

EX 1002

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.

UTILITY PATENT APPLICATION TRANSMITTAL <small>(ONLY FOR NEW NONPROVISIONAL APPLICATIONS UNDER 37 CFR 1.53(B))</small>		Attorney Docket No. 37617/011002; 08917906US	
		First Inventor Kevin Mcnamee	
		Title METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION	
		Express Mail Label No. N/A	

APPLICATION ELEMENTS <small>See MPEP chapter 600 concerning utility patent application contents.</small>	ADDRESS TO: Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450
<ol style="list-style-type: none"> 1. ☐ Fee Transmittal Form (e.g., PTO/SB/17) <small>(Submit an original and a duplicate for fee processing)</small> 2. ☒ Applicant claims small entity status. <small>See 37 CFR 1.27.</small> 3. ☒ Specification [Total Pages <u>27</u>] <small>Both the claims and abstract must start on a new page (For information on the preferred arrangement, see MPEP 608.01(a))</small> 4. ☒ Drawing(s) (35 U.S.C. 113) [Total Sheets <u>8</u>] 5. Oath or Declaration [Total Sheets <u>6</u>] <ol style="list-style-type: none"> a. ☒ Newly executed (original or copy) b. ☐ A copy from a prior application (37 CFR 1.63(d)) <small>(for continuation/divisional with Box 18 completed)</small> i. ☐ DELETION OF INVENTOR(S) <small>Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).</small> 6. ☒ Application Data Sheet. See 37 CFR 1.76 7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program <i>(Appendix)</i> ☐ Landscape Table on CD 8. Nucleotide and/or Amino Acid Sequence Submission <small>(if applicable, items a. – c. are required)</small> <ol style="list-style-type: none"> a. ☐ Computer Readable Form (CRF) b. Specification Sequence Listing on: <ol style="list-style-type: none"> i. ☐ CD-ROM or CD-R (2 copies); or ii. ☐ Paper c. ☐ Statements verifying identity of above copies 	ACCOMPANYING APPLICATION PARTS <ol style="list-style-type: none"> 9. ☐ Assignment Papers (cover sheet & document(s)) Name of Assignee <div style="border: 1px solid black; padding: 5px; width: 200px; margin: 5px auto;">Kindsight, Inc.</div> 10. ☐ 37 CFR 3.73(b) Statement ☐ Power of Attorney <small>(when there is an assignee)</small> 11. ☐ English Translation Document <small>(if applicable)</small> 12. ☐ Information Disclosure Statement (PTO/SB/08 or PTO-1449) ☐ Copies of citations attached 13. ☐ Preliminary Amendment 14. ☐ Return Receipt Postcard (MPEP 503) <small>(Should be specifically itemized)</small> 15. ☐ Certified Copy of Priority Document(s) <small>(if foreign priority is claimed)</small> 16. ☐ Nonpublication Request under 35 U.S.C. 122 (b)(2)(B)(i). <small>Applicant must attach form PTO/SB/35 or equivalent.</small> 17. ☐ Other: <div style="border: 1px solid black; height: 40px; width: 150px; margin-top: 5px;"></div>
18. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76: ☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____ Prior application information: Examiner _____ Art Unit: _____	
19. CORRESPONDENCE ADDRESS	
☒ The address associated with Customer Number: <div style="border: 1px solid black; padding: 2px 20px; display: inline-block;">22511</div> OR ☐ Correspondence address below	
Name	22511
Address	PATENT TRADEMARK OFFICE
City	State
Country	Zip Code
Telephone	Email Address
Signature	/Robert P. Lord/
Date	April 8, 2011
Name (Print/Type)	Robert P. Lord
Registration No. (Attorney/Agent)	46,479

APPLICATION
FOR
UNITED STATES LETTERS PATENT

**TITLE: METHOD AND SYSTEM FOR OPERATING SYSTEM
IDENTIFICATION IN A NETWORK BASED SECURITY
MONITORING SOLUTION**

**INVENTORS: Kevin MCNAMEE
Mike PELLEY
Darren DERIDDER
Paul EDWARDS**

22511

PATENT TRADEMARK OFFICE

METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims benefit of U.S. Provisional Patent Application No. 61/469,024, filed on March 29, 2011 and entitled “Method and System for Operating System Identification in a Network Based Security Monitoring Solution,” in the names of the same inventors as the present application.

TECHNICAL FIELD

[0002] The present disclosure relates to identification of computers coupled to a service provider network and in particular to identifying computers infected with malicious software (a.k.a. malware) from session traffic associated with the computers.

BACKGROUND

[0003] Residential and business networks LANs are typically connected to the Internet using a gateway or router that uses network address translation (NAT). The NAT device maps local area network (LAN) addresses of multiple devices to a single WAN IP address enabling multiple devices to access the internet using WAN address. All traffic emerging from that network will share the same IP address that is assigned to the gateway or router and Internet service providers typically only provide one wide area network (WAN) address to a modem or connection device at the premises. The NAT device modifies network address information in datagram (IP) packet headers while in transit across a traffic routing

device for the purpose of remapping one IP address space into another. From the WAN perspective it is difficult to determine which device behind a NAT device, is originating a particular stream of traffic. This is a particular problem when network based virus or malware detection is utilized where the WAN IP traffic is analyzed to determine the presence of potential malware originating from the LAN. The inability to determine a specific device means that any remediation procedures can not be applied in a focused manner.

[0004] Accordingly, systems and methods for Identifying computers behind a Network Address Translaton (NAT) device remains highly desirable.

SUMMARY OF INVENTION

[0005] In accordance with an aspect of the present disclosure there is provided a method of network based malware detection in a service provider network. The method comprising receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network. The one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network; determining an operating system identifier (OS ID) associated with the TCP session and the computing device. If malware is present in the TCP session an associated malware ID is determined by comparing a malware signature to the one or more TCP packets, an alert identifying a network address associated with the access device is generated with the malware ID and the OS ID associated with TCP session that generated the alert.

[0006] In accordance with another aspect of the present disclosure there is provided a system for network based malware detection in a service provider network. The system comprising a network sensor coupled to the service provider network. The network sensor receives one or more transmission control

protocol (TCP) packets originating from an access device coupled to the service provider network. The one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network and determines an operating system identifier (OS ID) associated with the TCP session and the computing device associated and then determines if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets. An alert is generated identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert. A remediation portal is coupled to the service provider network, the remediation portal identifies a subscriber accessing the remediation portal and identifies the OS associated with the computing device used by the subscriber to access the remediation portal. The portal compares the OS associated with the computing device to the OS ID identified in the alert and provides malware remediation to the computing device.

[0007] In accordance with yet another aspect of the present disclosure there is provided a computer readable memory containing instructions for network based malware detection in a service provider network. The instructions when executed by a processor performing receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network. The one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network; determining an operating system identifier (OS ID) associated with the TCP session and the computing device. If malware is present in the TCP session an associated malware ID is determined by comparing a malware signature to the one or more TCP packets and an alert is generated identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert.

BRIEF DESCRIPTION OF DRAWINGS

- [0008] Further features and advantages of the present disclosure will become apparent from the following detailed description, taken in combination with the appended drawings, in which:
- [0009] Various embodiments of a network based malware detection system will be described with reference to the figures in which:
- [0010] Figure 1 depicts in a block diagram of a system for malware detection and operating system detection are utilized for providing malware remediation;
- [0011] Figure 2 depicts an illustrative TCP session analysis;
- [0012] Figure 3 depicts a representation of session tracking and analysis;
- [0013] Figure 4 depicts a data flow diagram for operating system identification, malware detection and remediation;
- [0014] Figure 5 depicts a method of operating system detection and malware identification and remediation;
- [0015] Figure 6 depicts a method of operating system detection and malware identification;
- [0016] Figure 7 depicts a method of malware alert management;
- [0017] Figure 8 depicts a method of malware remediation.
- [0018] It will be noted that throughout the appended drawings, like features are identified by like reference numerals.

DETAILED DESCRIPTION

- [0019] Embodiments are described below, by way of example only, with reference to Figs. 1-8.

[0020] Residential and business networks are typically connected to the Internet using a gateway or router that uses NAT. All traffic emerging from that network share the same IP address that is assigned to the gateway or router. When NAT is utilized it is not possible for detection technologies that use the IP addresses to distinguish between individual devices that may be resident in the local network behind the NAT device. By combining TCP session tracking and OS fingerprinting a specific operating system can be associated with an individual TCP session which can improve the ability to distinguish between computing devices. In a network-based malware detection system, the ability to identify an operating system enables information to be provided to the user to speed the remediation process. A household with multiple computers, or computing devices, each potentially running different operating systems can require considerable time to remediate. The ability to provide identification of an operating system that is infected and request that the user access the remediation portal with a computer that has a particular operating system can improve the results of the remediation process.

[0021] In the present system when malware is detected in a session originating from an access device coupled to a service provider network a security alert is raised to identify the session contains an infection that should be addressed. When the infected device is a computing device that accesses the network by a NAT device, the ability to identify a specific computing device is a challenge. To enable proper identification of an associated computing device, the OS information that is determined for the session is sent with the alert. By providing OS identification the remediation process can focus on those computing devices that are infected rather than requiring remediation procedures on devices that are potentially not infected. The technique allows a distinction between the most of the popular operating systems used in computing devices such as personal computers, mobile phones, tablets and other networked devices that may be

susceptible to an infection. This includes (but is not limited to): Windows 98™, Windows NT™, Windows XP™, Windows Vista™, Windows 7™, Linux, Android™, BSD, Mac OS™, iOS™, Blackberry™ OS, Sun OS™, etc..

[0022] There are a number of techniques that can be used to identify a computer's operating system based on network traffic coming from that computer. One is TCP/IP stack fingerprinting to identify candidate operating systems based on the first SYN packet of the TCP session which is available for all TCP sessions. Another technique is to extract the operating system string from the browser User-Agent field on HTTP requests. These are combined to accurately identify the operation system associated with an individual session.

[0023] When malware is detected on the user's device, an alert notification is sent to the user informing them that they should visit the remediation portal to remove the malware from their system. The remediation process involves downloading malware cleaning tools to the infected machine. These tools scan the infected device and remove any malware found. These scans can take considerable time and must be run on all devices that may be infected. So, when there are multiple devices in the household, being able to identify the infected device can considerably shorten the remediation process. When the user visits the remediation portal from one of their household devices, the same OS fingerprinting techniques can be used. This enables the portal to determine if the device has the same operating system as the one identified in the alert and thus decide whether the remediation process is required for that device. If the OS of the device matches the one from the alert, the full remediation process is run. If the operating systems do not match, the user is informed that the device is clean and asked to reconnect to the portal from one of their devices that matches the OS detected with the security alert.

[0024] Figure 1 depicts, in a block diagram, a system for operating system identification and malware remediation. A user location 100 comprises multiple computing devices 104, 106, 108 in a local area network (LAN) that access an Internet service provider or service provider (SP) network 110 via an access device 102. The access device may provide access via wired or wireless interface for a single computing device to the network or may provide network address translation (NAT) to allow multiple devices to connect to the network as shown. NAT may be provided either directly through incorporation in a router or modem or through additional hardware or software functionality provided by one of the computing devices. TCP/IP traffic is received at the network edge node 112 which routes the data through the SP network 110 to the Internet 120. Destination device 122 is accessed through the Internet 120. The destination device may be a web server, peer computer, content server or another network to which a computer 104, 106, 108 is engaged in a TCP session.

[0025] The SP network 110 comprises a plurality of routers or switches 112, 114, 116 for directing network traffic between two endpoints, such as a subscriber computer 104 and a web site provided by a web server of destination device 122 on the public Internet 120. The system of the present disclosure, or parts thereof as described further below, are deployed within the SP network in order to capture and analyze the network traffic. Using the analyzed traffic, the system can determine if a subscriber's computer 104 is infected with malware. If the system determines that a subscriber's computer 104 is infected, it can provide a notification to the subscriber that a computer running a specific operating system is infected and direct them to remedy the infection.

[0026] The system helps to ensure that computers 104 connected to the SP network are not infected with malware aiding in the safe and reliable functioning of the SP network 110. Furthermore, since the system is network based, it is not necessary to have the subscriber download, install or update software. This can

help ensure that all of the components in the system are utilizing the most current malware detection means as possible .

[0027] The edge node 112 either provides or is connected to one or more network sensors 130 comprising at least a processor 132 and memory 134. The network sensor 130 either implements or is coupled to a network tap/filter that is capable of copying packets of information travelling over the SP network 110. The network sensor 130 analyzes packets from the network tap/filter to determine if the packets contain evidence of malware infection on the computers 100 from which the packets originate. In addition the sensor will also examine the packets to determine the operating system (OS) of the computer 104 from which the packets originate. When malware is identified, the network sensor sends an alert 136 to an alert manager 140 coupled to the SP network 110 either directly or indirectly. The alert 136 contains the source and destination IP addresses and port numbers from the packet that generated the alert, a time stamp indicating when the alert occurred, the OS identifier of the computer that caused the alert, an identifier that indicates which specific malware was detected several parameters that indicate the type of malware, in addition it may include threat level and severity of the alert in question.

[0028] Advantageously a network sensor device 130 located near a subscriber's computers 100 at the edge of the SP network for example edge node 112 will see both upstream and downstream packets for the subscriber's NAT device 102. This allows the detection engine to track state information for a connection and use signatures based on this session state information. Although this location for the deployment of network sensor devices has advantages, it may also require a large number of network sensors to be deployed, which would increase the capital expenditure and operating expenses for deploying the system. Additionally or alternatively, network sensor devices 130 may be deployed within the core of the SP network at location where each network sensor device may be

able to see, and so process, more network traffic. This may reduce the capital expenditures and operating expenses for deploying the system.

[0029] The alert manager 140, comprising at least a processor 142 and memory 144, receives the alerts 136 from one or more network sensors 130. The alert manager 140 may be in the SP network 110, coupled to the SP network 110 or accessible via an intermediary network, for example the Internet 120. .

[0030] The alert manager 140 stores the alerts 136 in the alert repository 146. The alert information that is stored in the database consists of a subscriber identifier that is derived from the IP address, the malware identifier, the OS identifier and the time stamp from when the alert was observed. Subsequent alerts for the same combination of subscriber, malware and OS identifies are not stored, but a counter is incremented in the alert record to track multiple occurrences of the same alert. The subscriber identifier is derived from the original alert information through an ID translator that is capable of translating a network identifier, such as an IP address, to an associated subscriber identifier, such as a user name or account number of a subscriber, a media access control (MAC) address assigned to the subscriber, network access server (NAS) port number, etc. The subscriber identifier uniquely identifies the residential user location 100 and may be retrieved or provided from a service provider subscriber ID repository 148.

[0031] The alert manager 140 may further comprise a subscriber notification generator to generate a notification to a subscriber on the first instance or once the subscriber's alerts have passed a threshold value or based upon time until the alert is cleared. The threshold value may vary depending on the configuration of the system. For example, if the detection engine in the network sensor 130 used to detect malware infection provides the malware detection with a very low false-positive rate; the threshold value may be set so that if the alert indicates that a

single detailed alert has been generated for the user a corresponding notification is generated. Alternatively, if the detection engine has a higher false-positive rate the threshold may be raised in order to account for potential false positives. Additionally, the threshold may be set for the particular malware or type of malware. For example, the threshold may be set to generate a notification if a single alert was generated for a particular piece of malware that is considered to be a significant threat, and also generate a notification if, for example, ten alerts have been generated for a particular piece of malware that is considered to be a medium threat.

[0032] The notification provided to the subscriber may be provided in various ways. For example, the notification may be an email sent to the subscriber, a text message sent to a phone number associated with the subscriber ID, a voicemail sent to a phone number associated with subscriber ID or as a domain name server (DNS) redirect for future traffic of the subscriber, or as a walled garden or web interstitial.

[0033] The notifications sent to a subscriber include directions for accessing a remediation portal 150, comprising at least a processor 152 and memory 154. For example, if the notification is an email, the indication may include a hypertext link, if the notification is a voicemail it may include instructions for accessing the remediation portal. If the notification is a DNS redirect, the indication may be a landing page of the remediation portal 150. The notification identifies the operating system that the malware was detected on and requests that the user access the remediation portal 150 with the computer that may contain the infection.

[0034] The remediation portal 150 determines the subscriber connecting to the portal and the operating system associated with the connection. The remediation portal 150 may be in the SP network 110, coupled to the SP network 110 or

accessible via an intermediary network, for example the Internet 120. Similar detection techniques may be utilized as in the network sensor 130 at the portal to determine an operating system associated with the computer accessing the portal. The remediation portal 150 can then provide the subscriber with instructions to follow in order to remove or quarantine the particular malware detected if the OS matches the OS identified in the alert information 136. The remediation portal may provide a dynamically generated instructions based on the specific malware that was detected on the subscriber's computer. The remediation process provided by the portal may include automated processes for automatically removing the malware from the computer. Additionally, or alternatively, the remediation process may comprise instructions for actions to be performed by the subscriber such as deleting a file, modifying configuration settings of the computer, etc. If the OS of the computer does not match the alert summary information the user may be requested to access with another computer have the identified operating system until an appropriate OS and malware are identified.

[0035] Once the user has accessed the remediation portal 150, and completed the remediation process, the remediation portal resets the alerts stored in the alert repository 146 for the subscriber associated with the remedied malware. As such, once the subscriber has performed the remediation process, no further notifications will be received, unless a further malware infection is detected. Alternatively, the malware identification may be maintained for tracking and trending purposes. It should be noted that the remediation portal 150 and the alert manager 140 are described as separate entities, however functionality may reside or be shared in a single system. Similarly the summary alert repository 146 may maintained at one or both locations.

[0036] Figure 2 depicts an illustrative TCP session analysis between computer 202 and 204 of different operating systems and web servers 222. For each session

204, 206, 208, 214 and 216 the following information is extracted from the SYN packet 210.

- Initial packet size (16 bits)
- Initial TTL (8 bits)
- Window size (16 bits)
- Max segment size (16 bits)
- Window scaling value (8 bits)
- "don't fragment" flag (1 bit)
- "sackOK" flag (1 bit)
- "nop" flag (1 bit)

[0037] These fields are set by the operating system in an attempt to optimize the TCP protocol. Different operating systems will choose different combinations and its these different combinations that enable fingerprinting to identify the OS. Some of the fields are optional (scaling, sackOK, nop, etc) and can appears in different orders and combinations. This information is also used to determine an associated operating system.

[0038] The correlation can occur by comparing the SYN fingerprint to a set of known SYN fingerprints. The SYN fingerprints can be correlated by data collection and comparison to the previous SYN fingerprints to associate and OS identifier with the SYN packet.

[0039] The user agent (UA) 214 field is extracted from TCP packets in the HTTP protocol to identify the application type, operating system, software vendor, or software version being utilized by the computer 202 and 204 and provide an

additional level of OS fingerprint confidence or possibly identify a discrepancy between the SYN packet analysis and UA field.

[0040] The data packets 212 are analyzed against malware signatures to determine the presence of possible malware. When malware is detected in the session information data packets 212, the session is flagged, for example session 206. In this example the SYN and UA fields would identify that a Windows/XP computer is infected. Sessions 204, 206 and 208 would all be identified as Windows/XP sessions. Similarly session 214 and 216 would be identified as Mac OS sessions. The Windows/XP sessions 204, 206 and 208 may all be from the same computer or from different computers if more than one computer in the residence is running Windows/XP. The FIN packet 218 may be utilized to define the termination of a TCP session.

[0041] Figure 3 depicts a representation 300 of session tracking and analysis performed at the network sensor 130. A session tracking engine receives packets at network sensor 130 that are decoded. Protocol analysis may also include determining the type of packet., for example TCP or UDP. From the protocol, protocol parameters are utilized, such TCP parameters in a SYN packet or associated with a SYN flag, to provide an OS signature. Application analysis is then performed to further identify the OS. The application analysis can be used to verify the protocol, for example HTTP protocol, and verify the user agent information available in a HTTP session.

[0042] The data of the packets are then analyzed for malware by comparing the data of the session to malware signatures. The signatures used by the malware detection may be stored in a repository, such as a local database. The signatures specify the characteristics that the malware network traffic will have. This includes data patterns that may be present in network packets, state information associated with the network protocols, and sequences of events that may be

considered anomalous network behaviour. These signatures are expressed as detection engine rules. When the malware detection process detects a packet or sequence of packets that matches a specific rule it generates an alert event. The detection engine rule includes a signature for detecting malware in the network traffic as well as an action to take when the rule is matched. The appropriate alert can then be generated. The alert combines malware information from the malware detection stage with operating system information from the protocol and application analysis phases.

[0043] Figure 4 depicts a data flow diagram for operating system identification and remediation. In this example a user location 100 having one or more computer behind a NAT device initiates a session with web server 422. Packets from the session are monitored by the network sensor 130 (402). The network sensor 130 determines the OS of computing device such as a personal computer at the user location and identifies the presence of an infection such as malware. An alert is generated by the network sensor 130 and sent to the alert manager 140 identifying the IP or network address, the OS of the infected device, malware that caused the infection and a timestamp (404). On the first occurrence of the alert, the alert manager 140 sends a message to the subscriber associated with the session identifying the presence of a computer with malware infection and the OS (406). The user receives the message and is directed to access a remediation portal 150. Upon user access the remediation portal retrieves the alert information from the alert manager database. In this example it is assumed that the user accessed the remediation portal 150 from a computer with an OS that did not match the alert (408). The user is informed of this OS/Alert mismatch and asked to connect to the remediation portal from a computer whose OS does match the alert (410). A subsequent access is then performed, and the appropriate OS and malware are identified on the computer (412). A remediation process is commenced by the portal 150 to remove the malware

infection (414) and the user is notified of success remediation. The remediation portal 150 can then notify the alert manager 140 of the success removal of the malware and remove the associated alert (416).

