c. ☐ Payment by credit card (Form PTO-2038 enclosed)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name (Print/Type)	Tae-Woong Koo	*Registration No. (Attorney/Agent)*	59,649
Signature		*Date*	June 17, 2014

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or by facsimile transmitted to fax no. 1-703- to the U.S. Patent and Trademark Office on the date indicated below.

Name (Print/Type)		*Registration No. (Attorney/Agent)*	
Signature		*Date*	

DB2/ 25156985.1

Electronically filed June 17, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☐ Each foreign patent;

☒ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

2. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☒ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☐ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☐ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application

not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☐ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: June 17, 2014



59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed June 17, 2014	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005US

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		NeuralIQ Inc., Office Action, CA 2,689,126, 23JAN2014, 3 pgs
		NeuralIQ Inc., Patent Examination Report No. 1, AU 2011271157, 05FEB2013, 4 pgs
		Tian, A Study of Intrusion Signature Based on Honeypot, Parallel and Distributed Computing, Applications and Technologies, PDCAT'2005, 08DEC2005, pp. 125-129
		Zhang, Honeypot: a supplemented active defense system for network security, Parallel and Distributed Computing, Applications and Technologies, PDCAT'2003, 29AUG2003, pp. 231-235

Examiner Signature		Date Considered	

IPR2025-00069
CrowdStrike EX1002 Page 288

Electronic Patent Application Fee Transmittal

Application Number:	13163590
Filing Date:	17-Jun-2011
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Tae-Woong Koo/Lamesha Robertson
Attorney Docket Number:	067292-5005-US

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for Continued Examination	2801	1	600	600
		Total in USD ($)		**600**

Electronic Acknowledgement Receipt

EFS ID:	19326202
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Lamesha Robertson
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US
Receipt Date:	17-JUN-2014
Filing Date:	17-JUN-2011
Time Stamp:	13:52:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$600
RAM confirmation Number	107
Deposit Account	500310
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

IPR2025-00069
CrowdStrike EX1002 Page 291

1	Request for Continued Examination (RCE)	067292_5005_RCE.pdf	70711 18e478fd4a5fe0b4221f23eb70fcf2cc1c597af8	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2		067292_5005IDS.pdf	225774 b7d602ccf00da6bd54632f7d90109fefc285c239	yes	5
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	4	
	Information Disclosure Statement (IDS) Form (SB08)		5	5	
Warnings:					
Information:					
3	Non Patent Literature	NeurallQ_OA_CA_2_689_126_23_January_2014.pdf	42778 81004cc8316e10811d3858b3ac763c3e2dc433d2	no	3
Warnings:					
Information:					
4	Non Patent Literature	NeurallQ_Patent_Examination_AU_2011271157_05_February_2013.pdf	252833 c4a6bf44190c2c9eb946a355c962e84a78444b0f	no	4
Warnings:					
Information:					
5	Non Patent Literature	Tian_A_Study_of_Intrusion.pdf	396445 c9949d427743519f06e211c2b88f444525ab3c10	no	5
Warnings:					
Information:					
6	Non Patent Literature	Zhang_Honeypot_A_Supplemented_Active_Defense.pdf	400188 7d8d8dbe1e058caf8bd9e593a3360efd2f2c75dd	no	5
Warnings:					
Information:					
7	Fee Worksheet (SB06)	fee-info.pdf	30475 f2b3e5dcc431a3d3508b58ae9154fa3c000354c6	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1419204		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/163,590	Filing Date 06/17/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)		
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3 minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT	06/17/2014	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	=	X $ =	
	Independent (37 CFR 1.16(h))	* 3	Minus	***3	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

		(Column 1)		(Column 2)	(Column 3)		
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))						
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
						TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/PEGGY YARBOROUGH/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

24341 7590 08/15/2014

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
08/15/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Office Action Summary	Application No. 13/163,590	Applicant(s) CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06/17/14*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *06/17/14*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

IPR2025-00069
CrowdStrike EX1002 Page 296

The present application is being examined under the pre-AIA first to invent provisions.

DETAILED ACTION

1. Claims **1- 20** are presented for examination.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after allowance or after an Office action under *Ex Parte Quayle*, 25 USPQ 74, 453 O.G. 213 (Comm'r Pat. 1935). Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 06/17/14 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of pre-AIA 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-20 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over **Jiang** U.S. Pub. No. **2008/0320594**, in view of **Aziz et al.,** U.S. Pub. No. **2012/0331553**.

4. As to claim 1, 20, **Jiang** teaches the invention as claimed, including a computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises: one or more processors; and memory storing:

a virtual machine (fig. 3, virtual machine 310); and

a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor (fig. 3, VM monitor 370):

monitoring activity on the virtual machine (par. 0031, 0033, 0039-0061, 0065-00067 -*VMWatcher*);

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061 – *VM states and events*).

Jiang does not explicitly teach storing in the memory the activity sources, activity targets, and associations; creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

Aziz teaches storing in the memory the activity sources, activity targets, and associations (par. 0019, 0050-0051, 0159-0161, 0179, 0190-0193);

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine (abstract, par. 0165-0166); and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (abstract, 0175-0180).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of **Jiang and Aziz** in order to preventing the spread of malware.

5. As to claim 2, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized (par. 0064-0067, 0212).

6. As to claim 3, **Aziz** teaches the invention as claimed, including the method of claim 1, wherein the fingerprint includes files that are affected by the unauthorized activities on the virtual machine (par. 0022, 0165-0166).

7. As to claim 4, **Aziz** teaches the invention as claimed, including the method of claim 1, wherein the fingerprint includes processes that are affected by the unauthorized activities on the virtual machine (par. 0022, 0165-0166).

8. As to claim 5, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network (abstract, par. 0102-0107).

9. As to claim 6, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections (par. 0032-0044).

10. As to claim 7, **Jiang** teaches the invention as claimed, including the method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections (par. 0032-0064, 0074-0077).

11. As to claim 8, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising graphically displaying at least a subset of the stored activities (par. 0090).

12. As to claim 9, **Jiang** teaches the invention as claimed, including the method of claim 8, wherein the displaying includes visually distinguishing at least a subset of the associations (par. 0032-0033, 0044, 0077).

13. As to claim 10, **Jiang** teaches the invention as claimed, including the method of claim 8, wherein the subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity (par. 0074-0075, 0077).

14. As to claim 11, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target (par. 0022, 0165-0166).

15. As to claim 12, **Aziz** teaches the invention as claimed, including the method of claim 11, further comprising tracking a transfer of malicious associations over time (par. 0098, 0101-0103, 0127, 0249).

16. As to claim 13, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising identifying activity sources that are affected by unauthorized activities (par. 0022, 0165-0166).

17. As to claim 14, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein the identifying activity sources that are affected by

unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable (par. 0022, 0165-0166).

18. As to claim 15, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein: instructions executed by the one or more processors have respective privilege levels; respective activity sources have respective privilege levels; and the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions (par. 0102).

19. As to claim 16, **Jiang** teaches the invention as claimed, including the method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system (abstract, par. 0029-0030, 0033-0043).

20. As to claim 17, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising determining an activity status for the stored events, the activity status comprising one of: a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and an incomplete status, which represents that the source of unauthorized activities is not

identified, or at least one activity target in the stored activities is not associated with the source through one or more associations (par. 0022, 0165-0166).

21. As to claim 18, **Jiang** teaches the invention as claimed, including the method of claim 1, further comprising determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval (par. 0119-0120).

22. As to claim 19, **Jiang** teaches the invention as claimed, including a system, comprising:

one or more processors (par. 0043); and

memory storing: a virtual machine (fig. 3);

a virtual machine monitor supervising the virtual machine (fig. 3); and

one or more programs, the one or more programs including instructions for: monitoring activity on the virtual machine (par. par. 0031, 0033, 0039-0061, 0065-00067-*VMWatcher*);

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061 – *VM states and events*).

Jiang does not explicitly teach storing in the memory the activity sources, activity targets, and associations; creating, from the stored activities, a fingerprint indicative of

the activity on the virtual machine; and transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

Aziz teaches storing in the memory the activity sources, activity targets, and associations (par. 0019, 0050-0051, 0159-0161, 0179, 0190-0193);

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine (abstract, par. 0165-0166); and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (abstract, 0175-0180).

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to combine the teaching of **Jiang and Aziz** in order to preventing the spread of malware.

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thu Ha Nguyen, whose telephone number is (571) 272-3989. The examiner can normally be reached Monday through Friday from 8:30 AM to 5:00 PM.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Krista Zele can be reached on 571-272-7288. The fax phone

number for the organization where this application or proceeding is assigned is 571-273-8300.

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/THU HA NGUYEN/

Primary Examiner, Art Unit 2453

Notice of References Cited	Application/Control No. 13/163,590	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2008/0222729 A1	09-2008	Chen et al.	726/24
*	B	US-2012/0255018 A1	10-2012	Sallam, Ahmed Said	726/24
*	C	US-2012/0255012 A1	10-2012	Sallam, Ahmed Said	726/24
*	D	US-2013/0047257 A1	02-2013	Aziz, Ashar	726/24
*	E	US-2013/0238785 A1	09-2013	Hawk et al.	709/224
*	F	US-2013/0304903 A1	11-2013	Mick et al.	709/224
*	G	US-2014/0096131 A1	04-2014	Sonnek et al.	718/1
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	09/14/2013	08/11/2014							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

IPR2025-00069
CrowdStrike EX1002 Page 307

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	2	"20120331553".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:04
L2	2	"20080320594".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:05
L3	17	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/554.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:32
L4	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/56.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:33
L5	13	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:33
L6	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/51.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:33
L7	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/52.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:33
L8	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:33
L9	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:34
L10	17	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:34
L11	26	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/22-25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2014/08/11 10:46

EAST Search History (Interference)

< This search history is empty>

8/ 11/ 2014 10:47:00 AM
C:\ Users\ tnguyen39\ Documents\ EAST\ Workspaces\ 13163590.wsp

IPR2025-00069
CrowdStrike EX1002 Page 309

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	Art Unit
	THU HA NGUYEN	2453

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/50-52, 21/56, 554, 566	08/11/14	THN
H04L63/145, 1491	08/11/14	THN

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	155, 164	09/14/13	THN
726	3, 14, 24	09/14/13	THN
Update search		04/06/14	THN
709	223, 224	04/06/14	THN
726	3, 14-15, 22, 24-26	04/06/14	THN
718	1, 100	04/06/14	THN
713	155, 164, 165	04/06/14	THN
726	22-25	08/11/14	THN

SEARCH NOTES		
Search Notes	Date	Examiner
East, Derwent, JPO, EPO, USPG-Pub search	09/14/13	THN
Inventor name, assignee name search	09/14/13	THN
Update search	04/06/14	THN
East, Derwent, JPO, EPO, USPG-Pub search	04/06/14	THN
Inventor name, assignee name search	04/06/14	THN
NPL, Google search	04/06/14	THN
Update search	08/11/14	THN

IPR2025-00069
CrowdStrike EX1002 Page 310

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
726	3, 14, 15, 24, 25	04/06/14	THN
709	223, 224	04/06/14	THN
713	155, 164, 165	04/06/14	THN
718	1, 100	04/06/14	THN

IPR2025-00069
CrowdStrike EX1002 Page 311

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed June 17, 2014	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005US

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		NeuralIQ Inc., Office Action, CA 2,689,126, 23JAN2014, 3 pgs
		NeuralIQ Inc., Patent Examination Report No. 1, AU 2011271157, 05FEB2013, 4 pgs
		Tian, A Study of Intrusion Signature Based on Honeypot, Parallel and Distributed Computing, Applications and Technologies, PDCAT'2005, 08DEC2005, pp. 125-129
		Zhang, Honeypot: a supplemented active defense system for network security, Parallel and Distributed Computing, Applications and Technologies, PDCAT'2003, 29AUG2003, pp. 231-235

Examiner Signature	/Thu Ha Nguyen/	Date Considered	08/11/2014

DB2/ 25155894.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

IPR2025-00069
CrowdStrike EX1002 Page 312

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed September 12, 2014**	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		NeuralIQ Inc., Extended European Search Report, 08745858-4, 12JUN2014, 4 pgs

Examiner Signature		Date Considered	

Electronic Acknowledgement Receipt

EFS ID:	20123279
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Ramona J Zaya
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US
Receipt Date:	12-SEP-2014
Filing Date:	17-JUN-2011
Time Stamp:	17:44:33
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292-5005-US-IDS.pdf	205221 a20aad6d5d6aca3a5c1ae5ff4cb2c3a79b0db504	yes	5

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	4
	Information Disclosure Statement (IDS) Form (SB08)	5	5

Warnings:					
Information:					
2	Non Patent Literature	NeurallQInc-ExtendedESR-08745858-4-12JUN2014-4pgs.pdf	107921 e999a5f955f3ed468130c75aba23f555cb9bd103	no	4
Warnings:					
Information:					
		Total Files Size (in bytes):	313142		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronically filed September 12, 2014

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Alen Capalik et al	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

INFORMATION DISCLOSURE STATEMENT

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information which the Examiner may consider material to the examination of the subject U.S. patent application. It is requested that the Examiner make this information of record if it is deemed material to the examination of the application.

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☐ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☒ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

2. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check Item 4a and 4b or 4c)

4a. ☒ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☒ Certification Statement (applicable if Item 3a or Item 4a is checked)

(Check either Item 5a, 5b, 5c or 5d)

5a. ☒ In accordance with 37 C.F.R. §1.97(e)(1), it is certified that each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application

not more than three months prior to the filing of this Information Disclosure Statement.

5b. ☐ In accordance with 37 C.F.R. §1.97(e)(2), it is certified that no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 C.F.R. §1.56(c) more than three months prior to the filing of this information disclosure statement.

5c. ☐ Each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

5d. ☐ Pursuant to 37 C.F.R. §1.704(d), each item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart application, and the communication was not **received** by any individual designated in 37 C.F.R. §1.56(c) more than thirty days prior to the filing of this information disclosure statement.

6. ☐ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: September 12, 2014

59,649

Tae-Woong Koo (Reg. No.)

MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

Electronically filed: January 15, 2015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

RESPONSE TO OFFICE ACTION

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This response is in reply to the Office Action from the U.S. Patent and Trademark Office dated August 15, 2014. Please enter the following amendments and remarks into the file of the above identified application.

Petition for Extension of Time under 37 CFR 1.136. It is respectfully requested that the time for response to the Office Action dated August 15, 2014 be extended for a period of two (2) months from November 15, 2014 to January 15, 2015.

The Commissioner has been authorized through the electronic filing system to charge any additional fees or credit any overpayment associated with this communication to Deposit Account No. 50-0310 (order No. 067292-5005-US).

Amendments to the Claims begin on page 2.

Remarks begin on page 6.

IPR2025-00069
CrowdStrike EX1002 Page 320

Amendments to the Claims

The following listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Original) A computer implemented method of identifying unauthorized activities on a decoy computer system attached to a computer network, wherein the decoy system comprises:

one or more processors; and

memory storing:

a virtual machine; and

a virtual machine monitor supervising the virtual machine, the method comprising, at the virtual machine monitor:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

2. (Original) The method of claim 1, wherein the monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.

3. (Original) The method of claim 1, wherein the fingerprint includes files that are affected by the unauthorized activities on the virtual machine.

4. (Original) The method of claim 1, wherein the fingerprint includes processes that are affected by the unauthorized activities on the virtual machine.

IPR2025-00069
CrowdStrike EX1002 Page 321

5. (Original) The method of claim 1, wherein the activities comprise two or more of: a file initiating an execution of an instruction, an instruction reading a file, an instruction writing to a file, and receiving data through the network.

6. (Original) The method of claim 1, wherein a respective activity target comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

7. (Original) The method of claim 1, wherein a respective activity source comprises one of: a file, a user, an instruction, a thread, data stream, and network socket connections.

8. (Original) The method of claim 1, further comprising graphically displaying at least a subset of the stored activities.

9. (Original) The method of claim 8, wherein the displaying includes visually distinguishing at least a subset of the associations.

10. (Original) The method of claim 8, wherein the subset of activities includes a first activity and a second activity, and the activity target of the first activity is the activity source of the second activity.

11. (Original) The method of claim 1, further comprising identifying a respective association between a first activity source and a first activity target as unauthorized, wherein the first activity target, when associated as a second activity source with a second activity target, causes unauthorized activities on the second activity target.