[0044] Figure 5 depicts a system level method of operating system detection and malware identification and remediation. As will be further described in Figure 6, from TCP packets received at one or more network sensors, an IP address of the access device is determined (504). If the IP address is not identified for monitoring, the packets may be discarded. An OS ID associated with the TCP packets is determined by one or more methods determining identifiable OS characteristics (506) and further described in Figure 6. The session is analysed by malware detection engine to determine if an infection is present in the session (508). An alert is then generated (510) to identify the IP address, the infection and an associated operating system. As will be further described in Figure 7, the alert is forwarded to an alert manager where the IP address is converted to a subscriber identifier (512). The user associated with the IP address, or user location, is then notified (514) that a computing device associated with the access point, for example behind a NAT device, is infected and identification of the operating system is provided. As will be further described in Figure 8, the user then visits the remediation portal (516) which identifies the operating system of their computing device using the same techniques as the sensor (518). If the operating system of the connected computing device matches the alert then the remediation process is executed from the portal (520). This involves scanning the infected computing device and removing the infection such as malware. If the operating system of the connected computing device does not match the alert, the user is asked to connect to the portal from the next computer. This is repeated until all computing devices associated with the access device have been cleaned.

[0045] Figure 6 depicts a method of operating system detection and malware identification. The method begins with receiving packets (602) that have been

captured from the SP network traffic. The packets are analyzed to determine an OS fingerprint by comparing the SYN packet for the session with known SYN fingerprints. If an OS ID is identified, (YES at 604) and OS identifier is generated (606). If an OS fingerprint is not identified (NO at 604), the packets are passed to the application protocol analysis module. If the HTTP UA information is not present, (NO at 608) malware analysis is performed (616). If the protocol is HTTP and a UA field is present (YES at 608), the OS specified in the UA field is compared with the OS identifier from the SYN packet. If they match (YES at 610) the OS identifier is verified (614). On a mismatch (NO at 610) the most reliable one is chosen (612). When the OS identifier is verified the UA information may be utilized to refine the OS identified by the SYN parameters. For example the SYN parameters may identify that the computing device is a Windows 7 computer where the UA may be able to refine the information and identify that it is a Windows 7 SP1 computer.

[0046] All packets are then passed to the malware analysis module for processing (616). Malware detection is performed by comparing each of the received packets to a detection rule, or a signature of the detection rule, for a particular piece of malware. If malware is not detected (NO at 616) packet processing continues for that session. If malware is detected based upon fingerprint analysis (YES at 616) and OS information is available (YES at 618), it is added to an alert event (620) and sent to an alert manager (622). If an OS is not identified (NO at 618) an alert is generated (622) without OS identification. The alert contains the source and destination IP addresses and port numbers from the packet that generated the alert, a time stamp indicating when the alert occurred, the OS identifier of the computing device that caused the alert, an identifier (signature id) that indicates which specific malware was detected several parameters that indicate the type of malware, threat level and severity of the alert in question.

[0047] Figure 7 depicts a method of malware alert management for notifying subscribers of a malware infection. The method begins with receiving alert events from one or more network sensors 130 at an alert manager 140 (702). The network identifier (for example source IP address) associated with the alert event is translated into a subscriber identifier (704). The subscriber identifier is derived from the original alert information through an ID translator that is capable of translating a network identifier, such as an IP address, to an associated subscriber identifier, such as a user name or account number of a subscriber, a media access control (MAC) address assigned to the subscriber, network access server (NAS) port number, etc.

[0048] The alerts are identified by three pieces of information: the subscriber ID, the malware ID and the OS ID. The system determines if and an alert already exists in the system with the same subscriber ID, malware ID and OS ID combination (YES at 706). If so a counter is incremented for this alert (708). If not, (NO at 706) it is treated as a new alert and a notification is sent to the subscriber (710). The user will then visit the portal to begin the remediation process. The end result of this process will be to reset the user's status for this alert to "remediation complete".

[0049] Periodically, the alert/notification process will check to ensure that the remediation status for each alert has been completed. If the remediation is completed (YES at 712), by receiving an indication from the remediation portal, the alert manager removes the alert event, or reset the counter (714) for the subscriber and OS. If the remediation is not completed (NO at 712), based upon a notification from the remediation portal, or a time interval, or counter threshold, another request may be sent (710) to the subscriber.

[0050] Figure 8 depicts a method of malware remediation for remediating a malware infection on a computing device coupled to a service provider network.

The method begins with a subscriber receiving a notification, which includes an indication for accessing a remediation portal, from the reporting infrastructure. The subscriber may then access the remediation portal (802). The subscriber ID is determined based upon the originating address or by a login user ID and password that is associated with their subscriber ID (804). The session with the computing device is analyzed to determine the OS and may be performed using SYN and UA techniques as previously described (806). If the OS ID in the alert event matches the OS in the current session (YES at 808) the remediation portal provides the subscriber with a remediation process (810). If the OS in the alert event does not match the OS in the current session (NO at 808) the user can indicate if additional computing devices are associated with the NAT device at the user location. If additional computing devices are present (YES at 812) the process is repeated (802) by the user accessing the portal using each of the associated computing devices until the process is complete. If not additional computing devices are present (NO at 812) the subscriber's alert record can be reset (814).

[0051] Although the above description has described various embodiments of a network based malware detection system, one skilled in the art will appreciate that changes and modifications may be made to the described illustrative embodiments. The above description provides a network based operating system and malware detection system and method. The components of the system, as well as their functioning have been described using various means, including flow charts specifying methods that the components of the system may implement. It is understood that the system may comprise hardware components that can be incorporated into a communication network. The hardware components may combine hardware, firmware and software in order to implement the system described herein. Alternatively, the system components may be implemented on hardware components by software expressed as a series

of computer executable instructions that configure the hardware components to implement the system described herein.

CLAIMS

What is claimed is:

1. A method of network based malware detection in a service provider network, the method comprising:
 - receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network, the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network;
 - determining an operating system identifier (OS ID) associated with the TCP session and the computing device;
 - determining if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets; and
 - generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert.
2. The method of claim 1 wherein determining the operating system ID further comprises:
 - determining a protocol associated with the TCP packets and matching an OS fingerprint from one or more protocol parameters if present in the TCP packets to determine a first operating system identifier (ID);
 - determining an application parameter associated with the TCP session if present, and identifying a second OS ID from the application parameter; and
 - wherein the OS ID in the alert comprises one of the first OS ID or second OS ID associated with one or more computing devices coupled to the access device.

3. The method of claim 2 further comprising sending a notification to a subscriber associated with the network address associated with the access device, the notification identifying a remediation portal to remove the determined malware in the alert.
4. The method of claim 3 further comprising:
 - identifying at the remediation portal the subscriber accessing the remediation portal;
 - identifying the OS associated with the computing device used by the subscriber to access the remediation portal;
 - comparing the OS associated with the computing device to the at least one of the first OS ID or second OS ID identified in the alert; and
 - providing malware remediation to the computing device when the at least one of the first OS ID or second OS ID matches the OS associated with the computing device.
5. The method of claim 3 wherein if the OS of the computing device is not the at least one of the first OS ID or second OS ID identified in the alert an indication is provided to the subscriber to connect to the remediation portal with an other computing device connected to the access device.
6. The method of claim 3 wherein the alert is cleared when all computing devices associated with the access device and the computing device having the at least one of the first OS ID or second OS ID have accessed the remediation portal.
7. The method of claim 2 wherein determining the first OS ID is performed by comparing one or more protocol parameters of the one or more TCP packets having a SYN flag associated with the session, wherein the OS fingerprints identify the protocol parameters of the SYN flagged packet and the OS ID associated with parameters.

8. The method of claim 2 wherein determining the application parameter associated with the session and identifying the second OS ID from the application parameter by inspecting an HTTP user agent string to determine the second OS ID.
9. The method of claim 2 further comprising verifying the first OS ID against the second OS ID, wherein if the second OS ID does not match the first OS ID the session is identified by the OS ID identified as a more reliable OS ID.
10. The method of claim 2 further comprising verifying the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID either OS ID is used.
11. The method of claim 2 further comprising verifying the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID but the second OS ID provides additional information, the second OS ID is used.
12. The method of claim 3 wherein sending the notification to the subscriber associated with the access device further comprises replacing the network address of the access device with a subscriber ID.
13. The method of claim 12 wherein sending the notification to the subscriber associated with the access device further comprises aggregating one or more detailed alerts having the subscriber ID into a single alert summary associated with the subscriber ID.
14. The method of claim 12 wherein the one or more computing devices are coupled to the access device through a local area network (LAN), the access device providing network address translation (NAT) or is coupled to NAT device to share the network address of the access device.
15. The method of claim 14 wherein the network address is an Internet Protocol (IP) address or a Media Access Control (MAC) address.

16. A system for network based malware detection in a service provider network, the system comprising:

a network sensor coupled to the service provider network, the network sensor:

receives one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network, the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network;

determines an operating system identifier (OS ID) associated with the TCP session and the computing device associated;

determines if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets; and

generates an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert; and

a remediation portal coupled to the service provider network, the remediation portal:

identifies a subscriber accessing the remediation portal;

identifies the OS associated with the computing device used by the subscriber to access the remediation portal;

compares the OS associated with the computing device to the OS ID identified in the alert; and

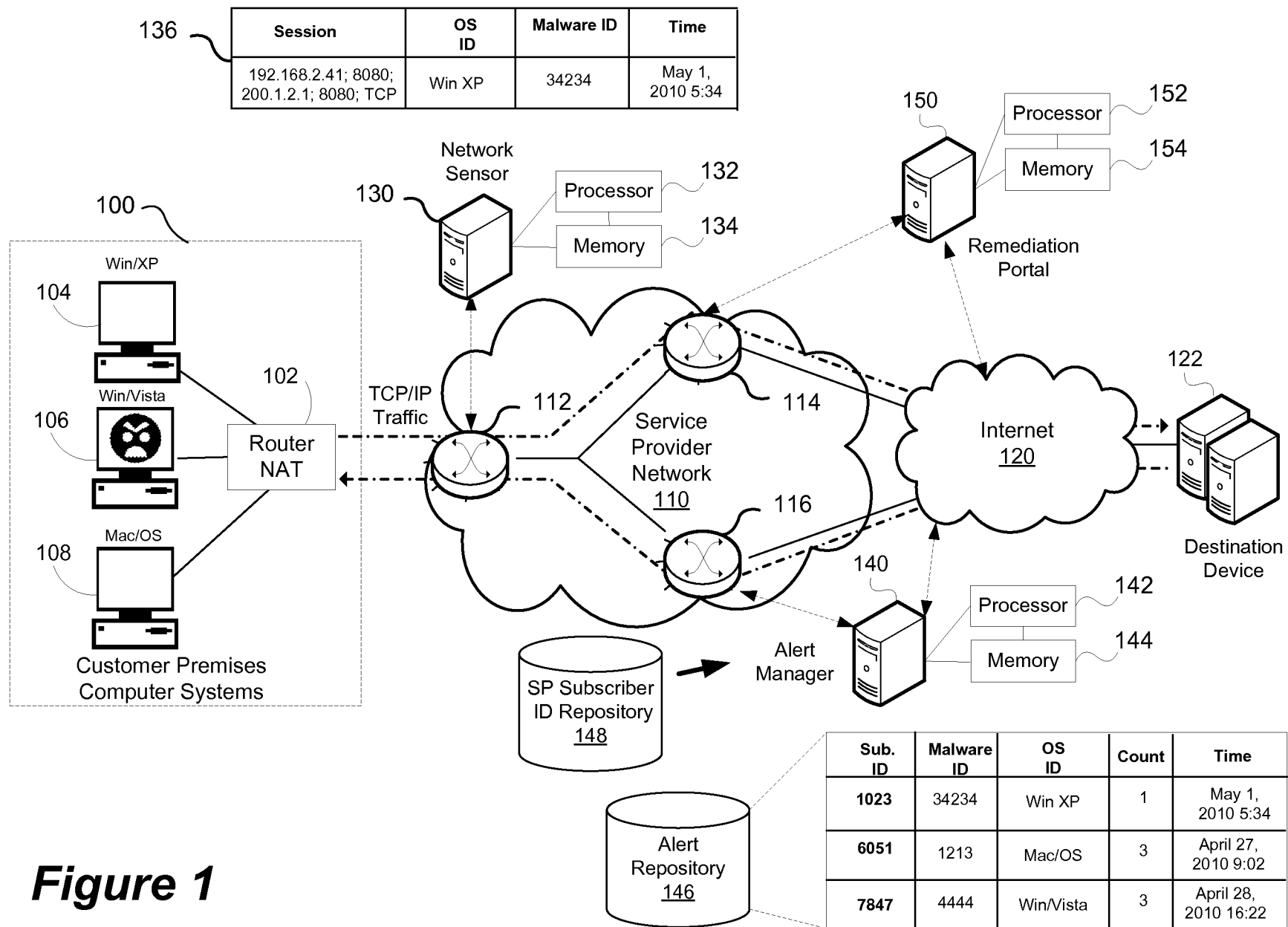
provides malware remediation to the computing device.

17. The system of claim 16 wherein determining the operating system ID at the network sensor:
- determines a protocol associated with the TCP packets and matching an OS fingerprint from one or more protocol parameters if present in the TCP packets to determine a first operating system identifier (ID);
 - determines an application parameter associated with the TCP session if present, and identifying a second OS ID from the application parameter; and
 - wherein the OS ID in the alert comprises one of the first OS ID or second OS ID associated with one or more computing devices coupled to the access device.
18. The system of claim 17 further comprising an alert manager to send a notification to a subscriber associated with the network address associated with the access device, the notification identifying the remediation portal to remove the determined malware in the alert.
19. The system of claim 18 wherein sending the notification to the subscriber associated with the access device further comprises retrieving a subscriber ID from a subscriber ID repository and replacing the network address of the access device with the subscriber ID.
20. The system of claim 17 wherein the network sensor determines the first OS ID by comparing one or more protocol parameters of the one or more TCP packets having a SYN flag associated with the session, the OS fingerprints identify the protocol parameters of the SYN flagged packet and the OS ID associated with parameters.
21. The system of claim 20 wherein the network sensor determines the application parameter associated with the session and identifies the second OS ID from the application parameter by inspecting an HTTP user agent string to determine the second OS ID.

22. The system of claim 21 wherein the network sensor verifies the first OS ID against the second OS ID, wherein if the second OS ID does not match the first OS ID the session is identified by the OS ID identified as a more reliable OS ID.
23. The system of claim 21 wherein the network sensor verifies the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID either OS ID is used.
24. The system of claim 21 wherein the network sensor verifies the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID but the second OS ID provides additional information, the second OS ID is used.
25. A computer readable memory containing instructions for network based malware detection in a service provider network, the instructions when executed by a processor performing:
- receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network, the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network;
 - determining an operating system identifier (OS ID) associated with the TCP session and the computing device;
 - determining if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets; and
 - generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert.

ABSTRACT

A method and system for providing network based malware detection in a service provider network is disclosed. Transmission control protocol (TCP) packets defining originating from an access device coupled to the service provider network defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network are received. An operating system identifier (OS ID) associated with the TCP session and the computing device is determined. If malware is present in the TCP session and an associated malware ID is determined by comparing a malware signature to the one or more TCP packets. An alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert can then be generated.