12. (Original) The method of claim 11, further comprising tracking a transfer of malicious associations over time.

13. (Original) The method of claim 1, further comprising identifying activity sources that are affected by unauthorized activities.

14. (Original) The method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.

15. (Original) The method of claim 13, wherein:

instructions executed by the one or more processors have respective privilege levels;

respective activity sources have respective privilege levels; and

IPR2025-00069
CrowdStrike EX1002 Page 322

the identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to execute underprivileged instructions.

16. (Original) The method of claim 13, wherein the identifying activity sources that are affected by unauthorized activities includes identifying data stream incoming from outside the computer system.

17. (Original) The method of claim 1, further comprising determining an activity status for the stored events, the activity status comprising one of:

a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and

an incomplete status, which represents that the source of unauthorized activities is not identified, or at least one activity target in the stored activities is not associated with the source through one or more associations.

18. (Original) The method of claim 1, further comprising determining an activity level representing a frequency of unauthorized activities on the virtual machine during a predefined time interval.

19. (Original) A system, comprising:

one or more processors; and

memory storing:

a virtual machine;

a virtual machine monitor supervising the virtual machine; and

one or more programs, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

IPR2025-00069
CrowdStrike EX1002 Page 323

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

20. (Previously Presented) A non-transitory computer readable storage medium, including one or more programs for execution by one or more processors of a computer system, the one or more programs including instructions for:

monitoring activity on the virtual machine;

identifying a plurality of activities being performed at the virtual machine, where each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;

storing in the memory the activity sources, activity targets, and associations;

creating, from the stored activities, a fingerprint indicative of the activity on the virtual machine; and

transmitting the fingerprint to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.

21. (New) The method of claim 1, wherein an activity target of a first activity of the plurality of activities is an activity source of a second activity of the plurality of activities.

22. (New) The method of claim 1, further comprising:

identifying a type of the association between the activity source and the activity target.

23. (New) The method of claim 1, further comprising:

identifying a respective activity as unauthorized based on a determination that the respective activity is associated with an unauthorized activity that is distinct from the respective activity.

IPR2025-00069
CrowdStrike EX1002 Page 324

REMARKS

This amendment responds to the office action mailed August 15, 2014. In the office action, the Examiner:

A. rejected claims 1-20 under 35 U.S.C. 103(a) over Jiang (US 2008/0320594) and Aziz et al (US 2012/0331553).

INTERVIEW SUMMARY

The Applicant's attorneys thank Examiner Nguyen for her comments during a telephone interview on September 15, 2014 with the Applicant's attorney, Tae-Woong Koo. In the interview, distinctions between the cited references and the pending claims were discussed. No agreement was reached in terms of allowability of the pending claims.

OVERVIEW OF CHANGES TO THE SPECIFICATION AND CLAIMS

Claims 21-23 have been added. Support for the new claims can be found in at least paragraphs [0066]-[0068], [0072], [0080], and [0083] of the specification as originally filed. No new matter has been added.

With respect to all amendments, the Applicant has not dedicated or abandoned any unclaimed subject matter. Moreover, the Applicant has not acquiesced to any characterizations of the invention, nor any rejections or objections of the claims, made by the Examiner.

After entry of this amendment, the pending claims are: claims 1-23.

ARGUMENT

Claim Rejections - 35 U.S.C. § 103

The Examiner has rejected claims 1-20 under 35 U.S.C. 103(a) over Jiang and Aziz. This set of claims contains 3 independent claims, namely claims 1, 19 and 20.

To establish prima facie obviousness of a claimed invention, all the claim elements must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Indeed, the Board of Patent Appeal and Interferences confirmed that a proper obviousness determination requires an Examiner to make "a searching comparison of the claimed invention - including all its limitations - with the teaching of the prior art." See *In re Wada and Murphy*, Appeal 2007-3733, citing *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir.

IPR2025-00069
CrowdStrike EX1002 Page 325

1995) (emphasis in original). Finding all the claim elements in the prior art is necessary, but not sufficient. *KSR Intern. Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1741 (2007) ("a patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art"). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970).

The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, and (3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18 (1966); *see also KSR Int'l Co. V. Teleflex Inc.*, 550 U.S. 398, 399 (2007). "Section 103 forbids issuance of a patent when the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." *KSR*, at 2 (internal quotations omitted). Thus, to be patentable, the differences between the claimed subject matter and the prior art must be substantial enough to not be obvious to a person of ordinary skill in the art.

A. Rejection of claims 1-20 under 35 U.S.C. 103(a) over Jiang and Aziz

(a) The combination of Jiang and Aziz does not teach or suggest "identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target" as recited in claims 1 and 19-20

Independent claims 1 and 19-20 recite:

> identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an **activity source**, an **activity target**, and an **association between the activity source and the activity target**.

As explained in paragraphs [0007] and [0013] of this application, zero-day attacks are a critical threat to computer networks, and the above-recited features are important in dealing with such zero-day attacks.

> [0007] A critical threat to computer networks is the so-called zero-day attack that exploits security vulnerabilities previously unknown to software developers or system operators. Because the security vulnerabilities are unknown to the software developers or system operators, often the fingerprints of such zero-day attacks are

IPR2025-00069
CrowdStrike EX1002 Page 326

> unavailable for comparison. Until the fingerprints are identified, attacks exploiting the same security vulnerabilities continue without detection by the network security systems. However, identifying the fingerprints of malicious activities in the middle of numerous other non-malicious processes is not a trivial task.
>
> [0013] These embodiments identify unauthorized activities by monitoring and identifying associations between activity sources and activity targets without using pre-determined fingerprints. The data collected by these embodiments can be used to generate fingerprint data in response to the zero-day attacks.

Following the guidelines set by the Supreme Court in *KSR,* one first determines the scope and content of the prior art. Jiang teaches a malware detector, while Aziz teaches a dynamic signature creation and enforcement system configured to analyze network data. However, neither Jiang nor Aziz, either alone or in combination, teach or suggest "identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an **activity source**, an **activity target**, and an **association between the activity source and the activity target**," as required by claims 1 and 19-20.

With respect to the above-recited features, the Examiner states:

> Jiang teaches ... identifying a plurality of activities being performed at the virtual machine, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target (par. 0035, 0048-0050, 0059-0061).[1]

However, paragraphs [0035], [0048]-[0050] and [0059]-[0061] of Jiang, cited by the Examiner, state (emphasis added):

> [0035] ... The open-source VMMs (QEMU, Xen, and UML) allow full access to low-level VM states and events. ...
>
> [0048] ... the instructions may further include, as shown in FIG. 2, retrieving for inspection virtual machine internal system events from the virtual resources S210. ... The virtual machine internal system events may comprise virtual memory events and/or virtual disk events.
>
> [0049] ... the instructions further include interpreting the **virtual memory events** and/or **virtual disk events** S220. After interpretation, the instructions may further include transparently encapsulating and presenting the interpreted virtual memory events and/or the interpreted virtual disk events to the anti-malware software S230.
>
> [0050] Interpreting either or both these types of events also help enable guest function extrapolation. Just as with the virtual machine internal system states, extrapolation can aid in extracting semantic-rich data ... from the virtual machine internal system events.

[1] Office action dated 10-25-2013, p. 3.

IPR2025-00069
CrowdStrike EX1002 Page 327

> [0059] Not only can the malware detection system 305 retrieve, interpret, and transparently encapsulate and present virtual machine internal system states, but it can also do the same for **virtual machine internal system events**. Such events can be retrieved from the virtual resources 340 for inspection. Retrieval of these events is also based on non-intrusive virtual machine introspection without perturbing their execution. The **virtual machine internal system events** may comprise **virtual memory events** ... and **virtual disk events** ....
>
> [0060] The malware detection system 305 may use the virtual machine inspector 362 may be configured to retrieve the virtual memory events from a virtual machine monitor .... Generally running between the host operating system ... and the virtual machine ..., the virtual machine monitor ... may be configured to intercept the virtual memory events. Upon interception, the guest function extrapolator 364 may extract semantic-rich data by interpreting the virtual memory events. Afterwards, the transparent presenter 366 may encapsulate and present the interpreted virtual memory events to the anti-malware software. Like above, the anti-malware software ... may be configured to use the virtual memory events to detect system compromises.
>
> [0061] Similarly, the malware detection system 305 may also use the virtual machine inspector 362 to retrieve the virtual disk events from a virtual machine monitor .... The virtual machine monitor ..., running between the host operating system ... and the virtual machine ... may be configured to intercept the virtual disk events. After interception, the guest function extrapolator 364 may extract semantic-rich data by interpreting the virtual disk events. Then, the transparent presenter 366 may encapsulate and present the interpreted virtual disk events to the anti-malware software ... for detecting any system comprise.

As shown above, paragraphs [0035], [0048]-[0050] and [0059]-[0061] of Jiang describe a malware detection system that detects virtual memory events and virtual disk events. These detected events in Jiang are interrupt, memory, and I/O access events.[2] Even if these events were targets, which they are not, Jiang simply does not disclose all of "an activity **source**, an activity **target**, and an **association between the activity source and the activity target**." As such, Jiang simply does not teach or even suggest the above-recited features. Aziz is not cited for, nor does it teach or suggest the above-recited features. This same argument was discussed with the Examiner during the telephone interview on January 23, 2014, and the Examiner agreed and allowed this application on May 1, 2014. Thus, the Applicant respectfully requests that the rejection of claims 1, 19, and 20 and their dependent claims be withdrawn.

[2] *See* paragraph [0067] of Jiang.

IPR2025-00069
CrowdStrike EX1002 Page 328

Claims 2-18 depends on independent claim 1 and thus include all the limitations in claim 1. As discussed above, Jiang and Aziz do not teach or suggest every limitation of independent claim 1. Because Jiang and Aziz, either alone or in combination, do not teach or suggest each and every claim limitation, it is respectfully submitted that independent claims 1, 19, and 20, and associated dependent claims 2-18, are patentable over the cited references.

New claims 21-23 are also patentable over the combination of Jiang and Aziz. The Applicant respectfully requests that the Examiner consider claims 21-23 with a view toward allowance.

CONCLUSION

In view of the foregoing, it is respectfully submitted that the application is now in a condition for allowance. However, should the Examiner believe that the claims are not in condition for allowance, the Applicant requests an Examiner Interview. The Examiner may contact the undersigned attorney at dbregman@morganlewis.com or 650.843.7519 to arrange a suitable time for the interview.

Respectfully submitted,

Date: January 15, 2015

45,645
Dion M. Bregman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, California 94306
(650) 843-4000

IPR2025-00069
CrowdStrike EX1002 Page 329

Electronic Patent Application Fee Transmittal

Application Number:	13163590
Filing Date:	17-Jun-2011
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Dion M. Bregman/Beverly Gemello
Attorney Docket Number:	067292-5005-US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	3	40	120
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Extension - 2 months with $0 paid	2252	1	300	300
Miscellaneous:				
			Total in USD ($)	**420**

Electronic Acknowledgement Receipt

EFS ID:	21225942
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Beverly Gemello
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	15-JAN-2015
Filing Date:	17-JUN-2011
Time Stamp:	20:43:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$420
RAM confirmation Number	6855
Deposit Account	500310
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		67292-5005_ResponseToOA.pdf	481048 b2f0a36516b246cd03f52793dc862e67ac3189b7	yes	10

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Specification	2	5
Applicant Arguments/Remarks Made in an Amendment	6	10

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	32236 bb6812bfa1f5e45d81dea090444b8ab72cb647ff	no	2

Warnings:

Information:

Total Files Size (in bytes):	513284

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/163,590	Filing Date 06/17/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **01/15/2015**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 23	Minus	** 20	= 3	X $40 =	120
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	**120**

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/NICOLE C. LAWRENCE/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 04/10/2015

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER
NGUYEN, THU HA T

ART UNIT	PAPER NUMBER
2453	

DATE MAILED: 04/10/2015

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

TITLE OF INVENTION: System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/10/2015

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

IPR2025-00069
CrowdStrike EX1002 Page 335

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 04/10/2015
MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

TITLE OF INVENTION: System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0	$0	$480	07/10/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
NGUYEN, THU HA T	2453	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ❑ Issue Fee
- ❑ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ❑ The director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ❑ Applicant certifying micro entity status. See 37 CFR 1.29 — NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
- ❑ Applicant asserting small entity status. See 37 CFR 1.27 — NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
- ❑ Applicant changing to regular undiscounted fee status. — NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

IPR2025-00069
CrowdStrike EX1002 Page 336

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

24341 7590 04/10/2015

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2453	

DATE MAILED: 04/10/2015

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

IPR2025-00069
CrowdStrike EX1002 Page 337

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/163,590	Applicant(s) CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *01/15/15*.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on_____.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-23*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 09/12/14
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/THU HA NGUYEN/
Primary Examiner, Art Unit 2453

Notice of References Cited	Application/Control No. 13/163,590	Applicant(s)/Patent Under Reexamination CAPALIK ET AL.	
	Examiner THU HA NGUYEN	Art Unit 2453	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2008/0222729 A1	09-2008	Chen et al.	726/24
*	B	US-7,581,219 B2	08-2009	Neiger et al.	718/1
*	C	US-7,596,654 B1	09-2009	Wong, Kai C.	711/6
*	D	US-2012/0255018 A1	10-2012	Sallam, Ahmed Said	726/24
*	E	US-2012/0255012 A1	10-2012	Sallam, Ahmed Said	726/24
*	F	US-8,365,180 B2	01-2013	Kawasaki et al.	718/104
*	G	US-8,448,170 B2	05-2013	Wipfel et al.	718/1
*	H	US-2013/0238785 A1	09-2013	Hawk et al.	709/224
*	I	US-2013/0304903 A1	11-2013	Mick et al.	709/224
*	J	US-2014/0096131 A1	04-2014	Sonnek et al.	718/1
*	K	US-8,776,050 B2	07-2014	Plouffe et al.	718/1
*	L	US-8,943,506 B2	01-2015	Tang et al.	718/100
*	M	US-8,949,826 B2	02-2015	Fitzgerald et al.	718/1

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	21	CAPALIK-ALEN.inv.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/04/02 23:29
L2	17	CAPALIK-ALEN.inv. and virtual$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/04/02 23:30
L3	11	CAPALIK-ALEN.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/04/02 23:34
L4	7	ANDREWS-DAVID.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/04/02 23:45
L5	4	BECKER-BEN.inv. and virtual$4 and monitor$4	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/04/02 23:47
L6	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L7	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L8	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L9	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L10	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53

IPR2025-00069
CrowdStrike EX1002 Page 341

L11	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L12	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L13	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L14	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L15	111	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L16	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L17	14	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L18	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L19	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L20	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L21	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L22	82	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L23	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53

		or map$4) and prevent$4 and attack$4 and 726/25.ccls.				
L24	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L25	24	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L26	7	("20010011254" | "20020194437" | "20040153672" | "20040177269" | "20070240221" | "20080127114" | "20100095281" | "5621886" | "5740413" | "6343280" | "6446062" | "7996836").PN. and (virtual adj machine$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L27	2	"20050136570".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L28	2	"20050136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L29	2	"20060136725".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L30	2	"20060136720".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L31	5	"2007000689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L32	2	"20070002689".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L33	2	"20060294592".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L34	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L35	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and figureprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L36	111	monitor$4 same ((virtual adj machine$4) or VM or VMM) same	US-PGPUB; USPAT; EPO;	OR	OFF	2015/04/02 23:53

		(activit$4 or event$4) and source and target$4 and fingerprint$4	JPO; DERWENT			
L37	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same source same target$4 same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L38	14	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L39	3	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 same decoy$4 same unauthor$6	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L40	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L41	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 same attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L42	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L43	82	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L44	11	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 726/25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L45	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and fingerprint$4 and auth$9 and (compar$4 or match$4 or map$4) and prevent$4 and attack$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L46	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L47	9011	718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L48	1	L46 and L47	US-PGPUB; USPAT; EPO; JPO;	OR	OFF	2015/04/02 23:53