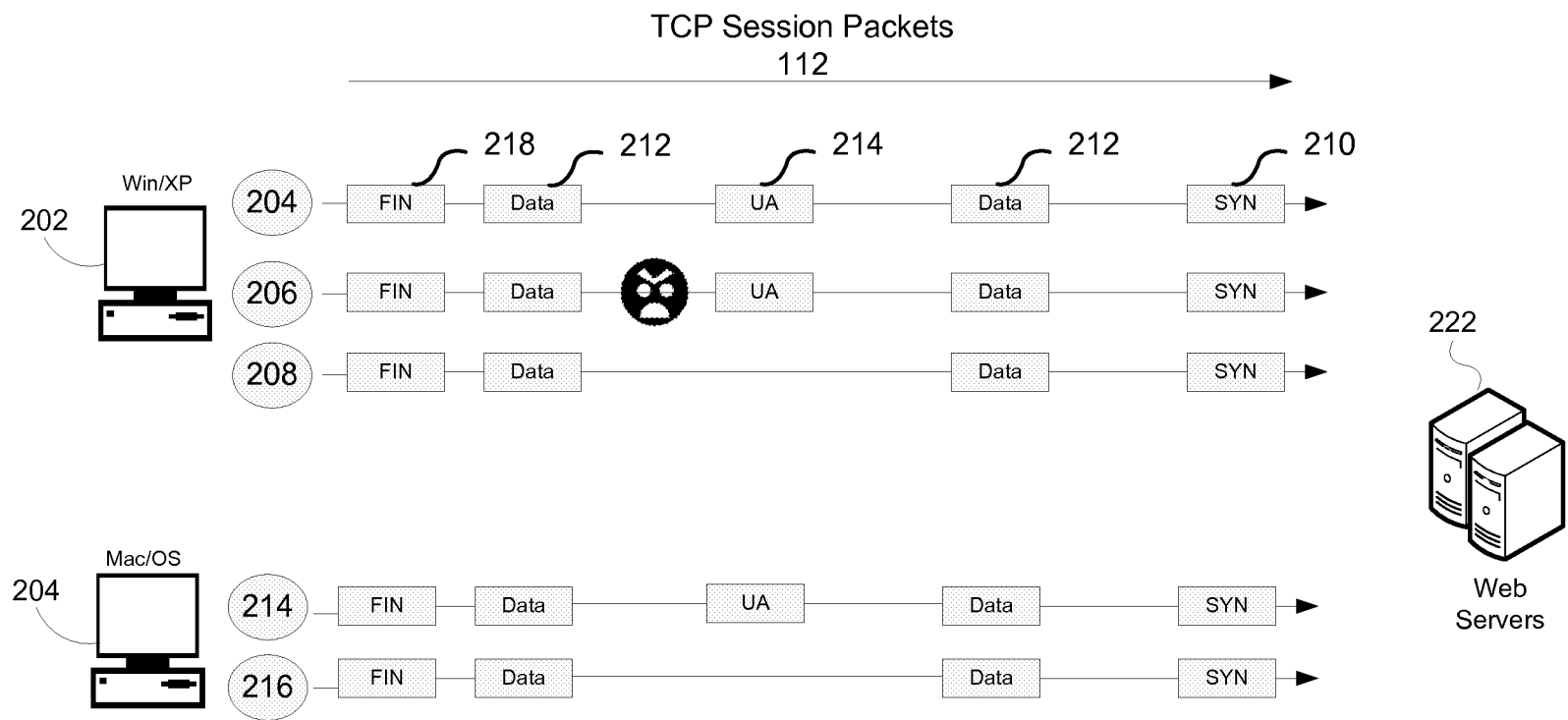


Figure 2

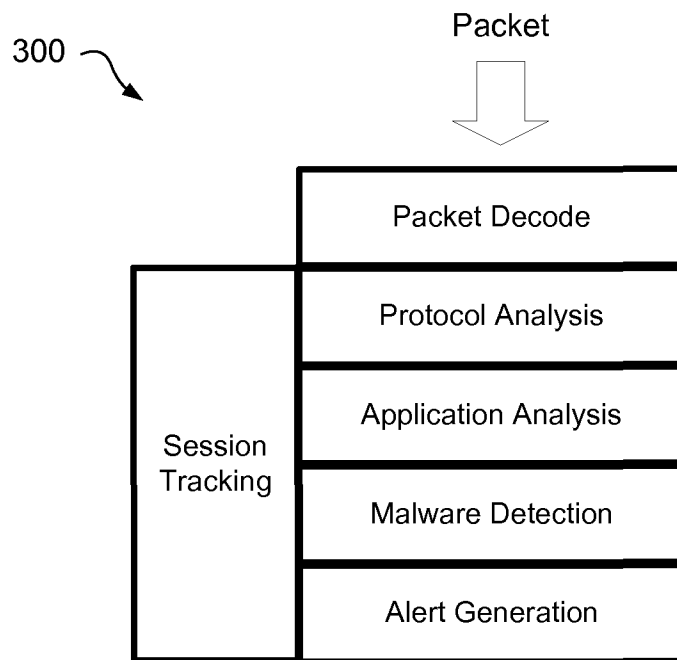


Figure 3

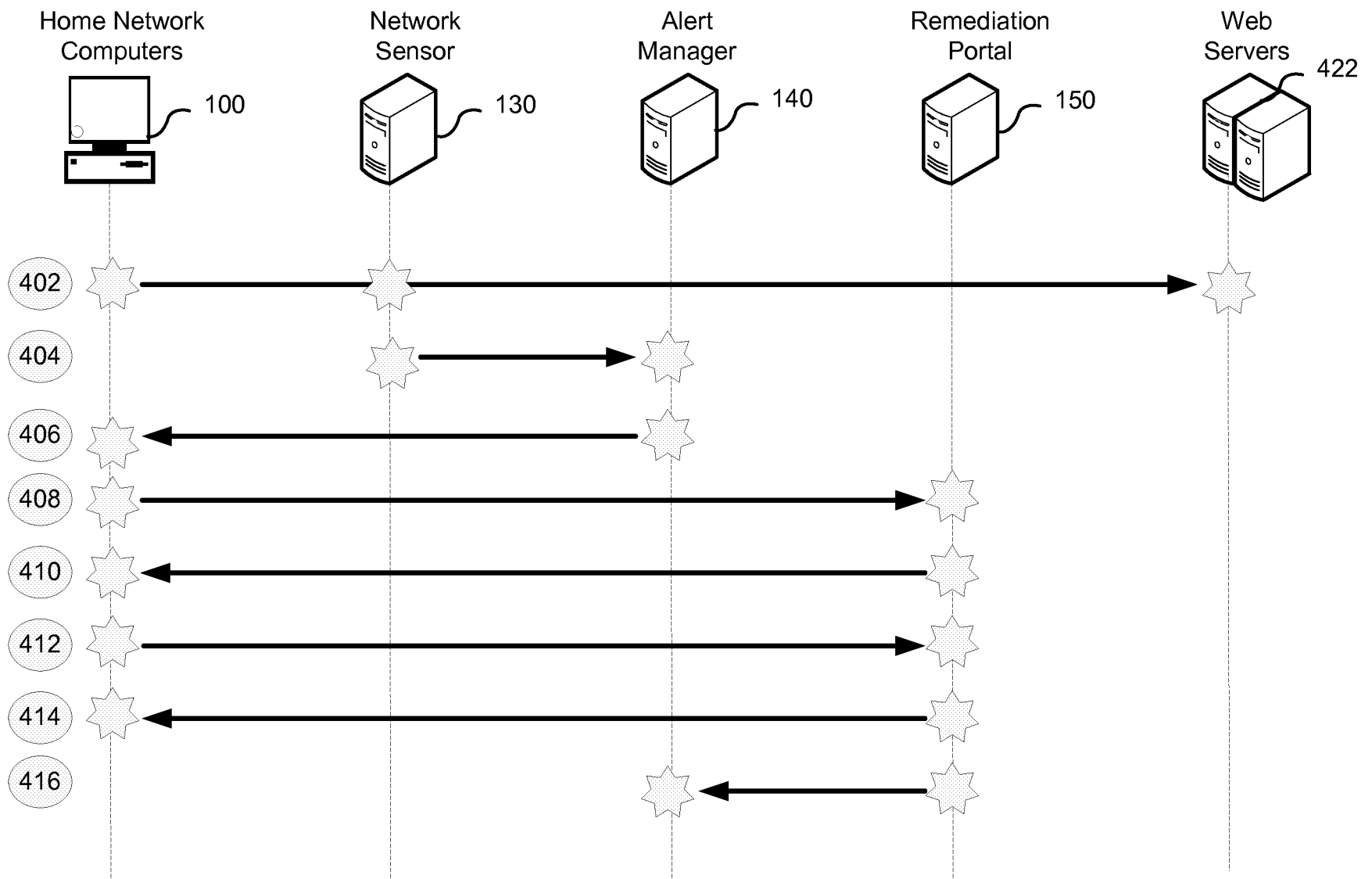


Figure 4

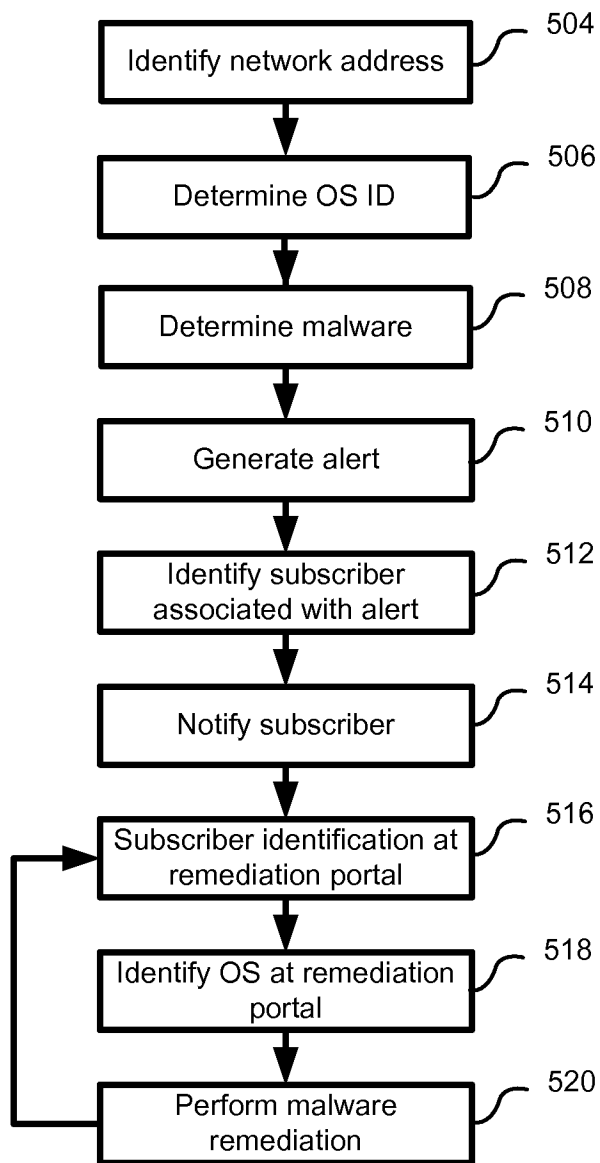
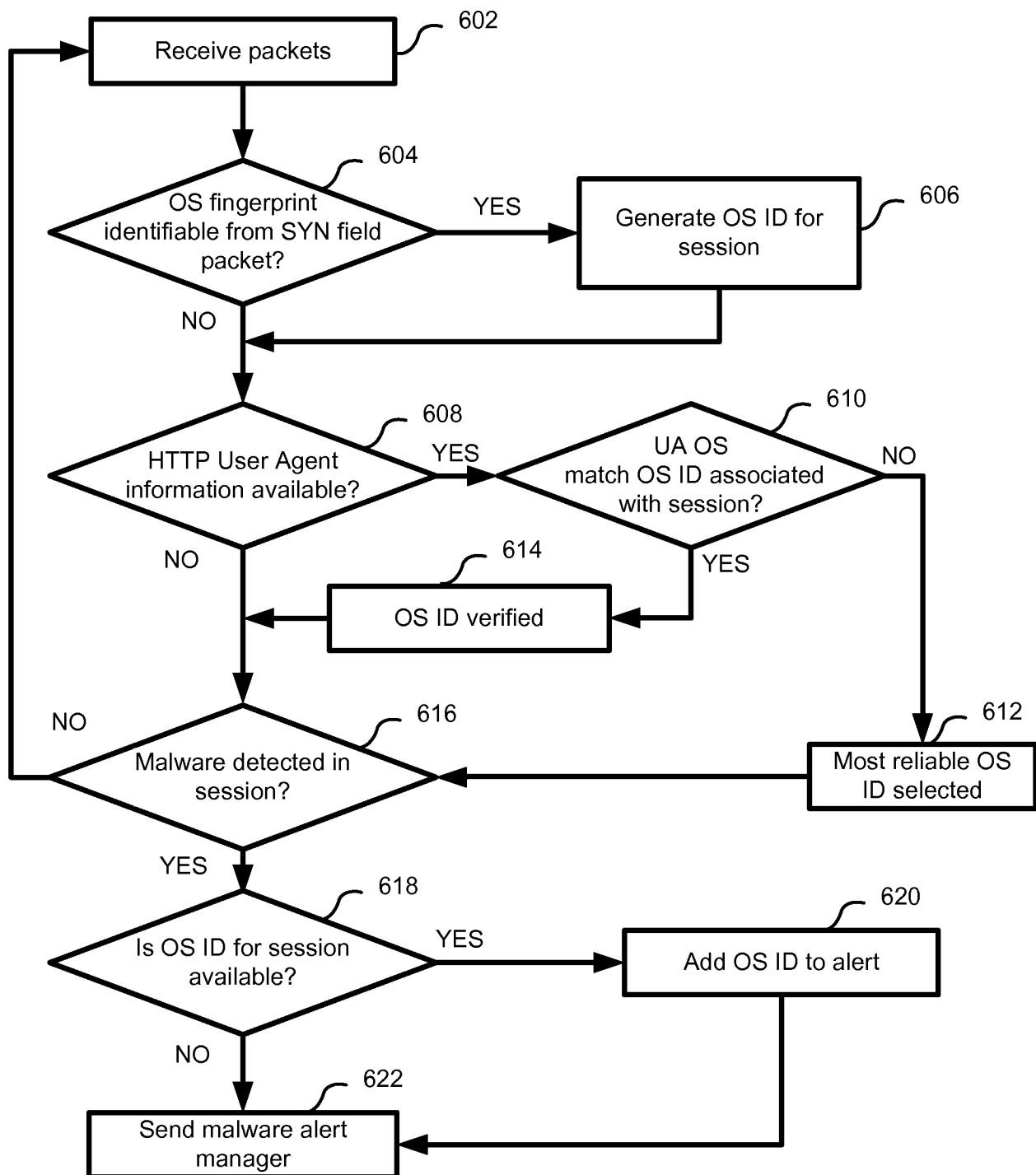


Figure 5

Figure 6



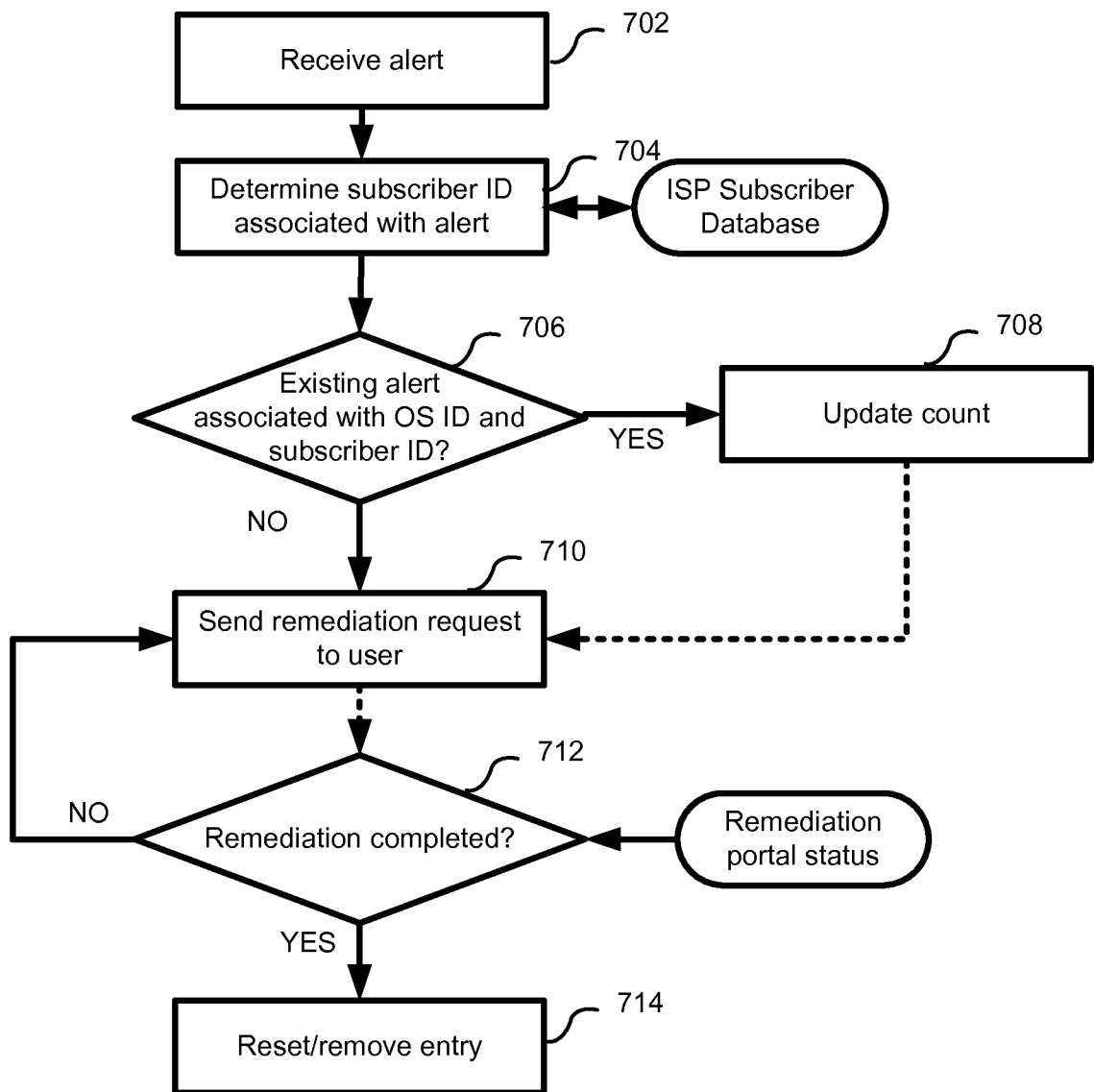


Figure 7

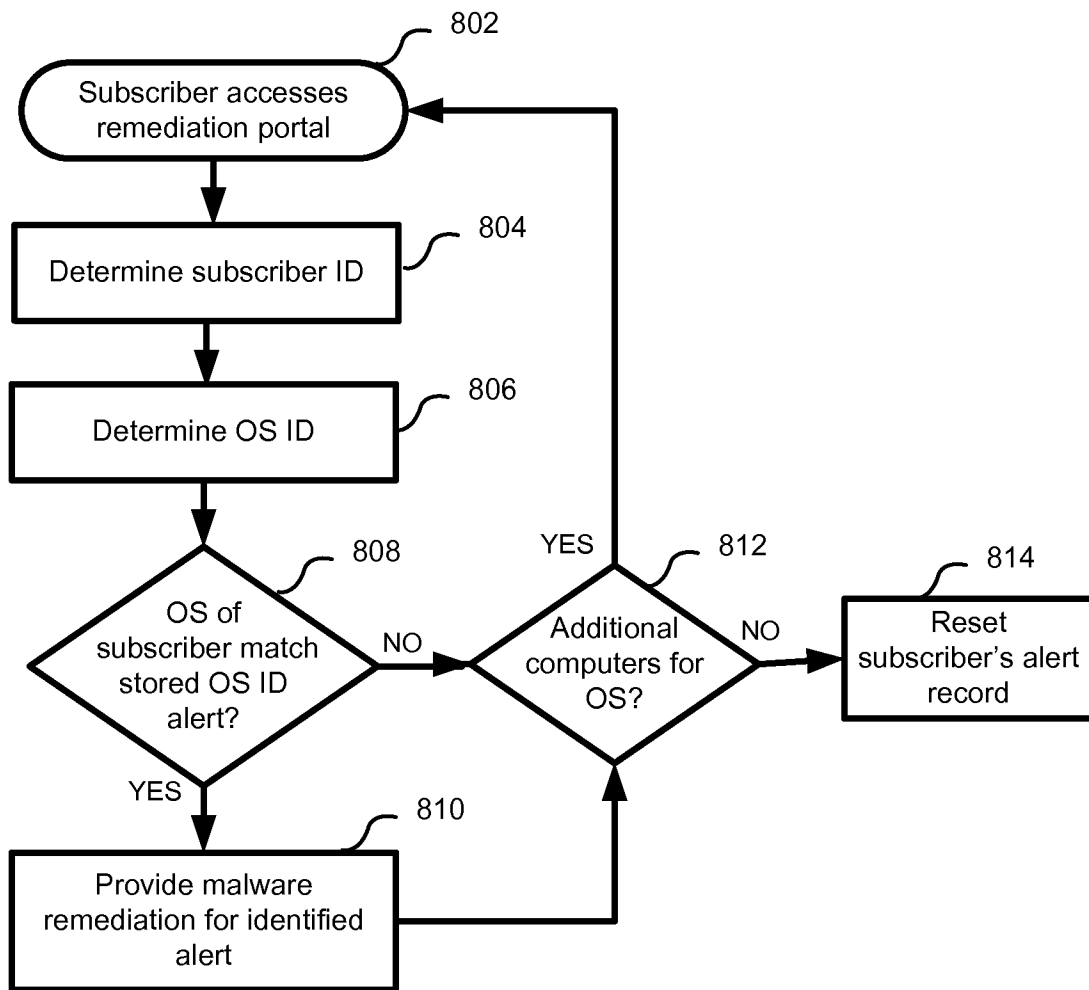


Figure 8

**DECLARATION FOR UTILITY OR
DESIGN
PATENT APPLICATION
(37 CFR 1.63)**

☒ Declaration Submitted With Initial Filing OR ☐ Declaration Submitted After Initial Filing (surcharge (37 CFR 1.16(f)) required)

Attorney Docket Number	
First Named Inventor	MCNAMEE, Kevin
COMPLETE IF KNOWN	
Application Number	
Filing Date	
Art Unit	
Examiner Name	

I hereby declare that: (1) Each inventor's residence, mailing address, and citizenship are as stated below next to their name; and (2) I believe the inventor(s) named below to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought on the invention titled:

METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION

(Title of the Invention)

the application of which

☒ is attached hereto

OR

☐ was filed on (MM/DD/YYYY) _____ as United States Application Number or PCT International

Application Number _____ and was amended on (MM/DD/YYYY) _____ (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 specifically referred to above.

I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT international filing date of the continuation-in-part application.

Authorization To Permit Access To Application by Participating Offices

☒ If checked, the undersigned hereby grants the USPTO authority to provide the European Patent Office (EPO), the Japan Patent Office (JPO), the Korean Intellectual Property Office (KIPO), the World Intellectual Property Office (WIPO), and any other intellectual property offices in which a foreign application claiming priority to the above-identified patent application is filed access to the above-identified patent application. See 37 CFR 1.14(c) and (h). This box should not be checked if the applicant does not wish the EPO, JPO, KIPO, WIPO, or other intellectual property office in which a foreign application claiming priority to the above-identified patent application is filed to have access to the above-identified patent application.

In accordance with 37 CFR 1.14(h)(3), access will be provided to a copy of the above-identified patent application with respect to: 1) the above-identified patent application-as-filed; 2) any foreign application to which the above-identified patent application claims priority under 35 U.S.C. 119(a)-(d) if a copy of the foreign application that satisfies the certified copy requirement of 37 CFR 1.55 has been filed in the above-identified patent application; and 3) any U.S. application-as-filed from which benefit is sought in the above-identified patent application.

In accordance with 37 CFR 1.14(c), access may be provided to information concerning the date of filing the Authorization to Permit Access to Application by Participating Offices.

[Page 1 of 3]

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 21 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.

DECLARATION — Utility or Design Patent Application

Claim of Foreign Priority Benefits

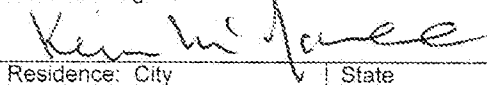
I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or (f), or 365(b) of any foreign application(s) for patent, inventor's or plant breeder's rights certificate(s), or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below, by checking the box, any foreign application for patent, inventor's or plant breeder's rights certificate(s), or any PCT international application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application Number(s)	Country	Foreign Filing Date (MM/DD/YYYY)	Priority Not Claimed	Certified Copy Attached?	
				YES	NO
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐
			☐	☐	☐

☐

Additional foreign application number(s) are listed on a supplemental priority data sheet PTO/SB/02B attached hereto.

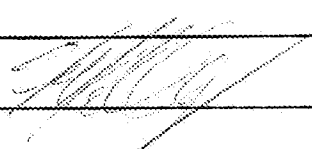
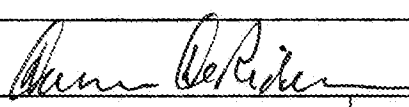
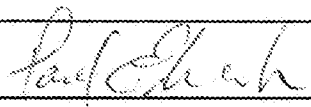
DECLARATION — Utility or Design Patent Application

Direct all correspondence to: ☒ The address associated with Customer Number: 22511		OR ☐ Correspondence address below	
Name			
Address			
City		State	Zip
Country	Telephone		Email
WARNING:			
<p>Petitioner/applicant is cautioned to avoid submitting personal information in documents filed in a patent application that may contribute to identity theft. Personal information such as social security numbers, bank account numbers, or credit card numbers (other than a check or credit card authorization form PTO-2038 submitted for payment purposes) is never required by the USPTO to support a petition or an application. If this type of personal information is included in documents submitted to the USPTO, petitioners/applicants should consider redacting such personal information from the documents before submitting them to the USPTO. Petitioner/applicant is advised that the record of a patent application is available to the public after publication of the application (unless a non-publication request in compliance with 37 CFR 1.213(a) is made in the application) or issuance of a patent. Furthermore, the record from an abandoned application may also be available to the public if the application is referenced in a published application or an issued patent (see 37 CFR 1.14). Checks and credit card authorization forms PTO-2038 submitted for payment purposes are not retained in the application file and therefore are not publicly available. Petitioner/applicant is advised that documents which form the record of a patent application (such as the PTO/SB/01) are placed into the Privacy Act system of records DEPARTMENT OF COMMERCE, COMMERCE-PAT-7, System name: <i>Patent Application Files</i>. Documents not retained in an application file (such as the PTO-2038) are placed into the Privacy Act system of COMMERCE/PAT-TM-10, System name: <i>Deposit Accounts and Electronic Funds Transfer Profiles</i>.</p> <p>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 18 U.S.C. 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.</p>			
NAME OF SOLE OR FIRST INVENTOR:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle [if any])		Family Name or Surname	
Kevin		McNamee	
Inventor's Signature		Date	
		March 28th, 2011	
Residence: City	State	Country	Citizenship
Ottawa	Ontario	Canada	Canadian
Mailing Address			
c/o Kindsight, Inc. 555 Legget Drive, Tower B, Suite 132			
City	State	Zip	Country
Ottawa	Ontario	K2K 2X3	Canada
☒ Additional inventors or a legal representative are being named on the <u>1</u> supplemental sheet(s) PTO/SB/02A or 02LR attached hereto			

[Page 3 of 3]

DECLARATION**ADDITIONAL INVENTOR(S)**
Supplemental Sheet

Page 1 of 1

Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))		Family Name or Surname	
MIKE		PELLEY	
Inventor's Signature 		Date Mar 23/11	
OTTAWA Residence: City	ON State	CANADA Country	CANADIAN Citizenship
c/o Kindsight, Inc. 555 Legget Drive Mailing Address			
Ottawa City	ON State	K2K 2X3 Zip	Canada Country
Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))		Family Name or Surname	
DARREN		DERIDDER	
Inventor's Signature 		Date 28 Mar. 2011	
OTTAWA Residence: City	ON State	CANADA Country	CANADIAN Citizenship
c/o Kindsight, Inc. 555 Legget Drive Mailing Address			
Ottawa City	ON State	K2K 2X3 Zip	CANADA Country
Name of Additional Joint Inventor, if any:		☐ A petition has been filed for this unsigned inventor	
Given Name (first and middle (if any))		Family Name or Surname	
PAUL		EDWARDS	
Inventor's Signature 		Date March 20, 2011	
OTTAWA Residence: City	ON State	CANADA Country	CANADIAN Citizenship
c/o Kindsight, Inc. 555 Legget Drive Mailing Address			
Ottawa City	ON State	K2K 2X3 Zip	CANADA Country

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 21 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.

~~Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.~~

DECLARATION – Supplemental Priority Data Sheet

[illegible]

This collection of information is required by 35 U.S.C. 115 and 37 CFR 1.63. 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 21 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 (1-800-786-9199) and select option 2.