			DERWENT			
L49	6456	718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L50	0	L46 and L49	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L51	1	L43 and L49	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L52	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "7263".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L53	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and "726/3".ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L54	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/3.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L55	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/14-15.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L56	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/24-26.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L57	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/22.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L58	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and (finger adj print$4) and auth$9 and (compar$4 or match$4 or map$4) and 726/11.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L59	211	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L60	12	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L61	90	monitor$4 same ((virtual adj	US-PGPUB;	OR	OFF	2015/04/02

		machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	USPAT; EPO; JPO; DERWENT			23:53
L62	9011	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L63	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same associat$6 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L64	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/1.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L65	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 same auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L66	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$7 same fingerprint$4 and 718/100.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L67	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L78	2	"20080320594".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/04/02 23:53
L79	2	"20120331553".did.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2015/04/02 23:53
L80	2	"20120331553".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L81	2	"20080320594".did.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L82	23	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/554.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L83	17	monitor$4 same ((virtual adj machine$4) or VM or VMM) same	US-PGPUB; USPAT; EPO;	OR	OFF	2015/04/02 23:53

		(activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/56.cpc.	JPO; DERWENT			
L84	18	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/566.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L85	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/51.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L86	5	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/52.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L87	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L88	30	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L89	22	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53
L90	39	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and 726/22-25.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2015/04/02 23:53

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L68	20	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and (finger adj print$4)	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L69	6152	718/1.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L70	5044	718/100.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L71	12	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 718/100.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53

IPR2025-00069
CrowdStrike EX1002 Page 347

L72	4	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 709/223-224.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L73	0	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/155.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L74	2	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and auth$4 and 713/164-165.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L75	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L76	90	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and 709/223-224.ccls.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L77	112	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/02 23:53
L91	30	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/145.cpc.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/03 00:00
L92	21	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and H04L63/1491.cpc.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/03 00:01
L93	1	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) and source and target$4 and fingerprint$4 and G06F21/50.cpc.	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/03 00:03
L94	6	monitor$4 same ((virtual adj machine$4) or VM or VMM) same (activit$4 or event$4) same fingerprint$4 and auth$9 and prevent$4 same attack$4	US-PGPUB; USPAT; UPAD	OR	OFF	2015/04/03 00:03

4/3/2015 12:05:39 AM
C:\Users\tnguyen39\Documents\EAST\Workspaces\13163590.wsp

IPR2025-00069
CrowdStrike EX1002 Page 348

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

CPC						
Symbol					**Type**	**Version**
H04L		63	/	1491	F	2013-01-01
H04L		63	/	1416	I	2013-01-01
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			
			/			

CPC Combination Sets							
Symbol					**Type**	**Set**	**Ranking**	**Version**
			/					
			/					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	23	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2453	04/01/15	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	SUBCLASS	CLAIMED	NON-CLAIMED
726	25	G 0 6 F 11 / 00 (2006.01.01)	

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
726	3	14	15	24	25
709	223	224			
713	155	164	165		
718	1	100			

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	23	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2453	04/01/15	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	2

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	**Art Unit**
	THU HA NGUYEN	2453

☒ **Claims renumbered in the same order as presented by applicant** ☐ **CPA** ☐ **T.D.** ☐ **R.1.47**

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		17												
	2		18												
	3		19												
	4		20												
	5		21												
	6		22												
	7		23												
	8														
	9														
	10														
	11														
	12														
	13														
	14														
	15														
	16														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 23	
/THU HA NGUYEN/ Primary Examiner.Art Unit 2453 (Primary Examiner)	04/01/15 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 2

IPR2025-00069
CrowdStrike EX1002 Page 351

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				Electronically filed September 12, 2014	
				Application Number	13/163,590
				Filing Date	June 17, 2011
				First Named Inventor	Alen Capalik
				Art Unit	2453
				Examiner Name	Nguyen, Thu Ha T.
Sheet	1	of	1	Attorney Docket Number	067292-5005-US

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		NeuralIQ Inc., Extended European Search Report, 08745858-4, 12JUN2014, 4 pgs

Examiner Signature	/Thu Ha Nguyen/	Date Considered	04/03/2015

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/
IPR2025-00069
CrowdStrike EX1002 Page 352

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13163590	CAPALIK ET AL.
	Examiner	Art Unit
	THU HA NGUYEN	2453

CPC- SEARCHED		
Symbol	Date	Examiner
G06F21/50-52, 21/56, 554, 566	08/11/14	THN
H04L63/145, 1491	08/11/14	THN
Update search	04/01/15	THN
H04L63/1416	04/01/15	THN
G06F21/50	04/01/15	THN

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	155, 164	09/14/13	THN
726	3, 14, 24	09/14/13	THN
Update search		04/06/14	THN
709	223, 224	04/06/14	THN
726	3, 14-15, 22, 24-26	04/06/14	THN
718	1, 100	04/06/14	THN
713	155, 164, 165	04/06/14	THN
726	22-25	08/11/14	THN
Update search		04/01/15	THN

SEARCH NOTES		
Search Notes	Date	Examiner
East, Derwent, JPO, EPO, USPG-Pub search	09/14/13	THN
Inventor name, assignee name search	09/14/13	THN
Update search	04/06/14	THN
East, Derwent, JPO, EPO, USPG-Pub search	04/06/14	THN
Inventor name, assignee name search	04/06/14	THN

IPR2025-00069
CrowdStrike EX1002 Page 353

SEARCH NOTES		
Search Notes	**Date**	**Examiner**
NPL, Google search	04/06/14	THN
Update search	08/11/14	THN
Conduct inventor name search	04/01/15	THN
East keywords, class/subclass search	04/01/15	THN

INTERFERENCE SEARCH			
US Class/ CPC Symbol	**US Subclass / CPC Group**	**Date**	**Examiner**
726	3, 14, 15, 24, 25	04/01/15	THN
709	223, 224	04/01/15	THN
713	155, 164, 165	04/01/15	THN
718	1, 100	04/01/15	THN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 1008

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/163,590	06/17/2011	726	2453	067292-5005-US

APPLICANTS

INVENTORS

Alen Capalik, Pacific Palisades, CA;
David Andrews, Los angeles, CA;
Ben Becker, Santa Monica, CA;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/358,367 06/24/2010

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **

06/29/2011

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /THU HA T NGUYEN/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		CA	17	20	3

ADDRESS

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306
UNITED STATES

TITLE

System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

FILING FEE RECEIVED		
582	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

IPR2025-00069
CrowdStrike EX1002 Page 355

Electronically filed: May 1, 2015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

AMENDMENT UNDER 37 CFR § 1.312

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This application was allowed on April 10, 2015. Please amend the application as set forth on the following pages.

Amendments to the Specification begin on page 2.

Remarks begin on page 3.

IPR2025-00069
CrowdStrike EX1002 Page 356

Amendments to the Specification

Please amend paragraph [0002] of the specification as follows:

Markup copy:

[0002] This relates to U.S. Patent Application No. [[____,]] 13/163,578, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States" filed concurrently herewith, which claims priority to U.S. Provisional Application Serial No. 61/358,363 filed on June 24, 2010, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States," both of which are incorporated by reference herein.

Clean copy:

[0002] This relates to U.S. Patent Application No. 13/163,578, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States" filed concurrently herewith, which claims priority to U.S. Provisional Application Serial No. 61/358,363 filed on June 24, 2010, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States," both of which are incorporated by reference herein.

IPR2025-00069
CrowdStrike EX1002 Page 357

REMARKS

Paragraph [0002] has been amended to replace a placeholder with an appropriate patent application number. No new matter has been added.

Although no fee is believed to be due, the Commissioner is hereby authorized to charge any fees associated with this paper communication or credit any overpayment to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US).

Respectfully submitted,

Date: May 1, 2015

/ Tae-Woong Koo / 59,649

Tae-Woong Koo (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, California 94306
(650) 843-4000

IPR2025-00069
CrowdStrike EX1002 Page 358

Electronically filed May 1, 2015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	Capalik et al.	Confirmation No.:	1008
Serial No.:	13/163,590	Art Unit:	2453
Filed:	June 17, 2011	Examiner:	Nguyen, Thu Ha T.
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No.:	067292-5005-US

INFORMATION DISCLOSURE STATEMENT SUBMITTED UNDER 37 C.F.R. § 1.97(i)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the duty of disclosure provisions of 37 C.F.R. §1.56, there is hereby provided certain information that the applicant considers cumulative with respect to references already of record in the subject U.S. patent application or otherwise not material to the examination of the application. It is requested that the references cited herein be made of record in the application in accordance with rule 37 C.F.R. §1.97(i).

1. Enclosures accompanying this Information Disclosure Statement are:

1a. ☒ A list of all patents, publications, applications, or other information submitted for consideration by the office.

1b. A legible copy of :

☐ Each foreign patent;

☐ Each publication or that portion which caused it to be listed on the PTO-1449;

☐ For each cited pending U.S. application, the application specification including the claims, and any drawing of the application, or portion of the application which caused it to be listed on the PTO-1449 including any claims directed to that portion;

☒ all other information or portion which caused it to be listed on the PTO-1449.

1c. ☐ An English language copy of search report(s) from a counterpart foreign application or PCT International Search Report.

1d. ☐ Explanations of relevancy (ATTACHMENT 1(d), hereto) or English language abstracts of the non-English language publications.

2. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(b):

IPR2025-00069
CrowdStrike EX1002 Page 359

☐ Within three months of the filing date of a national application other than a continued prosecution application under §1.53(d);

☐ Within three months of the date of entry of the national stage as set forth in §1.491 in an international application;

☐ Before the mailing of the first Office action on the merits;

☐ Before the mailing of a first Office action after the filing of a request for continued examination under §1.114.

3. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(c) after the period specified in 37 C.F.R. §1.97(b), but before the mailing date of any of a final action under 37 C.F.R. §1.113, a notice of allowance under 37 C.F.R. §1.311 or an action that otherwise closes prosecution in the application.

(Check either Item 3a, 3b or 3c)

3a. ☐ The Certification Statement in Item 5 below is applicable. Accordingly, no fee is required.

3b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

3c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

(Items 3b or 3c to be checked if any reference known for more than 3 months)

4. ☐ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(d) after the period specified in 37 C.F.R. §1.97(c), but on or before the date of payment of the issue fee.

(Check either Item 4a and 4b or 4c)

4a. ☐ The Certification Statement in Item 5 below is applicable.

4b. ☐ The $180.00 (large entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

4c. ☐ The $90.00 (small entity) fee set forth in 37 C.F.R. §1.17(p) in accordance with 37 C.F.R. §1.97(c) is to be charged to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no.).

5. ☒ This Information Disclosure Statement is filed under 37 C.F.R. §1.97(i) as it does not comply with § 1.97(a)-(d), Applicants request that this Information Disclosure Statement be placed in the file by the office.

6. ☐ Copies of each cited U.S. patent and each U.S. patent application publication are not enclosed pursuant to the USPTO OG Notice dated 05 August 2003 waiving the requirement under 37 C.F.R. 1.98(a)(2)(i) for U.S. patent applications filed after June 30, 2003.

7. ☐ This application is a continuation application under 37 C.F.R. §1.53(b) or (d).

(Check appropriate Items 7a, 7b and/or 7c)

7a. ☐ A Petition to Withdraw from issue under 37 C.F.R. §1.313(b)(5) is concurrently filed herewith.

7b. ☐ Copies of publications listed on Form PTO-1449 from prior application Serial No. , filed on , of which this application claims priority under 35 U.S.C. §120, are not being submitted pursuant to 37 C.F.R. §1.98(d).

7c. ☐ Copies of the publications listed on Form PTO-1449 were not previously cited in prior application Serial No. , filed on , and are provided herewith.

8. ☐ This is a Supplemental Information Disclosure Statement. (Check Item 8a)

8a. ☐ This Supplemental Information Disclosure Statement under 37 C.F.R. §1.97(f) supplements the Information Disclosure Statement filed on . A bona fide attempt was made to comply with 37 C.F.R. §1.98, but inadvertent omissions were made. These omissions have been corrected herein. Accordingly, additional time is requested so that this Supplemental Information Disclosure Statement can be considered as if properly filed on .

9. ☐ In accordance with 37 C.F.R. §1.98, a concise explanation of what is presently understood to be the relevance of each non-English language publication is:

(Check Item 9a, 9b, or 9c)

9a. ☐ satisfied because all non-English language publications were cited on the enclosed English language copy of the PCT International Search Report or the search report from a counterpart foreign application indicating the degree of relevance found by the foreign office.

9b. ☐ set forth in the application.

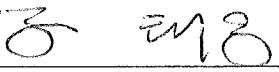
9c. ☐ enclosed as an attachment hereto.

10. ☒ The Commissioner is authorized to charge any additional fee required or credit any overpayment for this Information Disclosure Statement and/or Petition to Morgan, Lewis & Bockius LLP Deposit Account No. 50-0310 (order no. 067292-5005-US).

11. ☒ No admission is made that the information cited in this Statement is, or is considered to be, material to patentability nor a representation that a search has been made (other than a search report of a foreign counterpart application or PCT International Search Report if submitted herewith). 37 C.F.R. §§1.97(g) and (h).

Respectfully submitted,

Date: May 1, 2015



59,649 (Reg. No.)

Tae-Woong Koo
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed May 1, 2015*	
				Application Number	*13/163,590*
				Filing Date	*June 17, 2011*
				First Named Inventor	*Alen Capalik*
				Art Unit	*2453*
				Examiner Name	*Nguyen, Thu Ha T*
Sheet	1	of	1	Attorney Docket Number	*067292-5005-US*

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		Capalik, Final Office Action, US 11/788,795, 14AUG2014, 18 pgs.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Electronic Acknowledgement Receipt

EFS ID:	22233069
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Tae-Woong Koo/Edith Fuentes
Filer Authorized By:	Tae-Woong Koo
Attorney Docket Number:	067292-5005-US
Receipt Date:	01-MAY-2015
Filing Date:	17-JUN-2011
Time Stamp:	18:02:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		067292-5005US_Amendment-Rule312.pdf	70785 e9ffb32ce3772aad8d9dc467644e2e6a72b0db46	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment after Notice of Allowance (Rule 312)	1	1
	Specification	2	2
	Applicant Arguments/Remarks Made in an Amendment	3	3

Warnings:					
Information:					
2		067292-5005US_197i-IDS.pdf	189029 94b1637aa4f10e5c1d7f26c4a852262c3f480a5d	yes	4

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Transmittal Letter	1	3
	Information Disclosure Statement (IDS) Form (SB08)	4	4

Warnings:					
Information:					
3	Other Reference-Patent/App/Search documents	Capalik_Final-Office-Action-11788795_081414.pdf	613968 ed2469f959d706563970e928db9f7f9fce5b7306	no	18

Warnings:	
Information:	
Total Files Size (in bytes):	873782

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

Electronically filed: May 5, 2015

Complete and send this form with applicable fee(s), to: Mail — Mail Stop ISSUE FEE, Commissioner of Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450

or Fax — (703) 746-4000

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advanced orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS

MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306

Note: A certificate of mailing below can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing.

Certificate of Mailing

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (703) 746-4000, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

TITLE OF INVENTION: SYSTEM AND METHOD FOR IDENTIFYING UNAUTHORIZED ACTIVITIES ON A COMPUTER SYSTEM USING A DATA STRUCTURE MODEL

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	TOTAL FEE(S) DUE	DATE DUE
Nonprovisional	SMALL	$480	$0	$480	07/10/2015

EXAMINER	ART UNIT	CLASS-SUBCLASS
Nguyen, Thu Ha T.	2453	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed

1. **Morgan, Lewis & Bockius LLP**
2.
3.

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGN: NeuralIQ, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Santa Monica, California

Please check the appropriate assignee category or categories (will not be printed on the patent) ☐ Individual ☒ corporation or other private group entity ☐ government

4a. The following fee(s) are enclosed:

☒ Issue Fee

☐ Publication Fee

☐ Advanced Order - # of Copies ____

4b. Payment of Fee(s):

☐ A check in the amount of the fee(s) enclosed

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director has been authorized through the electronic filing system to charge any additional fee(s), or credit any overpayment associated with this communication to Deposit Account Number 50-0310 (order no.: 067292-5005-US)

5. **Change in Small Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

The Director of the USPTO is requested to apply the Issue Fee and Publication Fee (if any) or to re-apply any previously paid issue fee to the application identified above.
NOTE; The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the Patent and Trademark Office.