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

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	37617/011002; 08917906US
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION		
<p>The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.</p> <p>This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.</p>			

Secrecy Order 37 CFR 5.2

☐	Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)
--------------------------	---

Applicant Information:

Applicant 1					Remove
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	☐ Party of Interest under 35 U.S.C. 118
Prefix	Given Name	Middle Name	Family Name		Suffix
	Kevin		Mcnamee		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Ottawa	Country Of Residenceⁱ	CA		
Citizenship under 37 CFR 1.41(b)ⁱ		CA			
Mailing Address of Applicant:					
Address 1		c/o Kindsight, Inc.			
Address 2		555 Legget Drive, Tower B, Suite 132			
City	Ottawa	State/Province	ON		
Postal Code	K2K 2X3	Countryⁱ	CA		
Applicant 2					Remove
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	☐ Party of Interest under 35 U.S.C. 118
Prefix	Given Name	Middle Name	Family Name		Suffix
	Mike		Pelley		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Ottawa	Country Of Residenceⁱ	CA		
Citizenship under 37 CFR 1.41(b)ⁱ		CA			
Mailing Address of Applicant:					
Address 1		c/o Kindsight, Inc.			
Address 2		555 Legget Drive			
City	Ottawa	State/Province	ON		
Postal Code	K2K 2X3	Countryⁱ	CA		
Applicant 3					Remove
Applicant Authority		☒ Inventor		☐ Legal Representative under 35 U.S.C. 117	☐ Party of Interest under 35 U.S.C. 118
Prefix	Given Name	Middle Name	Family Name		Suffix
	Darren		Deridder		
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service					
City	Ottawa	Country Of Residenceⁱ	CA		

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	37617/011002; 08917906US
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION		

Citizenship under 37 CFR 1.41(b) i		CA	
Mailing Address of Applicant:			
Address 1	c/o Kindsight, Inc.		
Address 2	555 Legget Drive		
City	Ottawa	State/Province	ON
Postal Code	K2K 2X3	Country ⁱ	CA
Applicant 4			Remove
Applicant Authority		☒ Inventor ☐ Legal Representative under 35 U.S.C. 117 ☐ Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name Suffix
	Paul		Edwards
Residence Information (Select One) ☐ US Residency ☒ Non US Residency ☐ Active US Military Service			
City	Ottawa	Country Of Residence ⁱ	CA
Citizenship under 37 CFR 1.41(b) i		CA	
Mailing Address of Applicant:			
Address 1	c/o Kindsight, Inc.		
Address 2	555 Legget Drive, Tower B, Suite 132		
City	Ottawa	State/Province	ON
Postal Code	K2K 2X3	Country ⁱ	CA
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button. Add			

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
☐ An Address is being provided for the correspondence Information of this application.			
Customer Number	22511		
Email Address	docketing@oshaliang.com	Add Email	Remove Email

Application Information:

Title of the Invention	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION		
Attorney Docket Number	37617/011002; 08917906US	Small Entity Status Claimed	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)	N/A		
Total Number of Drawing Sheets (if any)	8	Suggested Figure for Publication (if any)	

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	37617/011002; 08917906US
		Application Number	
Title of Invention	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION		

Publication Information:

☐	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
☐	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not and will not be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.			
Please Select One:	☒ Customer Number	☐ US Patent Practitioner	☐ Limited Recognition (37 CFR 11.9)
Customer Number	22511		

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.			
Prior Application Status	Pending	Remove	
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61469024	2001-03-29
Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the Add button.			Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
			Remove
Application Number	Country i	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			☐ Yes ☐ No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.	
Assignee 1	Remove

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	37617/011002; 08917906US	
		Application Number		
Title of Invention	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION			

If the Assignee is an Organization check here. ☒			
Organization Name	Kindsight, Inc.		
Mailing Address Information:			
Address 1	755 Ravendale Drive		
Address 2			
City	Mountain View	State/Province	CA
Country i	US	Postal Code	94043
Phone Number		Fax Number	
Email Address			
Additional Assignee Data may be generated within this form by selecting the Add button. Add			

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.					
Signature	/Robert P. Lord/			Date (YYYY-MM-DD)	2011-04-08
First Name	Robert	Last Name	Lord	Registration Number	46479

This collection of information is required by 37 CFR 1.76. 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 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet 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.**

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 the Freedom of Information Act requires disclosure of these records.
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 inspections 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.

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION			
First Named Inventor/Applicant Name:	Kevin McNamee			
Filer:	Rober Lord/Kristina Lalata			
Attorney Docket Number:	37617/011002; 08917906US			
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:				
Claims in excess of 20	2202	5	26	130
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				592

Electronic Acknowledgement Receipt

EFS ID:	9846245
Application Number:	13083501
International Application Number:	
Confirmation Number:	8289
Title of Invention:	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION
First Named Inventor/Applicant Name:	Kevin McNamee
Customer Number:	22511
Filer:	Rober Lord/Kristina Lalata
Filer Authorized By:	Rober Lord
Attorney Docket Number:	37617/011002; 08917906US
Receipt Date:	08-APR-2011
Filing Date:	
Time Stamp:	21:16:11
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$592
RAM confirmation Number	6415
Deposit Account	500591
Authorized User	LORD,ROBERT P.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination fees)

Form PTO-501 (Rev. 10-2009) Page 50

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	37617_011002_Transmittal.pdf	191567	no	1
			7101f5227bd7ff489789fa21b74f0fede3682602		

Warnings:

Information:

2		37617_011002_Specification.pdf	178768	yes	27
			59fc5fada404335474208d02f047e2e0bf876b1d		

Multipart Description/PDF files in .zip description

	Document Description		Start	End
	Specification		1	20
	Claims		21	26
	Abstract		27	27

Warnings:

Information:

3	Drawings-only black and white line drawings	37617_011002_Figures.pdf	106090	no	8
			52b86c884acaace70590d9d57f9dc58f6a7b0b5		

Warnings:

Information:

4	Oath or Declaration filed	37617_011002_Declaration.pdf	5629093	no	6
			90743197ec507ab233e10fee77c69bd12650ef9		

Warnings:

Information:

5	Application Data Sheet	37617_011002_ADS.pdf	1173419	no	5
			bf634c3db8082d18b6e654b69575096f5d882843		

Warnings:

Information:

6	Fee Worksheet (PTO-875)	fee-info.pdf	36999	no	2
			fcf275cb1023e5c5e38c2a9b45cb0b80a35cbf2a		

Warnings:

Information:	
Total Files Size (in bytes):	7315936
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>	

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 13/083,501				
APPLICATION AS FILED - PART I										
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY				
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	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), (l), 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(j))	25	minus 20 = * 5	x 26 =	130	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						
				0.00						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00						
			TOTAL	592		TOTAL				
* If the difference in column 1 is less than zero, enter "0" in column 2.										
APPLICATION AS AMENDED - PART II										
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
AMENDMENT A		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	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))							OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
AMENDMENT B		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	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))							OR		
	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.										



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
13/083,501	04/08/2011	2447	592	37617/011002; 08917906US	25	3

CONFIRMATION NO. 8289

22511
OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

FILING RECEIPT



OC000000047233817

Date Mailed: 04/21/2011

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)

Kevin McNamee, Ottawa, CANADA;
Mike Pelley, Ottawa, CANADA;
Darren Deridder, Ottawa, CANADA;
Paul Edwards, Ottawa, CANADA;

Assignment For Published Patent Application

Kindsight, Inc., Mountain View, CA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/469,024 03/29/2011 *
(*Data provided by applicant is not consistent with PTO records.

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.)

Permission to Access - A proper **Authorization to Permit Access to Application by Participating Offices** (PTO/SB/39 or its equivalent) has been received by the USPTO.

If Required, Foreign Filing License Granted: 04/19/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/083,501**

Projected Publication Date: 10/04/2012

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED
SECURITY MONITORING SOLUTION

Preliminary Class

709

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 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 Assets Control, 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).

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.

<h1 style="text-align: center;">TRANSMITTAL FORM</h1> <p style="text-align: center;"><i>(to be used for all correspondence after initial filing)</i></p>		Application Number	13/083,501-Conf. #8289
		Filing Date	April 8, 2011
		First Named Inventor	Kevin McNamee
		Art Unit	2447
		Examiner Name	Not Yet Assigned
Total Number of Pages in This Submission		Attorney Docket Number	37617/011002

ENCLOSURES (Check all that apply)		
☐ Fee Transmittal Form ☐ Fee Attached ☐ Amendment/Reply ☐ After Final ☐ Affidavits/declaration(s) ☐ Extension of Time Request ☐ Express Abandonment Request ☐ Information Disclosure Statement ☐ Certified Copy of Priority Document(s) ☐ Reply to Missing Parts/Incomplete Application ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53	☐ Drawing(s) ☐ Licensing-related Papers ☐ Petition ☐ Petition to Convert to a Provisional Application ☐ Power of Attorney, Revocation Change of Correspondence Address ☐ Terminal Disclaimer ☐ Request for Refund ☐ CD, Number of CD(s) _____ ☐ Landscape Table on CD	☐ After Allowance Communication to TC ☐ Appeal Communication to Board of Appeals and Interferences ☐ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief) ☐ Proprietary Information ☐ Status Letter ☒ Other Enclosure(s) (please identify below): Supplemental ADS (5 pages)
<div style="border: 1px solid black; padding: 5px; min-height: 80px;"> Remarks </div>		

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT			
Firm Name	OSHA · LIANG LLP		
Signature	/Robert P. Lord/		
Printed name	Robert P. Lord		
Date	May 20, 2011	Reg. No.	46,479

Supplemental Application Data Sheet

Application Information

Application number:: 13/083,501

Filing Date:: 04/08/11

Application Type:: Regular

Subject Matter:: Utility

Suggested Group Art Unit:: 2447

Deleted: N/A

CD-ROM or CD-R?: None

Sequence submission?: None

Computer Readable Form (CRF)?:: No

Title:: METHOD AND SYSTEM FOR OPERATING
SYSTEM IDENTIFICATION IN A
NETWORK BASED SECURITY
MONITORING SOLUTION

Attorney Docket Number:: 37617/011002

Request for Early Publication?: No

Request for Non-Publication?: No

Total Drawing Sheets:: 8

Small Entity?: Yes

Petition included?: No

Secrecy Order in Parent Appl.?: No

Applicant Information

Applicant Authority Type:: Inventor

Primary Citizenship Country:: Canada

Status:: Full Capacity

Given Name:: Kevin
Family Name:: McNamee
City of Residence:: Ottawa
State or Province of Residence:: ON
Country of Residence:: Canada
Street of mailing address:: c/o Kindsight, Inc.
555 Legget Drive, Tower B, Suite 132
City of mailing address:: Ottawa
State or Province of mailing address:: ON
Country of mailing address:: Canada
Postal or Zip Code of mailing address:: K2K 2X3

Applicant Authority Type:: Inventor
Status:: Full Capacity
Given Name:: Mike
Family Name:: Pelley
City of Residence:: Ottawa
State or Province of Residence:: ON
Country of Residence:: Canada
Street of mailing address:: 555 Legget Drive, Tower B, Suite 132
City of mailing address:: Ottawa
State or Province of mailing address:: ON
Country of mailing address:: Canada
Postal or Zip Code of mailing address:: K2K 2X3

Applicant Authority Type:: Inventor
Primary Citizenship Country:: Canada
Status:: Full Capacity
Given Name:: Darren
Family Name:: Deridder
City of Residence:: Ottawa
State or Province of Residence:: ON
Country of Residence:: Canada
Street of mailing address:: 555 Legget Drive, Tower B, Suite 132
City of mailing address:: Ottawa
State or Province of mailing address:: ON
Country of mailing address:: Canada
Postal or Zip Code of mailing address:: K2K 2X3

Applicant Authority Type:: Inventor
Primary Citizenship Country:: Canada
Status:: Full Capacity
Given Name:: Paul
Family Name:: Edwards
City of Residence:: Ottawa
State or Province of Residence:: ON
Country of Residence:: Canada
Street of mailing address:: c/o Kindsight, Inc.
555 Legget Drive, Tower B, Suite 132
City of mailing address:: Ottawa

State or Province of mailing address:: ON
Country of mailing address:: Canada
Postal or Zip Code of mailing address:: K2K 2X3

Correspondence Information

Correspondence Customer Number:: 22511

Representative Information

Representative Customer Number:: 22511

Domestic Priority Information

Application::	Continuity Type::	Parent Application::	Parent Filing Date::
This Application	An application claiming the benefit under 35 USC 119(e)	61/469,024	3/29/2011

Deleted: 3/29/2001

Foreign Priority Information

Assignee Information

Assignee name:: Kindsight, Inc.
Street of mailing address:: 755 Ravendale Drive
City of mailing address:: Mountain View
State or Province of mailing address:: CA
Country of mailing address:: US
Postal or Zip Code of mailing address:: 94043

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.			
Signature	/Robert P. Lord/	Date	May 20, 2011
Name (Print/Type)	Robert P. Lord	Registration No. (Attorney/Agent)	46,479

956246_1

Electronic Acknowledgement Receipt

EFS ID:	10140967
Application Number:	13083501
International Application Number:	
Confirmation Number:	8289
Title of Invention:	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION
First Named Inventor/Applicant Name:	Kevin McNamee
Customer Number:	22511
Filer:	Rober Lord/Jaime Hathaway
Filer Authorized By:	Rober Lord
Attorney Docket Number:	37617/011002; 08917906US
Receipt Date:	20-MAY-2011
Filing Date:	08-APR-2011
Time Stamp:	19:11:26
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	Transmittal Letter	37617_011002_Transmittal.pdf	99732 22b1dfd1d94372cbb6d3544fb3a9158571485515	no	1

Warnings:

Information:

2	Application Data Sheet	37617_011002_Supp_ADS.pdf	111766 f5182cb972104623da7fcd9fd759da5caad19408	no	5
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
Total Files Size (in bytes):				211498	
<p>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.</p> <p><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.</p> <p><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.</p> <p><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.</p>					



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
13/083,501	04/08/2011	Kevin McNamee	37617/011002; 08917906US

CONFIRMATION NO. 8289

22511
OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

PUBLICATION NOTICE



OC000000056919631

Title:METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION

Publication No.US-2012-0255019-A1

Publication Date:10/04/2012

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 Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PLUS Search Results for S/N 13083501, Searched Tue Oct 16 15:52:22 EDT 2012
The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

20120255019 99	6128662 58
8020207 84	
8020207 84	
8250645 84	
20070162909 84	
20080289028 84	
20090328220 84	
20110185418 84	
20110185419 84	
20110197278 84	
20120023257 84	
7949114 71	
7949114 71	
8131997 71	
8156318 71	
8230503 71	
8256664 71	
20060210039 71	
20080163372 71	
20080219162 71	
20080287100 71	
20090044250 71	
20090055918 71	
20090307474 71	
20100100928 71	
20100146621 71	
20110023115 71	
20110185421 71	
20110302653 71	
7577993 68	
7600258 68	
7822818 68	
7823200 68	
20070006026 68	
20070006027 68	
20070006028 68	
20070006308 68	
6049833 58	
6263371 58	
6208620 58	
5740371 58	
6192411 58	
5566225 58	
5835725 58	
5867636 58	
5937169 58	
6021263 58	
6115357 58	
6122276 58	



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.
13/083,501	04/08/2011	Kevin McNamee	37617/011002; 08917906US	8289
22511	7590	02/01/2013	EXAMINER	
OSHA LIANG L.L.P. TWO HOUSTON CENTER 909 FANNIN, SUITE 3500 HOUSTON, TX 77010			NGUYEN, DUSTIN	
			ART UNIT	PAPER NUMBER
			2446	
			NOTIFICATION DATE	DELIVERY MODE
			02/01/2013	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):

docketing@oshaliang.com
hathaway@oshaliang.com
stewart@oshaliang.com

Office Action Summary	Application No. 13/083,501	Applicant(s) MCNAMEE ET AL.	
	Examiner DUSTIN NGUYEN	Art Unit 2446	

-- 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 08 April 2011.
- 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) 1-25 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) 1-25 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 08 April 2011 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).
- a) ☐ All b) ☐ Some * c) ☐ None of:
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) | 3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____. |
| 2) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date ____. | 4) ☐ Other: ____. |

DETAILED ACTION

1. Claims 1-25 are presented for examination.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1, 2, 7-11 and 25 are rejected under 35 U.S.C. 102(b) as being anticipated by Roesch et al. [US Patent No 7,317,693].

4. As per claim 1, Roesch discloses the invention as claimed including a method of network based malware detection in a service provider network [i.e. vulnerability analysis] [col 2, lines 45-56; and col 29, lines 24-31], the method comprising:

receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network [i.e. read a transmitted packet on the network] [Figures 1 and 2; and col 10, lines 37-67], the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network [Figure 9; and col 14, lines 63-col 15, lines 13];

determining an operating system identifier (OS ID) associated with the TCP session and the computing device [i.e. determining an operating system] [Figures 5 and 6; and col 11, lines 64-col 13, lines 25];

determining if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets [i.e. service identification to determine if a machine infected with a virus] [Figures 15 and 16; and col 22, lines 55-col 24, lines 36]; and

generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert [i.e. recorded information is reported to an IDS or a NMS] [col 2, lines 54-56; and col 14, lines 50-62].

5. As per claim 2, Roesch discloses wherein determining the operating system ID further comprises: determining a protocol associated with the TCP packets and matching an OS fingerprint from one or more protocol parameters if present in the TCP packets to determine a first operating system identifier (ID); determining an application parameter associated with the TCP session if present, and identifying a second OS ID from the application parameter; and wherein the OS ID in the alert comprises one of the first OS ID or second OS ID associated with one or more computing devices coupled to the access device [i.e. selecting an operating system of a network device from the results of two or more OS identification] [col 6, lines 25-35; and col 26, lines 46-col 27, lines 63].

6. As per claim 7, Roesch discloses wherein determining the first OS ID is performed by comparing one or more protocol parameters of the one or more TCP packets having a SYN flag associated with the session, wherein the OS fingerprints identify the protocol parameters of the SYN flagged packet and the OS ID associated with parameters [Figure 6; and col 12, lines 48-col 13, lines 25].

7. As per claim 8, Roesch discloses wherein determining the application parameter associated with the session and identifying the second OS ID from the application parameter by inspecting an HTTP user agent string to determine the second OS ID [col 31, lines 28-38].

8. As per claim 9, Roesch discloses verifying the first OS ID against the second OS ID, wherein if the second OS ID does not match the first OS ID the session is identified by the OS ID identified as a more reliable OS ID [Figure 20; and col 26, lines 57-col 27, lines 52].

9. As per claim 10, Roesch discloses verifying the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID either OS ID is used [Figure 20; and col 26, lines 57-col 27, lines 52].

10. As per claim 11, Roesch discloses verifying the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID but the second OS ID provides additional information, the second OS ID is used [Figure 20; and col 26, lines 57-col 27, lines 52].

11. As per claim 25, it is rejected for similar reasons as stated above in claim 1.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 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 negated by the manner in which the invention was made.

13. Claims 3-6, 12, 16-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roesch et al. [US Patent No 7,317,693], in view of Cheng et al. [US Patent No 8,065,712].

14. As per claim 3, Roesch does not specifically disclose sending a notification to a subscriber associated with the network address associated with the access device, the notification identifying a remediation portal to remove the determined malware in the alert. Cheng discloses sending a notification to a subscriber associated with the network address associated with the access device [i.e. notifying user] [col 12, lines 50-54], the notification identifying a remediation portal to remove the determined malware in the alert [i.e. the client may be redirected to remediation resources] [Abstract]. It would have been obvious to a person skill in the art at the time the invention was made to combine the teaching of Roesch, and Cheng because the teaching of Cheng would enable to provide a system and method for qualifying a client machine to access a network, based on policies governing required virus

Art Unit: 2446

checking, operating system updates, worm, adware and/or malware protection [Cheng, col 3, lines 12-15].

15. As per claim 4, Cheng discloses identifying at the remediation portal the subscriber accessing the remediation portal; identifying the OS associated with the computing device used by the subscriber to access the remediation portal; comparing the OS associated with the computing device to the at least one of the first OS ID or second OS ID identified in the alert [i.e. qualifying a client] [Figure 4; and col 10, lines 63-col 14, lines 8]; and providing malware remediation to the computing device when the at least one of the first OS ID or second OS ID matches the OS associated with the computing device [i.e. operating system updates can be downloaded as a remediation package] [col 13, lines 17-20].

16. As per claim 5, Cheng discloses wherein if the OS of the computing device is not the at least one of the first OS ID or second OS ID identified in the alert an indication is provided to the subscriber to connect to the remediation portal with an other computing device connected to the access device [i.e. qualifying a client machine to access a network] [Figure 4; and col 10, lines 63-col 14, lines 10].

17. As per claim 6, Cheng discloses wherein the alert is cleared when all computing devices associated with the access device and the computing device having the at least one of the first OS ID or second OS ID have accessed the remediation portal [col 10, lines 63-col 14, lines 8].

Art Unit: 2446

18. As per claim 12, Cheng discloses wherein sending the notification to the subscriber associated with the access device further comprises replacing the network address of the access device with a subscriber ID [col 10, lines 24-43].

19. As per claim 16, it is rejected for similar reasons as stated above in claims 1 and 4.

20. As per claims 17 and 18, they are rejected for similar reasons as stated above in claims 2 and 3.

21. As per claim 19, it is rejected for similar reasons as stated above in claim 12.

22. As per claims 20-24, they are rejected for similar reasons as stated above in claims 7-11.

23. Claims 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Roesch et al. [US Patent No 7,317,693], in view of Cheng et al. [US Patent No 8,065,712], and further in view of Aziz et al. [US Patent Application No 2007/0250930].

24. As per claim 14, Roesch and Cheng do not specifically disclose wherein the one or more computing devices are coupled to the access device through a local area network (LAN), the access device providing network address translation (NAT) or is coupled to NAT device to share the network address of the access device. Aziz discloses wherein the one or more

Art Unit: 2446

computing devices are coupled to the access device through a local area network (LAN), the access device providing network address translation (NAT) or is coupled to NAT device to share the network address of the access device [paragraphs 0048 and 0080]. It would have been obvious to a person skill in the art at the time the invention was made to combine the teaching of Roesch, Cheng and Aziz because the teaching of Aziz would enable to provide a system to prevent the spread of malware [Aziz, paragraph 0003].

25. As per claim 15, Roesch discloses wherein the network address is an Internet Protocol (IP) address or a Media Access Control (MAC) address [Figures 2 and 5].

26. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Roesch et al. [US Patent No 7,317,693], in view of Cheng et al. [US Patent No 8,065,712], and further in view of Beer [US Patent Application No 2008/0282338].

27. As per claim 13, Roesch and Cheng do not specifically disclose wherein sending the notification to the subscriber associated with the access device further comprises aggregating one or more detailed alerts having the subscriber ID into a single alert summary associated with the subscriber ID. Beer discloses wherein sending the notification to the subscriber associated with the access device further comprises aggregating one or more detailed alerts having the subscriber ID into a single alert summary associated with the subscriber ID [paragraphs 0047 and 0059]. It would have been obvious to a person skill in the art at the time the invention was

Art Unit: 2446

made to combine the teaching of Roesch, Cheng and Beer because the teaching of Beer would enable to provide a system and method for deterring the reception of malicious or objectionable content transmitted through a network [Beer, paragraph 0002].

28. A shortened statutory period for response to this action is set to expire **3 (three) months and 0 (zero) days** from the mail date of this letter. Failure to respond within the period for response will result in **ABANDONMENT** of the application (see 35 U.S.C 133, M.P.E.P 710.02, 710.02(b)).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dustin Nguyen whose telephone number is (571) 272-3971. The examiner can normally be reached on flex.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kamal Divecha can be reached at (571) 272-5863. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2446

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).

/DUSTIN NGUYEN/
Primary Examiner, Art Unit 2446

Notice of References Cited	Application/Control No. 13/083,501		Applicant(s)/Patent Under Reexamination MCNAMEE ET AL.	
	Examiner DUSTIN NGUYEN		Art Unit 2446	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2007/0250930	10-2007	Aziz et al.	726/24
*	B	US-8,065,712	11-2011	Cheng et al.	726/1
*	C	US-7,317,693	01-2008	Roesch et al.	370/252
*	D	US-2008/0282338	11-2008	BEER, KEVIN J.	726/12
*	E	US-2011/0213869	09-2011	Korsunsky et al.	709/223
*	F	US-8,020,211	09-2011	Keanini et al.	726/25
	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.



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. 8289

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
13/083,501	04/08/2011	726	2446	37617/011002; 08917906US		
APPLICANTS Kevin McNamee, Ottawa, CANADA; Mike Pelley, Ottawa, CANADA; Darren Deridder, Ottawa, CANADA; Paul Edwards, Ottawa, CANADA; ** CONTINUING DATA ***** This appln claims benefit of 61/469,024 03/29/2011 * (*)Data provided by applicant is not consistent with PTO records. ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED *** SMALL ENTITY ** 04/19/2011						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and /DUSTIN NGUYEN/ Acknowledged Examiner's Signature		☐ Met after Allowance DN Initials	STATE OR COUNTRY CANADA	SHEETS DRAWINGS 8	TOTAL CLAIMS 25	INDEPENDENT CLAIMS 3
ADDRESS OSHA LIANG L.L.P. TWO HOUSTON CENTER 909 FANNIN, SUITE 3500 HOUSTON, TX 77010 UNITED STATES						
TITLE METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION						
FILING FEE RECEIVED 592	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		

Index of Claims



Application/Control No.

13/083,501

Examiner

DUSTIN NGUYEN

Applicant(s)/Patent under Reexamination

MCNAMEE ET AL.

Art Unit

2446

✓	Rejected
=	Allowed

—	(Through numeral) Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claim		Date									
Final	Original	1/20/13									
	1	v									
	2	v									
	3	v									
	4	v									
	5	v									
	6	v									
	7	v									
	8	v									
	9	v									
	10	v									
	11	v									
	12	v									
	13	v									
	14	v									
	15	v									
	16	v									
	17	v									
	18	v									
	19	v									
	20	v									
	21	v									
	22	v									
	23	v									
	24	v									
	25	v									
	26										
	27										
	28										
	29										
	30										
	31										
	32										
	33										
	34										
	35										
	36										
	37										
	38										
	39										
	40										
	41										
	42										
	43										
	44										
	45										
	46										
	47										
	48										
	49										
	50										

Claim		Date									
Final	Original										
	51										
	52										
	53										
	54										
	55										
	56										
	57										
	58										
	59										
	60										
	61										
	62										
	63										
	64										
	65										
	66										
	67										
	68										
	69										
	70										
	71										
	72										
	73										
	74										
	75										
	76										
	77										
	78										
	79										
	80										
	81										
	82										
	83										
	84										
	85										
	86										
	87										
	88										
	89										
	90										
	91										
	92										
	93										
	94										
	95										
	96										
	97										
	98										
	99										
	100										

Claim		Date									
Final	Original										
	101										
	102										
	103										
	104										
	105										
	106										
	107										
	108										
	109										
	110										
	111										
	112										
	113										
	114										
	115										
	116										
	117										
	118										
	119										
	120										
	121										
	122										
	123										
	124										
	125										
	126										
	127										
	128										
	129										
	130										
	131										
	132										
	133										
	134										
	135										
	136										
	137										
	138										
	139										
	140										
	141										
	142										
	143										
	144										
	145										
	146										
	147										
	148										
	149										
	150										

Search Notes

Application/Control No.

13/083,501

Examiner

DUSTIN NGUYEN

Applicant(s)/Patent under
Reexamination

MCNAMEE ET AL.

Art Unit

2446

SEARCHED

Class	Subclass	Date	Examiner
726	1, 12, 24, 25	1/20/2013	DN
709	223	1/20/2013	DN
370	252	1/20/2013	DN

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner

**SEARCH NOTES
(INCLUDING SEARCH STRATEGY)**

	DATE	EXMR
search EAST	1/20/2013	DN
inventor search	1/20/2013	DN

Docket No.: 37617/011002
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kevin McNamee et al.

Application No.: 13/083,501

Confirmation No.: 8289

Filed: April 8, 2011

Art Unit: 2446

For: METHOD AND SYSTEM FOR OPERATING
SYSTEM IDENTIFICATION IN A NETWORK
BASED SECURITY MONITORING
SOLUTION

Examiner: D. Nguyen

REPLY UNDER 37 C.F.R. § 1.111

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

Dear Madam:

In response to the Office Action dated February 1, 2013 (hereinafter “Action”),
please reconsider this application in view of the following.

AMENDMENTS TO THE CLAIMS

Please amend the claims as follows.

1. (Original) A method of network based malware detection in a service provider network, the method comprising:
 - receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network, the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network;
 - determining an operating system identifier (OS ID) associated with the TCP session and the computing device;
 - determining if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets; and
 - generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert.
2. (Original) The method of claim 1 wherein determining the operating system ID further comprises:
 - determining a protocol associated with the TCP packets and matching an OS fingerprint from one or more protocol parameters if present in the TCP packets to determine a first operating system identifier (ID);
 - determining an application parameter associated with the TCP session if present, and identifying a second OS ID from the application parameter; and
 - wherein the OS ID in the alert comprises one of the first OS ID or second OS ID associated with one or more computing devices coupled to the access device.
3. (Original) The method of claim 2 further comprising sending a notification to a subscriber associated with the network address associated with the access device, the notification identifying a remediation portal to remove the determined malware in the alert.

4. (Original) The method of claim 3 further comprising:
 - identifying at the remediation portal the subscriber accessing the remediation portal;
 - identifying the OS associated with the computing device used by the subscriber to access the remediation portal;
 - comparing the OS associated with the computing device to the at least one of the first OS ID or second OS ID identified in the alert; and
 - providing malware remediation to the computing device when the at least one of the first OS ID or second OS ID matches the OS associated with the computing device.
5. (Original) The method of claim 3 wherein if the OS of the computing device is not the at least one of the first OS ID or second OS ID identified in the alert an indication is provided to the subscriber to connect to the remediation portal with an other computing device connected to the access device.
6. (Original) The method of claim 3 wherein the alert is cleared when all computing devices associated with the access device and the computing device having the at least one of the first OS ID or second OS ID have accessed the remediation portal.
7. (Original) The method of claim 2 wherein determining the first OS ID is performed by comparing one or more protocol parameters of the one or more TCP packets having a SYN flag associated with the session, wherein the OS fingerprints identify the protocol parameters of the SYN flagged packet and the OS ID associated with parameters.
8. (Original) The method of claim 2 wherein determining the application parameter associated with the session and identifying the second OS ID from the application parameter by inspecting an HTTP user agent string to determine the second OS ID.
9. (Original) The method of claim 2 further comprising verifying the first OS ID against the second OS ID, wherein if the second OS ID does not match the first OS ID the session is identified by the OS ID identified as a more reliable OS ID.

10. (Original) The method of claim 2 further comprising verifying the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID either OS ID is used.
11. (Original) The method of claim 2 further comprising verifying the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID but the second OS ID provides additional information, the second OS ID is used.
12. (Original) The method of claim 3 wherein sending the notification to the subscriber associated with the access device further comprises replacing the network address of the access device with a subscriber ID.
13. (Original) The method of claim 12 wherein sending the notification to the subscriber associated with the access device further comprises aggregating one or more detailed alerts having the subscriber ID into a single alert summary associated with the subscriber ID.
14. (Original) The method of claim 12 wherein the one or more computing devices are coupled to the access device through a local area network (LAN), the access device providing network address translation (NAT) or is coupled to NAT device to share the network address of the access device.
15. (Cancelled)
16. (Currently Amended) A system for network based malware detection in a service provider network, the system comprising:
 - a plurality of network ~~sensor~~ sensors coupled to the service provider network, each of the network ~~sensor~~ sensors for:
 - receiving ~~receives~~ one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network, the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network;

~~determining~~ determines an operating system identifier (OS ID) associated with the TCP session and the computing device associated;
~~determining~~ determines if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets; and
~~generating~~ generates an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert. [[:]] [[and]]
~~a remediation portal coupled to the service provider network, the remediation portal [[:]] identifies a subscriber accessing the remediation portal [[:]] identifies the OS associated with the computing device used by the subscriber to access the remediation portal [[:]] compares the OS associated with the computing device to the OS ID identified in the alert [[:]] [[and]] provides malware remediation to the computing device [[:]]~~

17. (Currently Amended) The system of claim 16 wherein the plurality of network sensors in determining the operating system OS ID at the network sensor further:

~~determine~~ determines a protocol associated with the TCP packets and matching an OS fingerprint from one or more protocol parameters if present in the TCP packets to determine a first ~~operating system identifier (ID)~~ OS ID;
~~determine~~ determines an application parameter associated with the TCP session if present, and identifying a second OS ID from the application parameter; and
 wherein the identified OS ID in the alert comprises one of the first OS ID or the second OS ID associated with one or more computing devices coupled to the access device.

18. (Currently Amended) The system of claim ~~17~~ 16 ~~further comprising an alert manager to~~ wherein the plurality of network sensors further: send a notification to a subscriber associated with the network address associated with the access device, the notification identifying ~~[[the]]~~ a remediation portal to remove the determined malware in the alert.

19. (Currently Amended) The system of claim 18 wherein the plurality of network sensors send ~~sending~~ the notification to the subscriber associated with the access device ~~further comprises~~ by retrieving a subscriber ID from a subscriber ID repository and replacing the network address of the access device with the subscriber ID.
20. (Currently Amended) The system of claim 17 wherein the plurality of network sensors ~~determine network sensor determines~~ the first OS ID by comparing one or more protocol parameters of the one or more TCP packets having a SYN flag associated with the session, the OS fingerprints identify the protocol parameters of the SYN flagged packet and the OS ID associated with parameters.
21. (Currently Amended) The system of claim 20 wherein the plurality of network sensors ~~determine network sensor determines~~ the application parameter associated with the session and identifies the second OS ID from the application parameter by inspecting an HTTP user agent string to determine the second OS ID.
22. (Currently Amended) The system of claim 21 wherein the plurality of network sensors verify ~~network sensor verifies~~ the first OS ID against the second OS ID, wherein if the second OS ID does not match the first OS ID the session is identified by the OS ID ~~identified as~~ providing a more reliable OS ID.
23. (Currently Amended) The system of claim 21 wherein the plurality of network sensors verify ~~network sensor verifies~~ the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID either OS ID is used.
24. (Currently Amended) The system of claim 21 wherein the plurality of network sensors verify ~~network sensor verifies~~ the first OS ID against the second OS ID, wherein if the second OS ID matches the first OS ID but the second OS ID provides additional information, the second OS ID is used.

25. (Original) A computer readable memory containing instructions for network based malware detection in a service provider network, the instructions when executed by a processor performing:

- receiving one or more transmission control protocol (TCP) packets originating from an access device coupled to the service provider network, the one or more TCP packets defining a TCP session between a computing device coupled to the access device, and a destination coupled to the service provider network;
- determining an operating system identifier (OS ID) associated with the TCP session and the computing device;
- determining if malware is present in the TCP session and an associated malware ID by comparing a malware signature to the one or more TCP packets; and
- generating an alert identifying a network address associated with the access device, the malware ID and the OS ID associated with TCP session that generated the alert.

26. (New) The system of claim 16 further comprising:

- a remediation portal coupled to the service provider network, the remediation portal for:
 - identifying a subscriber accessing the remediation portal;
 - identifying the OS associated with the computing device used by the subscriber to access the remediation portal;
 - comparing the OS associated with the computing device to the OS ID identified in the alert; and
 - providing malware remediation to the computing device.

REMARKS

Please reconsider the application in view of the above amendments and the following remarks. Applicants thank the Examiner for carefully considering this application and for indicating the acceptance of the drawings filed on April 8, 2011.

Disposition of Claims

Claims 1-25 were pending in the present application. By way of this reply, claim 15 is cancelled without prejudice or disclaimer. Also by way of this reply, new claim 26 is added. Accordingly, claims 1-14 and 16-26 are now pending in the present application. Claims 1, 16, and 25 are independent. The remaining claims depend, either directly or indirectly, from claims 1 and 16.

Claim Amendments

By way of this reply, claims 16-24 are amended for clarification. Applicants respectfully assert that no new matter is added by way of these amendments.

Rejections under 35 U.S.C. § 102

Claims 1, 2, 7-11, and 25 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by U.S. Patent No. 7,317,693 (hereinafter "Roesch"). For the reasons set forth below, this rejection is respectfully traversed.

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *See Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The

identical invention must be shown in as complete detail as is contained in the claim. *See Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989).

In order to anticipate under 35 U.S.C. § 102, the prior art reference must not only disclose all elements of the claim within the four corners of the document, but must also disclose those elements arranged as in the claim. The “arranged as in the claim” requirement applies to all claims and refers to the need for an anticipatory reference to show all the limitations of the claims arranged or combined in the same way as recited in the claims. *See Net Moneyin, Inc. v. Verisign, Inc.*, 2007-1565, at 15 and 16 (Fed. Cir. 2008).

One or more embodiments of the claimed invention provide a system and method that allows network based malware detection to be used effectively in a service provider’s network, where the devices are typically connected to the network through an access device, such as a modem or router. In service provider networks it is difficult for individual devices to be identified that are located behind the access device since the individual devices will utilize the network address of the access device (*see* originally-filed specification at paragraph [0020]). However, as disclosed by the originally-filed specification, it is possible to determine: a) if a device is infected with malware based on associated network traffic; and b) an identifier of an operating system of the device that is associated with the network traffic. By fingerprinting a device’s OS through the network traffic it is possible to identify the device that was determined to be infected with malware and therefore target remediation operations to the individual device as opposed to all devices connected to the access device.

According to amended independent claim 1, the method receives packets from an access device and determines an OS ID of a computing device sending the packets. The method also determines if malware is present by comparing the TCP packets to one or more malware signatures. When a malware signature matches one or more of the TCP packets the method generates an alert identifying the network address of the access device as well as an identification of the malware and the OS ID associated with the TCP packets.

In contrast, Roesch discloses systems and methods for determining the topology of a network by identifying a host configuration of a computer network. According to Roesch, network traffic is analyzed in order to identify operating systems and services that are running on devices connected to a network (*see* Roesch, col. 10, lines 19 – 27). The systems and methods of Roesch allow the network topology to be determined from network traffic. The network topology provides information as to what services are running on the network as well as their network addresses and other parameters of the device (*see* Roesch, Figure 2; col. 10, line 56 – col. 11, line 6; col. 14, lines 22 - 36). This network topology can be used in managing the network and assessing potential vulnerabilities of the network (*see* Roesch, col. 29, lines 24 – 39).

Applicants respectfully assert that Roesch fails to disclose at least determining from the network traffic if malware is present or determining an OS ID of the associated device, as recited by independent claims 1 and 25. The Examiner has pointed to Figures 15 and 16 as well as col 22, line 55 to col 24, line 36 of Roesch as disclosing service identification to determine if a machine is infected with a virus. Applicants respectfully assert that Roesch fails to disclose identifying

malware on a device. Instead, the passage noted by the Examiner discloses, in part (*see* Roesch, col 22, lines 55 – 64):

Services are generally served on well-known ports of a host. It is possible for an administrator or an unauthorized user acting as an administrator, however, to configure a system to bind services to alternate ports. It is also possible for a machine infected with a virus to bind services to non-standard ports. For this reason it is necessary to validate a service based on its data rather than its port.

In other words, Roesch discloses that the port a service is bound to (*i.e.*, the port the service listens to) can be changed, either by an administrator, an imposter of an administrator or a virus. Since the port number of a service can be changed, the port number should not be relied upon for identifying services. Applicants respectfully assert that Roesch fails to disclose that identification of malware present on a computing device can be determined from the network traffic.

In view of the above, the Examiner's contentions and the cited art do not support an anticipation rejection of independent claims 1 and 25. Claims 2 and 7-11 depend, either directly or indirectly, from claim 1. Accordingly, the Examiner's contentions and the cited art also do not support an anticipation rejection of claims 2 and 7-11, and withdrawal of this rejection is respectfully requested.

Rejections under 35 U.S.C. § 103

Claims 3-6 and 12-24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Roesch, in view of U.S. Patent No. 8,065,712 (hereinafter "Cheng"), in view of U.S. Patent Publication No. 2007/0250930 (hereinafter "Aziz"), and in further view of U.S. Patent Publication

No. 2008/0282338 (hereinafter “Beer”). By way of this reply, claim 15 is cancelled and thus the rejection is moot as to claim 15. As for remaining claims 3-6, 12-14, and 16-24, for the reasons set forth below, this rejection is respectfully traversed.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). Further, all the 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). When determining whether a claim is obvious, an Examiner must 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 added). The necessary presence of all claim features is axiomatic, since the Supreme Court has long held that obviousness is a question of law based on underlying factual inquiries, including ascertaining the differences between *the claimed invention* and the prior art. *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966) (emphasis added). Lastly, obviousness requires at least a suggestion of all of the features of a claim, since the Supreme Court in *KSR Int’l v. Teleflex Inc.* stated that “there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness.” *KSR Int’l v. Teleflex Inc.*, 127 S. Ct. 1727, 1741 (2007) (*quoting In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

As discussed above, Roesch fails to disclose or render obvious each and every limitation of independent claim 1. Amended independent claim 16 recites limitations that are similar to

independent claim 1. Accordingly, Roesch also fails to disclose or render obvious each and every limitation of amended independent claim 16.

None of the additionally cited references relied upon by the Examiner provide any teachings, which when combined with those of Roesch, would lead one of ordinary skill in the art to the subject matter provided by either independent claims 1 or 16.

Cheng teaches methods and devices for qualifying a client machine to access a network based on policies governing required protective measures such as virus checking and OS updates. *See* Chen at Abstract.

Aziz teaches a system for capturing suspicious activity. The system of Aziz includes a tap configured to copy network data from a communication network and a controller coupled to the tap. The controller is configured to receive the copy of the network data from the tap and analyze the network data with a heuristic to determine if the network data is suspicious. Suspicious network data is flagged and the transmission of the network data to a plurality of destination devices is concurrently simulated. *See* Aziz at Abstract.

Beer teaches a system and method for preventing the reception and transmission of malicious or objectionable content through a network. According to Beer, a thin client is installed on a user computer and is associated with a web browser on the computer. The web browser and thin client are coupled to a web proxy server of a network service provider. A protective server is located intermediate the web proxy server and the network. According to Beer the protective server

detects a type of malicious or objectionable content and attempts to deter the reception of the detected content by the user computer. *See Beer at Abstract.*

However, Chen, Aziz, and Beer do not cure what Roesch lacks. Accordingly, Roesch, Chen, Aziz, and Beer, whether viewed separately or in combination, fail to disclose or render obvious each and every limitation of independent claims 1 and 16.

In view of the above, the Examiner contentions and the cited art do not support an obviousness rejection of independent claims 1 and 16. Claims 3-6, 12-14, and 17-24 depend, either directly or indirectly, from claims 1 and 16. Accordingly, the Examiner contentions and the cited art also do not support an obviousness rejection of claims 3-6, 12-14, and 17-24, and withdrawal of this rejection is respectfully requested.

New Claims

New claim 26 is added by way of this reply. Applicants respectfully assert that no new matter is added by way of new claim 26, as support for new claim 26 may be found, for example, in original claim 16.

As discussed above, the Examiner's contentions and the cited art do not support an obviousness rejection of amended independent claim 16. New claim 26 depends directly from claim 16. Accordingly, the Examiner's contentions and the cited art also do not support an obviousness rejection of new claim 26. Thus, favorable consideration of new claim 26 is respectfully requested.

Conclusion

Applicants believe this reply is fully responsive to all outstanding issues and places this application in condition for allowance. If this belief is incorrect, or other issues arise, the Examiner is encouraged to contact the undersigned or his associates at the telephone number listed below. Please apply any charges not covered, or any credits, to Deposit Account 50-0591 (Reference Number 37617/011002).