Authorized Signature — Date: May 5, 2015

Printed Name: Dion M. Bregman — Registration No. 45,645

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Electronic Patent Application Fee Transmittal

Application Number:	13163590
Filing Date:	17-Jun-2011
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Dion M. Bregman/Sherri Ballbach
Attorney Docket Number:	067292-5005-US

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**480**

Electronic Acknowledgement Receipt

EFS ID:	22264435
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/Sherri Ballbach
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	05-MAY-2015
Filing Date:	17-JUN-2011
Time Stamp:	19:27:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$480
RAM confirmation Number	5302
Deposit Account	500310
Authorized User	BREGMAN, DION

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	067292-5005-US_PartBFeeTransmittal.pdf	106649 dca9df8c69093a6d1d246ddad861a8519228a616	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30540 10d50dcfefcb3d1ae68435aebd8cb2a6d79f29fa	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	137189		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

7590 05/06/2015

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER	
NGUYEN, THU HA T	

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
05/06/2015	ELECTRONIC

NOTICE OF NON-COMPLIANT INFORMATION DISCLOSURE STATEMENT

An Information Disclosure Statement (IDS) filed 05-01-15 in the above-identified application fails to meet the requirements of 37 CFR 1.97(d) for the reason(s) specified below. Accordingly, the IDS will be placed in the file, but the information referred to therein has not been considered.

The IDS is not compliant with 37 CFR 1.97(d) because:

☒ The IDS lacks a statement as specified in 37 CFR 1.97(e).

☐ The IDS lacks the fee set forth in 37 CFR 1.17(p).

☐ The IDS was filed after the issue fee was paid. Applicant may wish to consider filing a petition to withdraw the application from issue under 37 CFR 1.313(c) to have the IDS considered. See MPEP 1308.

571-272-4200 or 1-888-786-0101
Application Assistance Unit
Office of Data Management

FORM PTOM327-B (Rev. 02/08)

IPR2025-00069
CrowdStrike EX1002 Page 370

INFORMATION DISCLOSURE CITATION Substitute for Form 1449-PTO				*Electronically filed May 1, 2015*	
				Application Number	*13/163,590*
				Filing Date	*June 17, 2011*
				First Named Inventor	*Alen Capalik*
				Art Unit	*2453*
				Examiner Name	*Nguyen, Thu Ha T*
Sheet	1	of	1	Attorney Docket Number	*067292-5005-US*

NON PATENT LITERATURE DOCUMENTS		
Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		~~Capalik, Final Office Action, US 14/708,795, 14AUG2014, 18 pgs.~~

/Thu Ha Nguyen/

05/07/2015

Non-compliant
IDS.

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kind Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TN/

IPR2025-00069
CrowdStrike EX1002 Page 371

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

24341 7590 05/14/2015

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER
NGUYEN, THU HA T

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
05/14/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address : COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
13/163,590	17 June, 2011	CAPALIK ET AL.	067292-5005-US

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER	
THU HA NGUYEN	
ART UNIT	PAPER
2453	20150507

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

IDS filed 05/04/15 will be placed in the file but has not been considered by the examiner.

/THU HA NGUYEN/
Primary Examiner, Art Unit 2453

PTO-90C (Rev.04-03)

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

24341 7590 07/14/2015

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

EXAMINER
NGUYEN, THU HA T

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
07/14/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

Response to Rule 312 Communication	Application No. 13/163,590	Applicant(s)
	Examiner	Art Unit

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. ☒ The amendment filed on *01 May 2015* under 37 CFR 1.312 has been considered, and has been:

a) ☒ entered.

b) ☐ entered as directed to matters of form not affecting the scope of the invention.

c) ☐ disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.

d) ☐ disapproved. See explanation below.

e) ☐ entered in part. See explanation below.

/ A. Marty Willis /

A. Marty Willis

Publishing Division

Office of Data Management

IPR2025-00069
CrowdStrike EX1002 Page 375

Change(s) applied
to document,
/D.H.P./
6/21/2014

System and Method for Identifying Unauthorized Activities on a Computer System using a Data Structure Model

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Provisional Application Serial No. 61/358, 367, entitled "System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model" filed on June 24, 2010, which is incorporated by reference herein.

[0002] This relates to U.S. Patent Application No. 13/163578, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States" filed concurrently herewith, which claims priority to U.S. Provisional Application Serial No. 61/358,363 filed on June 24, 2010, entitled "System and Method for Sampling Forensic Data of Unauthorized Activities Using Executability States," both of which are incorporated by reference herein.

[0003] This application relates to U.S. Patent Application No. 11/788,795, entitled "System and Method for Analyzing Unauthorized Intrusion into a Computer Network," filed on April 20, 2007, which is a continuation-in-part of U.S. Patent Application No. 11/488,743, entitled "Decoy Network Technology With Automatic Signature Generation for Intrusion Detection and Intrusion Prevention Systems," filed on July 17, 2006, both of which are incorporated herein by reference in their entireties.

TECHNICAL FIELD

[0004] This invention relates generally to systems and methods for protecting computer networks, including but not limited to systems and methods for analyzing malicious activities on a computer system in order to better protect the computer system from future malicious activity.

BACKGROUND

[0005] An increasing number of computers are connected to computer networks (e.g., the Internet). Networked computers provide a significant benefit of accessing and sharing data over the networks. However, these networked computers are also vulnerable to attacks, unwanted intrusions, and unauthorized access.

IPR2025-00069
CrowdStrike EX1002 Page 376

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	08/11/2015	9106697	067292-5005-US	1008

24341 7590 07/22/2015

MORGAN, LEWIS & BOCKIUS LLP (PA)
2 PALO ALTO SQUARE
3000 EL CAMINO REAL, SUITE 700
PALO ALTO, CA 94306

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 491 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Alen Capalik, Pacific Palisades, CA;
David Andrews, Los angeles, CA;
Ben Becker, Santa Monica, CA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

Electronically filed October 28, 2015

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent:	Capalik et al.	Confirmation No.:	1008
Patent No.:	9,106,697 B2	Serial No.:	13/163,590
Issued:	August 11, 2015	Filed:	June 17, 2011
For:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model	Attorney Docket No:	067292-5005-US

REQUEST FOR CERTIFICATE OF CORRECTION

Certificate of Corrections Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Request for Certificate of Correction is filed under 37 CFR 3.81 (b). Upon review of the subject patent, Patentee's attorney discovered 1 error on the part of the Applicant in the (73) Assignee field of the bibliography page. The assignment was submitted for recordation on July 7, 2015, before issuance of the patent. Patentee's attorney requests correction of the issued patent. A Form PTO 1050 Certificate of Correction is enclosed.

The Commissioner is authorized to charge the required fees to our Deposit Account No. 50-0310 (order no. 067292-5005-US).

Respectfully submitted,

Date: October 28, 2015 45,645

Dion M. Bregman (Reg. No.)
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, California 94306
(650) 843-4000

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO.	:	9,106,697 B2
APPLICATION NO.	:	13/163,590
ISSUE DATE	:	August 11, 2015
INVENTOR(S)	:	Capalik et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Bibliography page, (73) Assignee, please delete "NeuralIQ, Inc." and insert --CounterTack, Inc.--.

MAILING ADDRESS OF SENDER:
MORGAN, LEWIS & BOCKIUS LLP
2 Palo Alto Square
3000 El Camino Real, Suite 700
Palo Alto, CA 94306
(650) 843-4000

IPR2025-00069
CrowdStrike EX1002 Page 379

Electronic Patent Application Fee Transmittal

Application Number:	13163590
Filing Date:	17-Jun-2011
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Filer:	Dion M. Bregman/deborah carney
Attorney Docket Number:	067292-5005-US

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
PROCESSING FEE, EXCEPT PROV. APPLS.	1830	1	140	140
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Certificate of Correction	1811	1	100	100
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**240**

Electronic Acknowledgement Receipt

EFS ID:	23913161
Application Number:	13163590
International Application Number:	
Confirmation Number:	1008
Title of Invention:	System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model
First Named Inventor/Applicant Name:	Alen Capalik
Customer Number:	24341
Filer:	Dion M. Bregman/deborah carney
Filer Authorized By:	Dion M. Bregman
Attorney Docket Number:	067292-5005-US
Receipt Date:	28-OCT-2015
Filing Date:	17-JUN-2011
Time Stamp:	11:51:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$240
RAM confirmation Number	13399
Deposit Account	500310
Authorized User	SKLIBA, VLADIMIR

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	067292-5005US_CertificateofCorrection.pdf	59976 ecf9fc416a3ddfab3b7ba602f7222d0752f3f91b	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32831 be6157acb3492cebb9fcc5b270a1f83d2444f3c7	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	92807		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/163,590	06/17/2011	Alen Capalik	067292-5005-US	1008

24341 7590 08/03/2016
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
NGUYEN, THU HA T

ART UNIT	PAPER NUMBER
2453	

NOTIFICATION DATE	DELIVERY MODE
08/03/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

padocketingdepartment@morganlewis.com
vskliba@morganlewis.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Patent No. 9,106,697	:	
Issue Date: August 11, 2015	:	
Application No. 13/163,590	:	ON PETITION
Filed: June 17, 2011	:	
Attorney Docket No. 067292-5005-US	:	

This is a decision on the petition filed October 28, 2015, which will be treated as a petition under 37 CFR 3.81(b) to correct the name of the assignee on the front page of the above-identified patent by way of a Certificate of Correction.