Dated: May 30, 2013

Respectfully submitted,

By /Robert P. Lord/

Robert P. Lord

Registration No.: 46,479

OSHA · LIANG LLP

3945 Freedom Circle, Suite 300

Santa Clara, California 95054

(408) 727-0600

(408) 727-8778 (Fax)

Attorney for Applicants

Electronic Patent Application Fee Transmittal

Application Number:	13083501			
Filing Date:	08-Apr-2011			
Title of Invention:	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION			
First Named Inventor/Applicant Name:	Kevin McNamee			
Filer:	Rober Lord/Jaime Hathaway			
Attorney Docket Number:	37617/011002; 08917906US			
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:				
Extension - 1 month with \$0 paid	2251	1	FOR TIME	002 Page 970

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				100

Electronic Acknowledgement Receipt

EFS ID:	15912373
Application Number:	13083501
International Application Number:	
Confirmation Number:	8289
Title of Invention:	METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION
First Named Inventor/Applicant Name:	Kevin McNamee
Customer Number:	22511
Filer:	Rober Lord/Jaime Hathaway
Filer Authorized By:	Rober Lord
Attorney Docket Number:	37617/011002; 08917906US
Receipt Date:	30-MAY-2013
Filing Date:	08-APR-2011
Time Stamp:	20:27:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Credit Card
Payment was successfully received in RAM	\$ 100
RAM confirmation Number	6475
Deposit Account	500591
Authorized User	LORD, ROBERT P.

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination fees)

Form PTO-510 (Rev. 12-2012) Page 99

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	37617_011002_Transmittal.pdf	89167 94fd58de9ada92caa950fa382c75a1b3c47c0ef1	no	1

Warnings:

Information:

2	Extension of Time	37617_011002_Ex_Time.pdf	132140 f68b317089c9484081e72638bc21ddff89d5baa7	no	1
---	-------------------	--------------------------	--	----	---

Warnings:

Information:

3		37617_011002_Response.pdf	153397 fe2e2ec12c293f474f562f041afdaf74c9310a7e	yes	15
---	--	---------------------------	--	-----	----

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Claims	2	7
Applicant Arguments/Remarks Made in an Amendment	8	15

Warnings:

Information:

4	Fee Worksheet (SB06)	fee-info.pdf	30713 af234e37d71780672a470ae5d1fb08502f8db9c9	no	2
---	----------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes):			405417
------------------------------	--	--	--------

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.

AMENDMENT TRANSMITTAL LETTER			Docket No. 37617/011002	
Application No. 13/083,501-Conf. #8289	Filing Date April 8, 2011	Examiner D. Nguyen	Art Unit 2446	

Applicant(s): Kevin McNamee et al.

Invention: METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION

TO THE COMMISSIONER FOR PATENTS

Transmitted herewith is an amendment in the above-identified application.

The fee has been calculated and is transmitted as shown below.

CLAIMS AS AMENDED					
	Claims Remaining After Amendment	Highest Number Previously Paid	Number Extra Claims Present	Rate	
Total Claims	25	- 25 =	0	x 40.00	0.00
Independent Claims	3	- 3 =	0	x 210.00	0.00
Multiple Dependent Claims (check if applicable) ☐					
Other fee (please specify): Extension for response within first month					100.00
TOTAL ADDITIONAL FEE FOR THIS AMENDMENT:					100.00

☐ Large Entity
 ☒ Small Entity

☐ No additional fee is required for this amendment.

☐ Please charge Deposit Account No. 50-0591 in the amount of \$ _____.

☐ A check in the amount of \$ _____ to cover the filing fee is enclosed.

☒ Payment by credit card.

☒ The Director is hereby authorized to charge and credit Deposit Account No. 50-0591 as described below. A duplicate copy of this sheet is enclosed.

☒ Credit any overpayment.

☒ Charge any additional filing or application processing fees required under 37 C.F.R. § 1.16 and 1.17.

/Robert P. Lord/

Robert P. Lord

Attorney/Agent Reg. No.: 46,479

OSHA · LIANG LLP

3945 Freedom Circle, Suite 300

Santa Clara, California 95054

(408) 727-0600

Dated: May 30, 2013

22511

PATENT TRADEMARK OFFICE

PTO/AIA/22 (03-13)

Approved for use through 03/31/2013. 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.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)		Docket Number (Optional) 37617/011002	
Application Number 13/083,501-Conf. #8289		Filed April 8, 2011	
For METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION			
Art Unit 2446		Examiner D. Nguyen	

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application. The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☒ One month (37 CFR 1.17(a)(1))	\$200	\$100	\$50	\$ 100.00
☐ Two months (37 CFR 1.17(a)(2))	\$600	\$300	\$150	\$
☐ Three months (37 CFR 1.17(a)(3))	\$1,400	\$700	\$350	\$
☐ Four months (37 CFR 1.17(a)(4))	\$2,200	\$1,100	\$550	\$
☐ Five months (37 CFR 1.17(a)(5))	\$3000	\$1,500	\$750	\$

☒ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☒ Payment by credit card.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to
Deposit Account Number 50-0591 .

☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant.

☒ attorney or agent of record. Registration Number 46,479 .

☐ attorney or agent acting under 37 CFR 1.34. Registration number .

/Robert P. Lord/
Signature

Robert P. Lord
Typed or printed name

May 30, 2013
Date

(408) 727-0600
Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐

*Total of 1 forms are submitted.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 13/083,501		Filing Date 04/08/2011		☐ 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)							
AMENDMENT	05/30/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)			
	Total (37 CFR 1.16(i))	* 26	Minus	** 25	= 1	X \$40 =		40			
	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		40			
(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					
<p>* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.</p> <p>** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".</p> <p>*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".</p> <p>The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.</p>										LIE /DEANNA RORIE/	

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

22511 7590 09/12/2013
OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

EXAMINER

NGUYEN, DUSTIN

ART UNIT

PAPER NUMBER

2446

DATE MAILED: 09/12/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

13/083,501

04/08/2011

Kevin McNamee

37617/011002;

8289

TITLE OF INVENTION: METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$890	\$300	\$0	\$1190	12/12/2013

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.

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)

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.

22511 7590 09/12/2013
OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

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.
13/083,501	04/08/2011	Kevin McNamee	37617/011002; 08917906US	8289

TITLE OF INVENTION: METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$890	\$300	\$0	\$1190	12/12/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
NGUYEN, DUSTIN	2446	726-024000

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, 1 _____ (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. 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 credit 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 form 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: 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 United States Patent and Trademark Office.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____

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, 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.



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.
13/083,501	04/08/2011	Kevin McNamee	37617/011002; 08917906US	8289
22511	7590	09/12/2013	EXAMINER	
OSHA LIANG L.L.P. TWO HOUSTON CENTER 909 FANNIN, SUITE 3500 HOUSTON, TX 77010			NGUYEN, DUSTIN	
			ART UNIT	PAPER NUMBER
			2446	

DATE MAILED: 09/12/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 209 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 209 day(s).

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 Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

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. 13/083,501	Applicant(s) MCNAMEE ET AL.	
	Examiner DUSTIN NGUYEN	Art Unit 2446	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 05/30/2013.
☐ 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 1-14 and 16-26, now renumbered as 1-25. 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) | 5. ☐ Examiner's Amendment/Comment |
| 2. ☐ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ | 6. ☐ Examiner's Statement of Reasons for Allowance |
| 3. ☐ Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 7. ☐ Other _____. |
| 4. ☐ Interview Summary (PTO-413),
Paper No./Mail Date _____. | |

/DUSTIN NGUYEN/
Primary Examiner, Art Unit 2446

Notice of References Cited	Application/Control No. 13/083,501		Applicant(s)/Patent Under Reexamination MCNAMEE ET AL.	
	Examiner DUSTIN NGUYEN		Art Unit 2446	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2012/0204266	08-2012	Yoo, InSeon	726/24
*	B	US-7,627,898	12-2009	Beck et al.	726/23
*	C	US-8,429,746	04-2013	Capalik, Alen	726/23
*	D	US-2011/0004935	01-2011	Moffie et al.	726/23
	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.

Index of Claims



Application/Control No.

13/083,501

Examiner

DUSTIN NGUYEN

Applicant(s)/Patent under Reexamination

MCNAMEE ET AL.

Art Unit

2446

✓	Rejected
=	Allowed

—	(Through numeral) Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claim		Date									
Final	Original	9/3/13									
1	1	=									
2	2	=									
3	3	=									
4	4	=									
5	5	=									
6	6	=									
7	7	=									
8	8	=									
9	9	=									
10	10	=									
11	11	=									
12	12	=									
13	13	=									
14	14	=									
	15										
15	16	=									
16	17	=									
17	18	=									
18	19	=									
19	20	=									
20	21	=									
21	22	=									
22	23	=									
23	24	=									
24	25	=									
25	26	=									
	27										
	28										
	29										
	30										
	31										
	32										
	33										
	34										
	35										
	36										
	37										
	38										
	39										
	40										
	41										
	42										
	43										
	44										
	45										
	46										
	47										
	48										
	49										
	50										

Claim		Date									
Final	Original										
	51										
	52										
	53										
	54										
	55										
	56										
	57										
	58										
	59										
	60										
	61										
	62										
	63										
	64										
	65										
	66										
	67										
	68										
	69										
	70										
	71										
	72										
	73										
	74										
	75										
	76										
	77										
	78										
	79										
	80										
	81										
	82										
	83										
	84										
	85										
	86										
	87										
	88										
	89										
	90										
	91										
	92										
	93										
	94										
	95										
	96										
	97										
	98										
	99										
	100										

Claim		Date									
Final	Original										
	101										
	102										
	103										
	104										
	105										
	106										
	107										
	108										
	109										
	110										
	111										
	112										
	113										
	114										
	115										
	116										
	117										
	118										
	119										
	120										
	121										
	122										
	123										
	124										
	125										
	126										
	127										
	128										
	129										
	130										
	131										
	132										
	133										
	134										
	135										
	136										
	137										
	138										
	139										
	140										
	141										
	142										
	143										
	144										
	145										
	146										
	147										
	148										
	149										
	150										

Issue Classification 	Application/Control No. 13/083,501	Applicant(s)/Patent under Reexamination MCNAMEE ET AL.
	Examiner DUSTIN NGUYEN	Art Unit 2446

ISSUE CLASSIFICATION												
ORIGINAL				INTERNATIONAL CLASSIFICATION								
CLASS		SUBCLASS		CLAIMED				NON-CLAIMED				
726		24		G	06	F	11	/00				/
CROSS REFERENCES				G	06	F	12	/14, 16				/
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)											
709	224							/				/
								/				/
								/				/
								/				/
								/				/

(Assistant Examiner) (Date)	/DUSTIN NGUYEN/ 09/03/2013 (Primary Examiner) (Date)	Total Claims Allowed: 25	
(Legal Instruments Examiner) (Date)		O.G. Print Claim(s) 1	O.G. Print Fig. 1

☐ 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		
1	1		31		61		91		121		151		181		
2	2		32		62		92		122		152		182		
3	3		33		63		93		123		153		183		
4	4		34		64		94		124		154		184		
5	5		35		65		95		125		155		185		
6	6		36		66		96		126		156		186		
7	7		37		67		97		127		157		187		
8	8		38		68		98		128		158		188		
9	9		39		69		99		129		159		189		
10	10		40		70		100		130		160		190		
11	11		41		71		101		131		161		191		
12	12		42		72		102		132		162		192		
13	13		43		73		103		133		163		193		
14	14		44		74		104		134		164		194		
	15		45		75		105		135		165		195		
15	16		46		76		106		136		166		196		
16	17		47		77		107		137		167		197		
17	18		48		78		108		138		168		198		
18	19		49		79		109		139		169		199		
19	20		50		80		110		140		170		200		
20	21		51		81		111		141		171		201		
21	22		52		82		112		142		172		202		
22	23		53		83		113		143		173		203		
23	24		54		84		114		144		174		204		
24	25		55		85		115		145		175		205		
25	26		56		86		116		146		176		206		
	27		57		87		117		147		177		207		
	28		58		88		118		148		178		208		
	29		59		89		119		149		179		209		
	30		60		90		120		150		180		210		

IEEE.org | IEEE Xplore Digital Library | IEEE Standards | IEEE Spectrum | More Sites



Access provided by:
United States Patent and
Trademark Office
Sign Out



SEARCH RESULTS

You searched for: malware operating system identifier compare tcp detect
14 Results returned

Detecting stealth software with Strider GhostBuster

Yi-Min Wang ; Sleek, D. ; Vo, B. ; Roussev, R. ; Verbowski, C.
Dependable Systems and Networks, 2005. DSN 2005.
Proceedings. International Conference on
Digital Object Identifier: 10.1109/DSN.2005.39
Publication Year: 2005 , Page(s): 368 - 377
Cited by: Papers (17) | Patents (19)
IEEE CONFERENCE PUBLICATIONS

HERO: A novel malware detection framework based on binary translation

Haoran Guo ; Jianmin Pang ; Yichi Zhang ; Feng Yue ;
Rongcai Zhao
Intelligent Computing and Intelligent Systems (ICIS), 2010
IEEE International Conference on
Volume: 1
Digital Object Identifier: 10.1109/ICICISYS.2010.5658566
Publication Year: 2010 , Page(s): 411 - 415
Cited by: Papers (2)
IEEE CONFERENCE PUBLICATIONS

A Session-based Mobile Socket Layer for Disruption Tolerance on the Internet

Kimura, B. ; Guardia, H. ; Moreira, E.
Mobile Computing, IEEE Transactions on
Volume: PP , Issue: 99
Digital Object Identifier: 10.1109/TMC.2013.76
Publication Year: 2013 , Page(s): 1
IEEE EARLY ACCESS ARTICLES

A New Malware Detection Method based on Raw Information

Qiao-Ling Han ; Yu-Jie Hao ; Yan Zhang ; Zhi-Peng Lu ;
Rui Zhang
Apperceiving Computing and Intelligence Analysis, 2008.
ICACIA 2008. International Conference on
Digital Object Identifier: 10.1109/ICACIA.2008.4770030
Publication Year: 2008 , Page(s): 307 - 310
IEEE CONFERENCE PUBLICATIONS

Malware Clearance for Secure Commitment of OS-Level Virtual Machines

Zhiyong Shan ; Xin Wang ; Tzi-cker Chiueh
Dependable and Secure Computing, IEEE Transactions on
Volume: 10 , Issue: 2
Digital Object Identifier: 10.1109/TDSC.2012.88
Publication Year: 2013 , Page(s): 70 - 83
IEEE JOURNALS & MAGAZINES

Survey on malware evasion techniques: State of the art and challenges

Marpaung, J.A.P. ; Sain, M. ; Hoon-Jae Lee
Advanced Communication Technology (ICACT), 2012 14th
International Conference on

Publication Year: 2012 , Page(s): 744 - 749

Cited by: Papers (1)

IEEE CONFERENCE PUBLICATIONS

Behavior-Based Malware Detection on Mobile Phone

Shuaifu Dai ; Yaxin Liu ; Tietei Wang ; Tao Wei ; Wei Zou
Wireless Communications Networking and Mobile Computing
(WiCOM), 2010 5th International Conference on
Digital Object Identifier: 10.1109/WICOM.2010.5501291
Publication Year: 2010 , Page(s): 1 - 4

Cited by: Papers (2)

IEEE CONFERENCE PUBLICATIONS

Performance comparison of four anomaly detectors in detecting self-propagating malware on endpoints

Ashtaq, A.B. ; Khayam, S.A.
Biometrics and Security Technologies, 2008. ISBAST 2008.
International Symposium on
Digital Object Identifier: 10.1109/ISBAST.2008.4547650
Publication Year: 2008 , Page(s): 1 - 9

IEEE CONFERENCE PUBLICATIONS

A throughput deadlock-free TCP for high-speed Internet

Chang, R.K.C. ; Chan, H.Y.
Networks, 2000. (ICON 2000). Proceedings. IEEE International
Conference on
Digital Object Identifier: 10.1109/ICON.2000.875773
Publication Year: 2000 , Page(s): 87 - 92

IEEE CONFERENCE PUBLICATIONS

BTMD: A Framework of Binary Translation Based Malcode Detector

Zheng Shan ; Haoran Guo ; Jianmin Pang
Cyber-Enabled Distributed Computing and Knowledge
Discovery (CyberC), 2012 International Conference on
Digital Object Identifier: 10.1109/CyberC.2012.16
Publication Year: 2012 , Page(s): 39 - 43

IEEE CONFERENCE PUBLICATIONS

Fingerprinting custom botnet protocol stacks

DiBenedetto, S. ; Gadkari, K. ; Diel, N. ; Steiner, A. ;
Massey, D. ; Papadopoulos, C.
Secure Network Protocols (NPSec), 2010 6th IEEE Workshop
on
Digital Object Identifier: 10.1109/NPSEC.2010.5634448
Publication Year: 2010 , Page(s): 61 - 66

IEEE CONFERENCE PUBLICATIONS

ModChecker: Kernel Module Integrity Checking in the Cloud Environment

Ahmed, I. ; Zoranic, A. ; Javaid, S. ; Richard, G.G.
Parallel Processing Workshops (ICPPW), 2012 41st
International Conference on
Digital Object Identifier: 10.1109/ICPPW.2012.46
Publication Year: 2012 , Page(s): 306 - 313

IEEE CONFERENCE PUBLICATIONS

Passive testing on TCP

Dongluo Chen ; Jianping Wu ; HuiCheng Chi
Communication Technology Proceedings, 2003. ICCT 2003.
International Conference on
Volume: 1
Digital Object Identifier: 10.1109/ICCT.2003.1209064
Publication Year: 2003 , Page(s): 182 - 186 vol.1

IEEE CONFERENCE PUBLICATIONS

Sensor in the Dark: Building Untraceable Large-Scale Honeypots Using Virtualization Technologies

Shimoda, A. ; Mori, T. ; Goto, S.

Applications and the Internet (SAINT), 2010 10th IEEE/IPSJ International Symposium on

Digital Object Identifier: 10.1109/SAINT.2010.42

Publication Year: 2010 ; Page(s): 22 - 30

IEEE CONFERENCE PUBLICATIONS

[Sign In](#) | [Create Account](#)**IEEE Account**[Change Username/Password](#)[Update Address](#)**Purchase Details**[Payment Options](#)[Order History](#)[Access Purchased Documents](#)**Profile Information**[Communications Preferences](#)[Profession and Education](#)[Technical Interests](#)**Need Help?**[US & Canada: +1 800 678 4330](#)[Worldwide: +1 732 981 0080](#)[Contact & Support](#)[About IEEE Xplore](#) | [Contact](#) | [Help](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Site Map](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest professional association for the advancement of technology.

© Copyright 2013 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.



Searching for: (tcp and operating and system and identifier and malware and signature and alert and compare and packet) ([start a new search](#))

Found **36** within *The ACM Guide to Computing Literature* (Bibliographic citations from major publishers in computing)

Limit your search to [Publications from ACM and Affiliated Organizations](#) (Full-Text collection: **384,083** items)

REFINE YOUR SEARCH

▼ Refine by Keywords

▼ Refine by People

[Names](#)
[Institutions](#)
[Authors](#)
[Reviewers](#)

▼ Refine by Publications

[Publication Year](#)
[Publication Names](#)
[ACM Publications](#)
[All Publications](#)
[Content Formats](#)
[Publishers](#)

▼ Refine by Conferences

[Sponsors](#)
[Events](#)
[Proceeding Series](#)

ADVANCED SEARCH

[Advanced Search](#)

FEEDBACK

[Please provide us with feedback](#)

Found **36** of **2,132,334**

Search Results

Results 1 - 20 of 36

Related Journals

Related Magazines

Related SIGs

Related Conferences

Sort by [relevance](#) in [expanded](#)

Result page: [1](#) [2](#) [n](#)

1 [Analysis of connectivity and session management for mobile peer-to-peer applications](#)

[Olso Kassinen, Timo Koskela, Erkki Mäntylä, Jukka Pekkari, Mika Ylämä](#)

June 2009

Journal of Mobile Multimedia, Volume 5 Issue 2

Publisher: Rinton Press, Incorporated

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

Mobile applications utilizing wireless networks are growing in popularity as increasingly capable terminals and advanced networking technologies emerge. In order to provide a seamless user experience, applications must be able to rely on intelligent ...

Keywords: content distribution, cross-layer optimization, mobile middleware, state machines

2 [Attribution of malicious behavior](#)

[Jonathon Giffin, Abhinav Srivastava](#)

December 2010

ICISS'10: Proceedings of the 6th international conference on Information systems security

Publisher: Springer-Verlag

Full text available: [Publisher Site](#)

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

Internet-connected computer systems face ongoing software attacks. Existing defensive solutions, such as intrusion detection systems, rely on the ability to identify malicious software (malware) in order to prevent its installation. This approach remains ...

3 [Communications of the ACM: Volume 55 Issue 8](#)

August 2012

Communications of the ACM

Publisher: ACM

Full text available: [Digital Edition](#), [PDF](#) (8.38 MB)

Bibliometrics: Downloads (6 Weeks): 1971, Downloads (12 Months): 41378, Downloads (Overall): 54515, Citation Count:

4 [Semantic context aware security policy deployment](#)

[Siera Prada, Frédéric Cuppens, Nora Cuppens-Boutahia, Joaquin G. Alfaro, Laurent Louvain, Yehia Elkhalby](#)

March 2009

ASI ACCS '09: Proceedings of the 4th International Symposium on Information, Computer, and Communications Security

Publisher: ACM [Request Permissions](#)

Full text available: [Pdf](#) (1.54 MB)

Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 53, Downloads (Overall): 540, Citation Count: 4

The successful deployment of a security policy is closely related not only to the complexity of the security requirements, but also to the capabilities/functionalities of the security devices. The complexity of the security requirements is additive ...

Keywords: PDP, PEP, access control, network security

5 [ATLANTIDES: an architecture for alert verification in network intrusion detection systems](#)

[Damiano Bozoni, Bruno Crispo, Sandro Etalle](#)

November 2007

LISA'07: Proceedings of the 21st conference on Large Installation System Administration Conference

Publisher: USENIX Association

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 0, Downloads (Overall): 10, Citation Count: 4

We present an architecture designed for alert verification (i.e., to reduce false positives) in network intrusion-detection systems. Our technique is based on a systematic (and automatic) anomaly-based analysis of the system output, which provides useful ...

6 [An architecture for generating semantics-aware signatures](#)

[Vinod Yegneswaran, Jonathon T. Giffin, Paul Barford, Somesh Jha](#)

July 2005

SSYM'05: Proceedings of the 14th conference on USENIX Security Symposium - Volume 14, v

Publisher: USENIX Association

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 0, Downloads (Overall): 67, Citation Count: 32

Identifying new intrusions and developing effective signatures that detect them is essential for protecting computer networks. We present Nemean, a system for automatic generation of intrusion signatures from honeynet packet tra
Our architecture ...

7 [Characterizing Intelligence Gathering and Control on an Edge Network](#)

[Martin Ariitt](#), [Niklas Carlsson](#), [Phillipa Gill](#), [Aniket Mahanti](#), [Carey Williamson](#)

July 2011 **Transactions on Internet Technology (TOIT)**, Volume 11 Issue 1

Publisher: ACM [Request Permissions](#)

Full text available: [PDF](#) (5.12 MB)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 64, Downloads (Overall): 265, Citation Count:

There is a continuous struggle for control of resources at every organization that is connected to the Internet. The organization wishes to use its resources to achieve strategic goals. Some external entities seek direct control of the resources, ...

Keywords: Workload characterization

8 [Communications of the ACM: Volume 53 Issue 2](#)

February 2010 **Communications of the ACM**

Publisher: ACM

Full text available: [Digital Edition](#), [PDF](#) (19.69 MB)

Bibliometrics: Downloads (6 Weeks): 3325, Downloads (12 Months): 32461, Downloads (Overall): 282109, Citation Co

9 [A secure energy-efficient m-banking application for mobile devices](#)

[Maria-Dolores Cano](#), [Gines Domenech-Asensi](#)

November 2011 **Journal of Systems and Software**, Volume 84 Issue 11

Publisher: Elsevier Science Inc.

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

Mobile banking is one of the emerging services in telecommunications due to the explosive increase in the number mobile customers around the world. Solutions for mobile banking are varied, ranging from the use of Wireless Tran
Layer Security, ...

Keywords: Application-layer protocol, Energy-efficient protocol, Mobile banking, Security, Wireless networks

10 [Not-a-Bot: improving service availability in the face of botnet attacks](#)

[Ramakrishna Gummadi](#), [Hari Balakrishnan](#), [Petros Maniatis](#), [Sylvia Ratnasamy](#)

April 2009 **NSDI'09: Proceedings of the 6th USENIX symposium on Networked systems design and implement**

Publisher: USENIX Association

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 18

A large fraction of email spam, distributed denial-of-service (DDoS) attacks, and click-fraud on web advertisements caused by traffic sent from compromised machines that form botnets. This paper posits that by identifying human-generated traffic ...

11 [Communications of the ACM: Volume 55 Issue 1](#)

January 2012 **Communications of the ACM**

Publisher: ACM

Full text available: [Digital Edition](#), [PDF](#) (9.41 MB)

Bibliometrics: Downloads (6 Weeks): 4612, Downloads (12 Months): 39176, Downloads (Overall): 113847, Citation Co

12 [Communications of the ACM: Volume 53 Issue 12](#)

December 2010 **Communications of the ACM**

Publisher: ACM

Full text available: [Digital Edition](#), [PDF](#) (6.57 MB)

Bibliometrics: Downloads (6 Weeks): 1119, Downloads (12 Months): 11821, Downloads (Overall): 94745, Citation Cou

13 [Communications of the ACM: Volume 54 Issue 11](#)

November 2011 **Communications of the ACM**

Publisher: ACM

Full text available: [Digital Edition](#), [PDF](#) (8.42 MB)

Bibliometrics: Downloads (6 Weeks): 3921, Downloads (12 Months): 26710, Downloads (Overall): 88331, Citation Cou

14 [Communications of the ACM: Volume 52 Issue 9](#)

September 2009 **Communications of the ACM**

Publisher: ACM

Full text available: [Digital Edition](#), [PDF](#) (7.28 MB)

Bibliometrics: Downloads (6 Weeks): 2834, Downloads (12 Months): 27763, Downloads (Overall): 256609, Citation Co

15 Puppetnets: misusing web browsers as a distributed attack infrastructure

 V. T. Lam, S. Antonatos, P. Akrividis, K. G. Anagnostakis

October 2006

CCS '06: Proceedings of the 13th ACM conference on Computer and communications security

Publisher: ACM  [Request Permissions](#)

Full text available:  [PDF](#) (871.35 KB)

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 44, Downloads (Overall): 1671, Citation Count: 23

Most of the recent work on Web security focuses on preventing attacks that *directly* harm the browser's host machine user. In this paper we attempt to quantify the threat of browsers being *indirectly* misused for attacking third parties.

Keywords: distributed attacks, malicious software, web security

16 Communications of the ACM: Volume 55 Issue 3

 March 2012

Communications of the ACM

Publisher: ACM

Full text available:  [Digital Edition](#),  [PDF](#) (10.61 MB)

Bibliometrics: Downloads (6 Weeks): 1254, Downloads (12 Months): 13646, Downloads (Overall): 62715, Citation Count: 23

17 A service model for network security applications

 [Mario Riccardi](#)

April 2010

CS IIRW '10: Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research

Publisher: ACM  [Request Permissions](#)

Full text available:  [PDF](#) (587.40 KB)

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 51, Downloads (Overall): 289, Citation Count: 1

We describe a new architecture designed to outsource the complexity of configuring, deploying and operating network security monitoring systems. Our architecture is designed to allow the concurrent operation of best-of-breed network security applications ...

Keywords: anomaly detection, cloud computing, cyber-security, honeypot, intrusion detection, management systems, network security, sensor

18 A robust SNMP based infrastructure for intrusion detection and response in tactical MANETs

[Marko Jahnske](#), [Jens Tölle](#), [Gischa Lettgen](#), [Michael Bussmann](#), [Uwe Weddige](#)

July 2006

DIMVA'06: Proceedings of the Third international conference on Detection of Intrusions and Malware & Vulnerability Assessment

Publisher: Springer-Verlag

Full text available:  [Publisher Site](#)

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 1

Intrusion Detection Systems (IDS) for adhoc networks need secure, reliable, flexible, and lightweight infrastructure exchanging available sensor data and security event messages. Cooperation is a major concept of Mobile Adhoc Networks (MANETs). ...

19 Improving the performance of passive network monitoring applications with memory locality enhancements

[Antonis Papadogiannakis](#), [Giorgos Vasiliadis](#), [Dimitris Antoniadis](#), [Michalis Pavchironakis](#), [Evangelos P. Markatos](#)

January 2012

Computer Communications, Volume 35 Issue 1

Publisher: Elsevier Science Publishers B. V.

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 1

Passive network monitoring is the basis for a multitude of systems that support the robust, efficient, and secure operation of modern computer networks. Emerging network monitoring applications are more demanding in terms of memory and CPU resources ...

Keywords: Intrusion detection systems, Locality buffering, Packet capturing, Passive network monitoring

20 Argos: an emulator for fingerprinting zero-day attacks for advertised honeypots with automatic signature generation



[Georgios Portokalidis](#), [Asia Slowinska](#), [Herbert Bos](#)

April 2006 **EuroSys '06**: Proceedings of the 1st ACM SIGOPS/EuroSys European Conference on Computer Systems

Publisher: ACM

Full text available:  [PDF](#) (471.94 KB)

Bibliometrics: Downloads (6 Weeks): 23, Downloads (12 Months): 101, Downloads (Overall): 866, Citation Count: 44

As modern operating systems and software become larger and more complex, they are more likely to contain bugs may allow attackers to gain illegitimate access. A fast and reliable mechanism to discern and generate vaccines for attacks is vital ...

Also published in:

October 2006 **SIGOPS Operating Systems Review** Volume 40 Issue 4

Result page: [1](#) [2](#) [3](#)

The ACM Digital Library is published by the Association for Computing Machinery. Copyright © 2013 ACM, Inc.

[Terms of Use](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)



US Patent & Trademark Office

SIGN IN SIGN UP

Searching for: (tcp and operating and system and identifier and malware and signature and alert and compare and packet) ([start a new search](#))Found **36** within *The ACM Guide to Computing Literature* (Bibliographic citations from major publishers in computing)Limit your search to [Publications from ACM and Affiliated Organizations](#) (Full-Text collection: **384,083** items)

REFINE YOUR SEARCH

Search Results

Related Journals

Related Magazines

Related SIGs

Related Conferences

Results 21 - 36 of 36

Sort by {relevance} in {expanded}

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#) [33](#) [34](#) [35](#) [36](#)

▼ Refine by Keywords

▼ Refine by People

[Names](#)
[Institutions](#)
[Authors](#)
[Reviewers](#)

▼ Refine by Publications

[Publication Year](#)
[Publication Names](#)
[ACM Publications](#)
[All Publications](#)
[Content Formats](#)
[Publishers](#)

▼ Refine by Conferences

[Sponsors](#)
[Events](#)
[Proceeding Series](#)

ADVANCED SEARCH

[Advanced Search](#)

FEEDBACK

[Please provide us with feedback](#)Found **36** of **2,132,334****21** [Dynamic spyware analysis](#)[Manuel Eggels, Christopher Kruegel, Engin Kirda, Hong Yin, Dawn Song](#)June 2007 **ATC'07: 2007 USENIX Annual Technical Conference on Proceedings of the USENIX Annual Technical Conference****Publisher:** USENIX Association**Bibliometrics:** Downloads (6 Weeks): 0, Downloads (12 Months): 0, Downloads (Overall): 15, Citation Count: 48

Spyware is a class of malicious code that is surreptitiously installed on victims' machines. Once active, it silently monitors the behavior of users, records their web surfing habits, and steals their passwords. Current anti-spyware tools operate in ...

22 [Communications of the ACM: Volume 54 Issue 3](#)

March 2011

Communications of the ACM

Publisher: ACMFull text available: [Digital Edition](#), [PDF](#) (11.32 MB)**Bibliometrics:** Downloads (6 Weeks): 3173, Downloads (12 Months): 19696, Downloads (Overall): 82671, Citation Count: 0**23** [Communications of the ACM: Volume 54 Issue 8](#)

August 2011

Communications of the ACM

Publisher: ACMFull text available: [Digital Edition](#), [PDF](#) (7.31 MB)**Bibliometrics:** Downloads (6 Weeks): 5587, Downloads (12 Months): 41333, Downloads (Overall): 128099, Citation Count: 0**24** [Babel: a secure computer is a polyglot](#)[John Aycock, Daniel Medeiros Nunes de Castro, Michael E. Locasto, Chris Jarahek](#)

October 2012

CCSW '12: Proceedings of the 2012 ACM Workshop on Cloud computing security workshop**Publisher:** ACM [Request Permissions](#)Full text available: [PDF](#) (510.18 KB)**Bibliometrics:** Downloads (6 Weeks): 10, Downloads (12 Months): 109, Downloads (Overall): 109, Citation Count: 0

Why should a user's computer be trusted at all? We propose a new model of the computer, Babel, that makes a user's computer appear as it normally would, but is actually untrusted to the point where it cannot run the code installed on it. Each computer, ...

Keywords: client-server, diversity**25** [Communications of the ACM: Volume 53 Issue 8](#)

August 2010

Communications of the ACM

Publisher: ACMFull text available: [Digital Edition](#), [PDF](#) (14.13 MB)**Bibliometrics:** Downloads (6 Weeks): 2152, Downloads (12 Months): 17889, Downloads (Overall): 146512, Citation Count: 0**26** [Communications of the ACM: Volume 55 Issue 11](#)

November 2012

Communications of the ACM

Publisher: ACMFull text available: [Digital Edition](#), [PDF](#) (8.36 MB)**Bibliometrics:** Downloads (6 Weeks): 4241, Downloads (12 Months): 118953, Downloads (Overall): 118953, Citation Count: 0**27** [Proximity breeds danger: emerging threats in metro-area wireless networks](#)[P. Akrividis, W. Y. Chin, V. T. Lam, S. Sidiropoulos, E. G. Anagnostakis](#)

August 2007

SS'07: Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium**Publisher:** USENIX Association**Bibliometrics:** Downloads (6 Weeks): 0, Downloads (12 Months): 0, Downloads (Overall): 17, Citation Count: 9

The growing popularity of wireless networks and mobile devices is starting to attract unwanted attention especially potential targets for malicious activities reach critical mass. In this study, we try to quantify the threat from large-scale distributed ...

28 [Communications of the ACM: Volume 54 Issue 5](#)

May 2011

Communications of the ACM

Publisher: ACM

Full text available: [Digital Edition](#), [PDF](#) (7.71 MB)

Bibliometrics: Downloads (6 Weeks): 4883, Downloads (12 Months): 41573, Downloads (Overall): 167281, Citation Co

29 [The feature selection and intrusion detection problems](#)

[Andrew H. Sung](#), [Srinivas Mulkamala](#)

December 2004 **ASI AN'04**: Proceedings of the 9th Asian Computing Science conference on Advances in Computer Science dedicated to Jean-Louis Lassez on the Occasion of His 5th Cycle Birthday

Publisher: Springer-Verlag

Full text available: [Publisher Site](#)

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count:

Cyber security is a serious global concern. The potential of cyber terrorism has posed a threat to national security; meanwhile the increasing prevalence of malware and incidents of cyber attacks hinder the utilization of the Internet's greatest ...

30 [Automatic handling of protocol dependencies and reaction to 0-day attacks with scriptgen based honeypots](#)

[Corrado Leita](#), [Marc Dacier](#), [Frederic Massicotte](#)

September 2006 **RAID'06**: Proceedings of the 9th international conference on Recent Advances in Intrusion Detection

Publisher: Springer-Verlag

Full text available: [Publisher Site](#)

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 4

Spitzner proposed to classify honeypots into low, medium and high interaction ones. Several instances of low interaction exist, such as honeyd, as well as high interaction, such as GenII. Medium interaction systems have recently received increased attention. ...

31 [Puppetnets: Misusing Web Browsers as a Distributed Attack Infrastructure](#)

[Spiros Antonatos](#), [Periklis Akrividis](#), [Vinh The Lam](#), [Kostas G. Anagnostakis](#)

December 2008

Transactions on Information and System Security (TISSEC), Volume 12 Issue 2

Publisher: ACM [Request Permissions](#)

Full text available: [PDF](#) (1.55 MB)

Bibliometrics: Downloads (6 Weeks): 6, Downloads (12 Months): 73, Downloads (Overall): 961, Citation Count: 2

Most of the recent work on Web security focuses on preventing attacks that directly harm the browser's host machine user. In this paper we attempt to quantify the threat of browsers being indirectly misused for attacking third parties. Specifically, ...

Keywords: Web security, distributed attacks, malicious software

32 [Privacy oracle: a system for finding application leaks with black box differential testing](#)

[Jaeyoon Jung](#), [Amotz Shain](#), [Ben Greenstein](#), [David Wetherall](#), [Gabriel Magana](#), [Tadayoshi Kohno](#)

October 2008

CCS '08: Proceedings of the 15th ACM conference on Computer and communications security

Publisher: ACM [Request Permissions](#)

Full text available: [PDF](#) (455.75 KB)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 72, Downloads (Overall): 625, Citation Count: 10

We describe the design and implementation of Privacy Oracle, a system that reports on application leaks of user information via the network traffic that they send. Privacy Oracle treats each application as a black box, without access to either its internal ...

Keywords: black-box testing, data loss prevention, differential fuzz testing, personal information leaks, sequence alignment algorithm

33 [Internet Security Glossary](#)

[R. Shirey](#)

May 2000

Internet Security Glossary

Publisher: RFC Editor

Full text available: [Text](#) (489.29 KB)

Bibliometrics: Downloads (6 Weeks): 1, Downloads (12 Months): 10, Downloads (Overall): 761, Citation Count: 24

This Glossary (191 pages of definitions and 13 pages of references) provides abbreviations, explanations, and recommendations for use of information system security terminology. The intent is to improve the comprehensibility of writing that deals with ...

34 [Communications of the ACM: Volume 53 Issue 6](#)

 June 2010

Communications of the ACM

Publisher: ACM

Full text available:  [Digital Edition](#) ,  [PDF](#)

Bibliometrics: Downloads (6 Weeks): 1698, Downloads (12 Months): 16065, Downloads (Overall): 112546, Citation Co

35 [SweetBait: Zero-hour worm detection and containment using low- and high-interaction honeypots](#)

[Georgios Portokalidis](#), [Herbert Bos](#)

April 2007

Computer Networks: The International Journal of Computer and Telecommunications Network
Volume 51 Issue 5

Publisher: Elsevier North-Holland, Inc.

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Downloads (Overall): n/a, Citation Count: 3

As next-generation computer worms may spread within minutes to millions of hosts, protection via human intervention is no longer an option. We discuss the implementation of SweetBait, an automated protection system that employs low- and high-interaction ...

Keywords: Emulators, Honeypots, Intrusion detection/prevention, Security

36 [Communications of the ACM: Volume 55 Issue 6](#)

 June 2012

Communications of the ACM

Publisher: ACM

Full text available:  [Digital Edition](#) ,  [PDF](#) (10.85 MB)

Bibliometrics: Downloads (6 Weeks): 1650, Downloads (12 Months): 21373, Downloads (Overall): 54879, Citation Cou