The petition is **GRANTED**.

The patent file is being forwarded to the Certificates of Correction Branch for issuance of the requested Certificate of Correction.

A courtesy copy of this decision is being mailed to the address noted on the petition. However, until otherwise instructed, all future correspondence regarding this application will be mailed solely to the address of record.

Telephone inquiries concerning this decision may be directed to the Kimberly Inabinet at (571) 272-4618. Inquiries regarding the issuance of a certificate of correction should be directed to the Certificate of Correction Branch at (703) 756-1814.

/Kimberly Inabinet/

Kimberly Inabinet
Paralegal Specialist
Office of Petitions

cc: Dion M. Bregman
Morgan, Lewis & Bockius, LLP
2 Palo Alto Square
3000 E. Camino Real, Suite 700
Palo Alto, CA 94306

Transmittal Communication on Petition	Application No. 13/163,590	Applicant/Patent Under Reexamination CAPALIK ET AL.	
	Deciding Official KIMBERLY INABINET	Office of Petitions OPET	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address. --

(ADDITIONAL PARTY'S CORRESPONDENCE ADDRESS)

Dion M. Bregman
Morgan, Lewis & Bockius, LLP
2 Palo Alto Square
3000 E. Camino Real, Suite 700
Palo Alto, CA 94306

Enclosed is a copy of the latest communication from the United States Patent and Trademark Office in the above-identified Application/Patent.

Office of Petitions: Routing Sheet



Application No. 13/163,590

This application is being forwarded to your office for further processing. A decision has been rendered on a petition filed in this application, as indicated below. For details of this decision, please see the document PET.OP.DEC filed on the same date as this document.

- [X] **GRANTED**
- [ ] **DISMISSED**
- [ ] **DENIED**

Office of Petitions: Decision Count Sheet

Mailing Month

Application No. 13163590

13163590

For US serial numbers: enter number only, no slashes or commas. Ex: 10123456

For PCT: enter "51+single digit of year of filing+last 5 numbers", Ex. for PCT/US05/12345, enter 51512345

Deciding Official: Kimberly Inabinet

Count (1) - Palm Credit 13/163,590

Decision: GRANT

FINANCE WORK NEEDED

☐ Select Check Box for YES

GRANT

Decision Type: 523 - 37 CFR 3.81(b) - ISSUE PATENT IN NAME OF ASS

523

Notes:

Count (2)

Decision: n/a

FINANCE WORK NEEDED

☐ Select Check Box for YES

Decision Type: NONE

Notes:

Count (3)

Decision: n/a

FINANCE WORK NEEDED

☐ Select Check Box for YES

Decision Type: NONE

Notes:

Initials of Approving Official (if required)

If more than 3 decisions, attach 2nd count sheet & mark this box ☐

Printed on: *7/30/2016*

Office of Petitions Internal Document - Ver. 5.0

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 9,106,697 B2
APPLICATION NO.	: 13/163590
DATED	: August 11, 2015
INVENTOR(S)	: Capalik et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the title page, item (73) Assignee, please delete "NeurallQ, Inc." and insert --CounterTack, Inc.--.

Signed and Sealed this
Sixth Day of September, 2016

Michelle K. Lee

Michelle K. Lee
Director of the United States Patent and Trademark Office

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
13/163,590	**12/14/2023 08:44:25 PM Z ET**	**067292-5005-US**

Title of Invention

System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	9106697
CONFIRMATION #	1008	FILED BY	Emily Aguilar
PATENT CENTER #	63623904	FILING DATE	06/17/2011
CUSTOMER #	24341	FIRST NAMED INVENTOR	Alen Capalik
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Kannan Narayanan

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
135973-5000 GoSecure General Power of Attorney.pdf	1	Power of Attorney	91 KB
135973-5006 Statemnt Under 37 CFR_A.pdf	3	Assignee showing of ownership per 37 CFR 3.73	86 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
135973-5000 GoSecure	54866C6D5D4457D5A62E686AF7BBF5C569878026D1A9ADCEA

General Power of Attorney.pdf	82B741BE0F5B6883540C436F63C326766645C325DA1AEAD8B2C075A49407988D90420182873794C
135973-5006 Statemnt Under 37 CFR_A.pdf	854AFAEEBEC38487ADBB7125FFFF85FD3FF1E84F13FFD8261FA70E5994CBA4F28D37CF71264397342 5B7E5E50A62CA4DE3DFCD8D4EC8235B15D1909B25402B93

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(c).

I hereby appoint the practitioners of Morgan, Lewis & Bockius LLP, Customer Number **24341** as attorneys or agents to represent the undersigned and to transact all business before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications and patents assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 C.F.R. § 3.73(c), said appointment to be to the exclusion of the inventor(s) and their attorney(s) in accordance with the provisions of 37 C.F.R. § 3.71, provided that, if any one of these attorneys ceases being affiliated with the law firm of Morgan, Lewis & Bockius LLP as partner, counsel, or employee, then the appointment of that attorney and all powers derived therefrom shall terminate on the date such attorney ceases being so affiliated.

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(c) to the address associated with Customer Number **24341**.

Assignee Name and Address: **GoSecure Inc.**
13220 Evening Creek Drive, S
San Diego, California 92128

SIGNATURE of Assignee of Record

The undersigned whose signature and title is supplied below is authorized to act on behalf of the assignee.

Signature Stan Eramia

Name Stan Eramia Date 07/27/2023

Title IP Manager Telephone (310) 866-1069

A copy of this form, together with a statement under 37 C.F.R. § 3.73(c) (Form PTO/SB96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 C.F.R. § 3.73(c) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee and must identify the application in which this Power of Attorney is to be filed.

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: GoSecure, Inc.

Application No./Patent No.: US 9,106,697 Filed/Issue Date: August 11, 2015

Titled: System and Method for Identifying Unauthorized Activities on a Computer System Using a Data Structure Model

GoSecure, Inc., a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. ☑ The assignee of the entire right, title, and interest.

2. ☐ An assignee of less than the entire right, title, and interest (check applicable box):

☐ The extent (by percentage) of its ownership interest is _____%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

☐ There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. ☐ The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. ☐ The recipient, via a court proceeding or the like (*e.g.*, bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. ☐ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

B. ☑ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: Inventors To: NEURALIQ, INC.

The document was recorded in the United States Patent and Trademark Office at
Reel 026504, Frame 0689, or for which a copy thereof is attached.

2. From: NEURALIQ, INC. To: COUNTERTACK INC.

The document was recorded in the United States Patent and Trademark Office at
Reel 036074, Frame 0499, or for which a copy thereof is attached.

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

IPR2025-00069
CrowdStrike EX1002 Page 393

PTO/AIA/96 (08-12)
Approved for use through 01/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: COUNTERTACK INC. To: GOSECURE, INC.

The document was recorded in the United States Patent and Trademark Office at
Reel 065082, Frame 0434, or for which a copy thereof is attached.

4. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

5. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

6. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at
Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☑ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Kannan Narayanan/	December 14, 2023
Signature	Date
Kannan Narayanan	79,060
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/163,590	06/17/2011	Alen Capalik	067292-5005-US

CONFIRMATION NO. 1008

24341
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

POA ACCEPTANCE LETTER

OC000000066081930

Date Mailed: 12/20/2023

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/14/2023.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sltorres/

IPR2025-00069
CrowdStrike EX1002 Page 396