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [11](#) [12](#) [13](#) [14](#) [15](#) [16](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#) [33](#) [34](#) [35](#) [36](#) [37](#) [38](#) [39](#) [40](#) [41](#) [42](#) [43](#) [44](#) [45](#) [46](#) [47](#) [48](#) [49](#) [50](#) [51](#) [52](#) [53](#) [54](#) [55](#) [56](#) [57](#) [58](#) [59](#) [60](#) [61](#) [62](#) [63](#) [64](#) [65](#) [66](#) [67](#) [68](#) [69](#) [70](#) [71](#) [72](#) [73](#) [74](#) [75](#) [76](#) [77](#) [78](#) [79](#) [80](#) [81](#) [82](#) [83](#) [84](#) [85](#) [86](#) [87](#) [88](#) [89](#) [90](#) [91](#) [92](#) [93](#) [94](#) [95](#) [96](#) [97](#) [98](#) [99](#) [100](#) [101](#) [102](#) [103](#) [104](#) [105](#) [106](#) [107](#) [108](#) [109](#) [110](#) [111](#) [112](#) [113](#) [114](#) [115](#) [116](#) [117](#) [118](#) [119](#) [120](#) [121](#) [122](#) [123](#) [124](#) [125](#) [126](#) [127](#) [128](#) [129](#) [130](#) [131](#) [132](#) [133](#) [134](#) [135](#) [136](#) [137](#) [138](#) [139](#) [140](#) [141](#) [142](#) [143](#) [144](#) [145](#) [146](#) [147](#) [148](#) [149](#) [150](#) [151](#) [152](#) [153](#) [154](#) [155](#) [156](#) [157](#) [158](#) [159](#) [160](#) [161](#) [162](#) [163](#) [164](#) [165](#) [166](#) [167](#) [168](#) [169](#) [170](#) [171](#) [172](#) [173](#) [174](#) [175](#) [176](#) [177](#) [178](#) [179](#) [180](#) [181](#) [182](#) [183](#) [184](#) [185](#) [186](#) [187](#) [188](#) [189](#) [190](#) [191](#) [192](#) [193](#) [194](#) [195](#) [196](#) [197](#) [198](#) [199](#) [200](#) [201](#) [202](#) [203](#) [204](#) [205](#) [206](#) [207](#) [208](#) [209](#) [210](#) [211](#) [212](#) [213](#) [214](#) [215](#) [216](#) [217](#) [218](#) [219](#) [220](#) [221](#) [222](#) [223](#) [224](#) [225](#) [226](#) [227](#) [228](#) [229](#) [230](#) [231](#) [232](#) [233](#) [234](#) [235](#) [236](#) [237](#) [238](#) [239](#) [240](#) [241](#) [242](#) [243](#) [244](#) [245](#) [246](#) [247](#) [248](#) [249](#) [250](#) [251](#) [252](#) [253](#) [254](#) [255](#) [256](#) [257](#) [258](#) [259](#) [260](#) [261](#) [262](#) [263](#) [264](#) [265](#) [266](#) [267](#) [268](#) [269](#) [270](#) [271](#) [272](#) [273](#) [274](#) [275](#) [276](#) [277](#) [278](#) [279](#) [280](#) [281](#) [282](#) [283](#) [284](#) [285](#) [286](#) [287](#) [288](#) [289](#) [290](#) [291](#) [292](#) [293](#) [294](#) [295](#) [296](#) [297](#) [298](#) [299](#) [300](#) [301](#) [302](#) [303](#) [304](#) [305](#) [306](#) [307](#) [308](#) [309](#) [310](#) [311](#) [312](#) [313](#) [314](#) [315](#) [316](#) [317](#) [318](#) [319](#) [320](#) [321](#) [322](#) [323](#) [324](#) [325](#) [326](#) [327](#) [328](#) [329](#) [330](#) [331](#) [332](#) [333](#) [334](#) [335](#) [336](#) [337](#) [338](#) [339](#) [340](#) [341](#) [342](#) [343](#) [344](#) [345](#) [346](#) [347](#) [348](#) [349](#) [350](#) [351](#) [352](#) [353](#) [354](#) [355](#) [356](#) [357](#) [358](#) [359](#) [360](#) [361](#) [362](#) [363](#) [364](#) [365](#) [366](#) [367](#) [368](#) [369](#) [370](#) [371](#) [372](#) [373](#) [374](#) [375](#) [376](#) [377](#) [378](#) [379](#) [380](#) [381](#) [382](#) [383](#) [384](#) [385](#) [386](#) [387](#) [388](#) [389](#) [390](#) [391](#) [392](#) [393](#) [394](#) [395](#) [396](#) [397](#) [398](#) [399](#) [400](#) [401](#) [402](#) [403](#) [404](#) [405](#) [406](#) [407](#) [408](#) [409](#) [410](#) [411](#) [412](#) [413](#) [414](#) [415](#) [416](#) [417](#) [418](#) [419](#) [420](#) [421](#) [422](#) [423](#) [424](#) [425](#) [426](#) [427](#) [428](#) [429](#) [430](#) [431](#) [432](#) [433](#) [434](#) [435](#) [436](#) [437](#) [438](#) [439](#) [440](#) [441](#) [442](#) [443](#) [444](#) [445](#) [446](#) [447](#) [448](#) [449](#) [450](#) [451](#) [452](#) [453](#) [454](#) [455](#) [456](#) [457](#) [458](#) [459](#) [460](#) [461](#) [462](#) [463](#) [464](#) [465](#) [466](#) [467](#) [468](#) [469](#) [470](#) [471](#) [472](#) [473](#) [474](#) [475](#) [476](#) [477](#) [478](#) [479](#) [480](#) [481](#) [482](#) [483](#) [484](#) [485](#) [486](#) [487](#) [488](#) [489](#) [490](#) [491](#) [492](#) [493](#) [494](#) [495](#) [496](#) [497](#) [498](#) [499](#) [500](#) [501](#) [502](#) [503](#) [504](#) [505](#) [506](#) [507](#) [508](#) [509](#) [510](#) [511](#) [512](#) [513](#) [514](#) [515](#) [516](#) [517](#) [518](#) [519](#) [520](#) [521](#) [522](#) [523](#) [524](#) [525](#) [526](#) [527](#) [528](#) [529](#) [530](#) [531](#) [532](#) [533](#) [534](#) [535](#) [536](#) [537](#) [538](#) [539](#) [540](#) [541](#) [542](#) [543](#) [544](#) [545](#) [546](#) [547](#) [548](#) [549](#) [550](#) [551](#) [552](#) [553](#) [554](#) [555](#) [556](#) [557](#) [558](#) [559](#) [560](#) [561](#) [562](#) [563](#) [564](#) [565](#) [566](#) [567](#) [568](#) [569](#) [570](#) [571](#) [572](#) [573](#) [574](#) [575](#) [576](#) [577](#) [578](#) [579](#) [580](#) [581](#) [582](#) [583](#) [584](#) [585](#) [586](#) [587](#) [588](#) [589](#) [590](#) [591](#) [592](#) [593](#) [594](#) [595](#) [596](#) [597](#) [598](#) [599](#) [600](#) [601](#) [602](#) [603](#) [604](#) [605](#) [606](#) [607](#) [608](#) [609](#) [610](#) [611](#) [612](#) [613](#) [614](#) [615](#) [616](#) [617](#) [618](#) [619](#) [620](#) [621](#) [622](#) [623](#) [624](#) [625](#) [626](#) [627](#) [628](#) [629](#) [630](#) [631](#) [632](#) [633](#) [634](#) [635](#) [636](#) [637](#) [638](#) [639](#) [640](#) [641](#) [642](#) [643](#) [644](#) [645](#) [646](#) [647](#) [648](#) [649](#) [650](#) [651](#) [652](#) [653](#) [654](#) [655](#) [656](#) [657](#) [658](#) [659](#) [660](#) [661](#) [662](#) [663](#) [664](#) [665](#) [666](#) [667](#) [668](#) [669](#) [670](#) [671](#) [672](#) [673](#) [674](#) [675](#) [676](#) [677](#) [678](#) [679](#) [680](#) [681](#) [682](#) [683](#) [684](#) [685](#) [686](#) [687](#) [688](#) [689](#) [690](#) [691](#) [692](#) [693](#) [694](#) [695](#) [696](#) [697](#) [698](#) [699](#) [700](#) [701](#) [702](#) [703](#) [704](#) [705](#) [706](#) [707](#) [708](#) [709](#) [710](#) [711](#) [712](#) [713](#) [714](#) [715](#) [716](#) [717](#) [718](#) [719](#) [720](#) [721](#) [722](#) [723](#) [724](#) [725](#) [726](#) [727](#) [728](#) [729](#) [730](#) [731](#) [732](#) [733](#) [734](#) [735](#) [736](#) [737](#) [738](#) [739](#) [740](#) [741](#) [742](#) [743](#) [744](#) [745](#) [746](#) [747](#) [748](#) [749](#) [750](#) [751](#) [752](#) [753](#) [754](#) [755](#) [756](#) [757](#) [758](#) [759](#) [760](#) [761](#) [762](#) [763](#) [764](#) [765](#) [766](#) [767](#) [768](#) [769](#) [770](#) [771](#) [772](#) [773](#) [774](#) [775](#) [776](#) [777](#) [778](#) [779](#) [780](#) [781](#) [782](#) [783](#) [784](#) [785](#) [786](#) [787](#) [788](#) [789](#) [790](#) [791](#) [792](#) [793](#) [794](#) [795](#) [796](#) [797](#) [798](#) [799](#) [800](#) [801](#) [802](#) [803](#) [804](#) [805](#) [806](#) [807](#) [808](#) [809](#) [810](#) [811](#) [812](#) [813](#) [814](#) [815](#) [816](#) [817](#) [818](#) [819](#) [820](#) [821](#) [822](#) [823](#) [824](#) [825](#) [826](#) [827](#) [828](#) [829](#) [830](#) [831](#) [832](#) [833](#) [834](#) [835](#) [836](#) [837](#) [838](#) [839](#) [840](#) [841](#) [842](#) [843](#) [844](#) [845](#) [846](#) [847](#) [848](#) [849](#) [850](#) [851](#) [852](#) [853](#) [854](#) [855](#) [856](#) [857](#) [858](#) [859](#) [860](#) [861](#) [862](#) [863](#) [864](#) [865](#) [866](#) [867](#) [868](#) [869](#) [870](#) [871](#) [872](#) [873](#) [874](#) [875](#) [876](#) [877](#) [878](#) [879](#) [880](#) [881](#) [882](#) [883](#) [884](#) [885](#) [886](#) [887](#) [888](#) [889](#) [890](#) [891](#) [892](#) [893](#) [894](#) [895](#) [896](#) [897](#) [898](#) [899](#) [900](#) [901](#) [902](#) [903](#) [904](#) [905](#) [906](#) [907](#) [908](#) [909](#) [910](#) [911](#) [912](#) [913](#) [914](#) [915](#) [916](#) [917](#) [918](#) [919](#) [920](#) [921](#) [922](#) [923](#) [924](#) [925](#) [926](#) [927](#) [928](#) [929](#) [930](#) [931](#) [932](#) [933](#) [934](#) [935](#) [936](#) [937](#) [938](#) [939](#) [940](#) [941](#) [942](#) [943](#) [944](#) [945](#) [946](#) [947](#) [948](#) [949](#) [950](#) [951](#) [952](#) [953](#) [954](#) [955](#) [956](#) [957](#) [958](#) [959](#) [960](#) [961](#) [962](#) [963](#) [964](#) [965](#) [966](#) [967](#) [968](#) [969](#) [970](#) [971](#) [972](#) [973](#) [974](#) [975](#) [976](#) [977](#) [978](#) [979](#) [980](#) [981](#) [982](#) [983](#) [984](#) [985](#) [986](#) [987](#) [988](#) [989](#) [990](#) [991](#) [992](#) [993](#) [994](#) [995](#) [996](#) [997](#) [998](#) [999](#) [1000](#) [1001](#) [1002](#) [1003](#) [1004](#) [1005](#) [1006](#) [1007](#) [1008](#) [1009](#) [1010](#) [1011](#) [1012](#) [1013](#) [1014](#) [1015](#) [1016](#) [1017](#) [1018](#) [1019](#) [1020](#) [1021](#) [1022](#) [1023](#) [1024](#) [1025](#) [1026](#) [1027](#) [1028](#) [1029](#) [1030](#) [1031](#) [1032](#) [1033](#) [1034](#) [1035](#) [1036](#) [1037](#) [1038](#) [1039](#) [1040](#) [1041](#) [1042](#) [1043](#) [1044](#) [1045](#) [1046](#) [1047](#) [1048](#) [1049](#) [1050](#) [1051](#) [1052](#) [1053](#) [1054](#) [1055](#) [1056](#) [1057](#) [1058](#) [1059](#) [1060](#) [1061](#) [1062](#) [1063](#) [1064](#) [1065](#) [1066](#) [1067](#) [1068](#) [1069](#) [1070](#) [1071](#) [1072](#) [1073](#) [1074](#) [1075](#) [1076](#) [1077](#) [1078](#) [1079](#) [1080](#) [1081](#) [1082](#) [1083](#) [1084](#) [1085](#) [1086](#) [1087](#) [1088](#) [1089](#) [1090](#)

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2	("20120255019").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/12/10 19:43
S2	4	((("20050204011") or ("20050198153")).PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/12/11 15:46
S3	527	(detect\$3 near4 (mal\$ware or malicious)) and ((determin\$3 or identif\$6) near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:34
S4	20	(detect\$3 near4 (mal\$ware or malicious)) and ((determin\$3 or identif\$6) near4 ((operating adj2 system) or os)) and (tcp adj3 session)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:34
S5	8	(detect\$3 near4 (mal\$ware or malicious)) and (finger\$print near4 ((operating adj2 system) or os)) and (tcp adj3 session)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:40
S6	2	(tcp near4 (mal\$ware or malicious)) and (finger\$print near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:42
S7	30	(detect\$3 near4 (mal\$ware or malicious)) and (finger\$print near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:44
S8	3	(detect\$3 near4 (mal\$ware or malicious)) and (finger\$print near4 ((operating adj2 system) or os)) and (tcp near4 packet)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:44
S9	73	(detect\$3 near4 (mal\$ware or malicious)) and (tcp near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:45
S10	1	(detect\$3 near4 (mal\$ware or malicious)) and (tcp near4 ((operating adj2 system) or os) near4 (id or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:45
S11	112	(detect\$3 near4 (mal\$ware or malicious)) and (((operating adj2 system) or os) near4 (id or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:45
S12	6	(detect\$3 near4 (mal\$ware or malicious)) and (((operating adj2 system) or os) near4 (id or identifier)) and (tcp near4 packet)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:46

S13	7	(detect\$3 near4 (mal\$ware or malicious)) and ((determin\$3 or identif\$5) near4 ((operating adj2 system) or os) near4 device) and (tcp near4 packet)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:48
S14	1	(infect\$3 near4 (mal\$ware or malicious)) and ((determin\$3 or identif\$5) near4 ((operating adj2 system) or os) near4 device) and (tcp near4 packet)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:51
S15	9	(infect\$3 near4 (mal\$ware or malicious)) and ((determin\$3 or identif\$5) near4 ((operating adj2 system) or os)) and (tcp near4 packet)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:51
S16	17	(detect\$3 near4 (mal\$ware or malicious)) and (infect\$3 near4 ((operating adj2 system) or os)) and (tcp near4 packet)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 16:55
S17	6	((id or identifier) near4 (mal\$ware or malicious)) and ((id or identifier) near4 ((operating adj2 system) or os)) and (tcp near4 packet)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:27
S18	3	((id or identifier) near4 (mal\$ware or malicious)) and ((id or identifier) near4 ((operating adj2 system) or os)) and (tcp near4 header)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:30
S19	2	((id or identifier) near4 (mal\$ware or malicious)) and ((id or identifier) near4 ((operating adj2 system) or os)) and (tcp near4 session)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:30
S20	22	((id or identifier) near4 (mal\$ware or malicious)) and ((id or identifier) near4 ((operating adj2 system) or os)) and (tcp)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:30
S21	1	((determin\$3 or identif\$6) near4 tcp near4 (mal\$ware or malicious)) and ((id or identifier) near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:34
S22	4	((determin\$3 or identif\$6) near4 tcp near4 (mal\$ware or malicious)) and finger\$print\$3	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:34
S23	1	((determin\$3 or identif\$6) near4 tcp near4 (mal\$ware or malicious)) and ((monitor\$3) near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:38
S24	1	((determin\$3 or identif\$6) near4 tcp near4 (mal\$ware or malicious)) and (device near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:38
S25	20	((session or header or packet) near4 tcp near4 (mal\$ware or malicious)) and (device near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:40
S26	1	((session or header or packet) near4 tcp near4 (mal\$ware or malicious)) and (finger\$print near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:40
S27	2	((session or header or packet) near4	US-PGPUB;	OR	ON	2012/12/11

		tcp near4 (mal\$ware or malicious)) and ((id or identifier) near4 ((operating adj2 system) or os))	USPAT; EPO; JPO; DERWENT			17:40
S28	3	((session or header or packet) near4 tcp near4 (mal\$ware or malicious)) and ((determin\$3 or identif\$5) near4 ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:40
S29	22	((session or header or packet) near4 tcp near4 (mal\$ware or malicious)) and (finger\$print and ((operating adj2 system) or os))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/11 17:42
S30	4263	((determin\$3 or identif\$6) near4 (os or (operating adj2 system)) near4 (id or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:31
S31	80	((determin\$3 or identif\$6) near4 (os or (operating adj2 system)) near4 (id or identifier)) and (tcp adj2 packet)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:31
S32	6	((determin\$3 or identif\$6) near4 (os or (operating adj2 system)) near4 (id or identifier)) and (tcp adj2 packet) and mal\$ware	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:32
S33	6	((determin\$3 or identif\$6) near4 (os or (operating adj2 system)) near4 (finger\$print or id or identifier)) and (tcp adj2 packet) and mal\$ware	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:34
S34	6	((os or (operating adj2 system)) near4 (finger\$print or id or identifier)) and (tcp adj2 packet) and mal\$ware	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:35
S35	94	((determin\$3 or identif\$6) near4 (os or (operating adj2 system)) near4 (finger\$print))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:36
S36	4	((determin\$3 or identif\$6) near4 (os or (operating adj2 system)) near4 (finger\$print)) and mal\$ware	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:36
S37	18	((determin\$3 or identif\$6) near4 (os or (operating adj2 system)) near4 (finger\$print)) and virus	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:37
S38	16	((determin\$3 or identif\$6) near4 (os or (operating adj2 system)) near4 (finger\$print)) and virus and tcp	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2012/12/26 17:37
S39	2	("20050246450").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/12/27 13:53
S40	2	("5897595").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/12/27 18:28
S41	2	("5987595").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/12/27 18:28

S42	2	("20120246453").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/12/27 18:34
S43	3	(malware near4 signature) and (tcp near4 finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:03
S44	3	(malware same compar\$5 same signature) and (tcp near4 finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:05
S45	6	(malware near4 signature) and (os near4 finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:05
S46	6	(virus near4 signature) and (os near4 finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:11
S47	0	(virus near4 signature) and (tcp near4 finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:13
S48	4	(virus or malware) and (compar\$6 near4 signature) and (tcp near4 finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:14
S49	20	(virus or malware) and (compar\$6 near4 signature) and (tcp same finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:14
S50	3	(virus or malware) and (compar\$6 near4 signature) and (tcp same syn same finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:19
S51	1	((virus or malware) near4 signature) and (tcp same syn same finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:19
S52	4	((virus or malware) near4 detect\$3) and (tcp same syn same finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:20
S53	13	(intrusion near4 detect\$3) and (tcp same syn same finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 20:21
S54	4	(intrusion near4 detect\$3) and (determin\$3 near4 os near4 (id or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 21:20
S55	4	((virus or malware) near4 detect\$3) and (determin\$3 near4 os near4 (id or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 21:22
S56	4	((virus or malware) near4 detect\$3) and (determin\$3 near4 operating near4 (id or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/24 21:23
S57	1	(subscrib\$3 near4 (id or identifier)) and (malware near4 (id or identifier)) and (os near4 (id or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 01:43
S58	1	(subscrib\$3 near4 (id or identifier)) and (malware near4 signature) and (os near4 (id or identifier))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 01:43
S59	1	(subscrib\$3 near4 (id or identifier)) and (malware near4 signature) and (os near4 fingerprint)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 01:44

S60	1	(subscrib\$3 near4 (id or identifier)) and (malware near4 (id or identifier)) and (os near4 fingerprint)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 01:44
S61	2	("20120255019").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/25 02:40
S62	7	(virus near4 signature) and (remediat\$3 near4 portal)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 13:49
S63	10	((malware or virus) near4 signature) and (remediat\$3 near4 portal)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 13:50
S64	3	(malware or virus) same (remediat\$3 near4 portal)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 13:51
S65	6	((malware or virus) near4 signature near4 down\$load\$3) and (portal)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 13:52
S66	2	((malware or virus) near4 signature) and (portal) and (subscrib\$3 near4 down\$load\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 13:54
S67	64	((malware or virus) near4 signature) and (portal) and (subscrib\$3 and down\$load\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 13:54
S68	9	((malware or virus) near4 signature) and (portal) and (subscrib\$3 and down\$load\$3) and remediat\$3	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 13:54
S69	2	("20120255019").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/25 14:07
S70	3	(malicious near4 signature) and (tcp near4 finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 14:09
S71	25	(malicious) and (compar\$6 near4 signature) and (tcp same finger\$print\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 14:10
S72	4	((identif\$6 or determin\$3) near4 os near4 fingerprint\$3) and (detect\$3 near4 (virus or malicious or malware))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 14:11
S73	11	((identif\$6 or determin\$3) near4 operating near4 fingerprint\$3) and (detect\$3 near4 (virus or malicious or malware))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	ON	2013/01/25 14:13
S74	16	((determin\$3 or identif\$6) near4 operating adj2 system) and (alert\$3 near4 subscrib\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:10
S75	43	((determin\$3 or identif\$6) near4 operating adj2 system) and (notif\$6 near4 subscrib\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:16
S76	1	((determin\$3 or identif\$6) near4 operating adj2 system) and (notif\$6 near4 subscrib\$3) and (different	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:17

		near4 machine)				
S77	2	((determin\$3 or identif\$6) near4 operating adj2 system) and (notif\$6 near4 subscrib\$3) and malware	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:18
S78	1	(detect\$3 near4 operating adj2 system) and (notif\$6 near4 subscrib\$3) and malware	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:19
S79	31	(detect\$3 near4 operating adj2 system) and (notif\$6 near4 subscrib\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:19
S80	0	(detect\$3 near4 operating adj2 system) and (notif\$6 near4 wrong)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:21
S81	5	((determin\$3 or identif\$6 or detect\$3) near4 operating adj2 system) and (notif\$6 near4 wrong)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:22
S82	0	((determin\$3 or identif\$6 or detect\$3) near4 operating adj2 system same (alert\$3 or notif\$6) near4 wrong)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:23
S83	627	((determin\$3 or identif\$6 or detect\$3) near4 operating adj2 system same (alert\$3 or notif\$6))	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:23
S84	5	((determin\$3 or identif\$6 or detect\$3) near4 operating adj2 system same (alert\$3 or notif\$6) same in\$correct\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:24
S85	1	(operating adj2 system near5 (alert\$3 or notif\$6) near5 in\$correct\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:27
S86	5	(operating adj2 system near5 (alert\$3 or notif\$6) near5 improper)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:28
S87	23	(operating adj2 system near5 (alert\$3 or notif\$6) near5 violat\$3)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:29
S88	0	(operating adj2 system near5 (alert\$3 or notif\$6) near5 violat\$3) and (multiple near4 devices)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:39
S89	11	(operating adj2 system near5 violat\$3) and (multiple near4 devices)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:39
S90	2	("20120255019").PN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/01/27 13:40
S91	3	(remediat\$3 near4 portal same malware)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:42
S92	208	(remediat\$3 same malware)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:42
S93	35	(remediat\$3 same malware same operating adj2 system)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:42
S94	0	(qualif\$6 near4 operating adj2	US-PGPUB;	OR	OFF	2013/01/27

		system same remediat\$3)	USPAT; EPO; JPO; DERWENT			13:51
S95	69	(qualif\$6 near4 operating adj2 system)	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:52
S96	3	(qualif\$6 near4 operating adj2 system) and malware	US-PGPUB; USPAT; EPO; JPO; DERWENT	OR	OFF	2013/01/27 13:52
S97	1	(os adj2 (id or identifier)) and (signature adj2 (id or identifier)) and (mal\$ware adj2 (id or identifier))	US-PGPUB; USPAT	OR	ON	2013/08/31 15:01
S98	0	(os adj2 (id or identifier)) and (signature adj2 (id or identifier)) and (attack adj2 (id or identifier))	US-PGPUB; USPAT	OR	ON	2013/08/31 15:01
S99	18	(os adj2 (id or identifier)) and (signature adj2 (id or identifier))	US-PGPUB; USPAT	OR	ON	2013/08/31 15:01
S100	1	(os adj2 (id or identifier)) and (signature adj2 (id or identifier)) and alert\$3	US-PGPUB; USPAT	OR	ON	2013/08/31 15:02
S101	16	(os adj2 (id or identifier)) and (signature adj2 (id or identifier)) and compar\$5	US-PGPUB; USPAT	OR	ON	2013/08/31 15:02
S102	20	(os adj2 (id or identifier)) and mal\$ware	US-PGPUB; USPAT	OR	ON	2013/08/31 15:03
S103	63	((operating adj2 system) or os) adj2 (id or identifier)) and mal\$ware	US-PGPUB; USPAT	OR	ON	2013/08/31 15:08
S104	5	((operating adj2 system) or os) adj2 (id or identifier)) and (compar\$5 near4 mal\$ware)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:09
S105	5	((operating adj2 system) or os) adj2 (id or identifier)) same mal\$ware	US-PGPUB; USPAT	OR	ON	2013/08/31 15:10
S106	9	((operating adj2 system) or os) adj2 (id or identifier)) and (mal\$ware near4 signature)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:12
S107	21	((operating adj2 system) or os) adj2 (id or identifier)) and (mal\$ware near4 detect\$3)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:16
S108	11	((operating adj2 system) or os) adj2 (finger\$print)) and (mal\$ware near4 detect\$3)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:19
S109	0	("20120255019").PN.	USPAT; USOCR	OR	OFF	2013/08/31 15:24
S110	1	("20120255019").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/31 15:24
S111	44	((operating adj2 system) or os) near4 compar\$5) and (mal\$ware near4 signature)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:27
S112	8	((operating adj2 system) or os) near4 compar\$5) and (mal\$ware near4 signature) and finger\$print	US-PGPUB; USPAT	OR	ON	2013/08/31 15:27
S113	9	((operating adj2 system) or os) near4 fingerprint) and (mal\$ware near4 signature)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:34

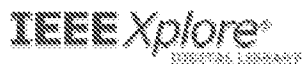
S114	2	((operating adj2 system) or os) near4 fingerprint near4 mal\$ware)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:40
S115	3	((operating adj2 system) or os) near4 (id or identifier) near4 mal\$ware)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:41
S116	2	((operating adj2 system) or os) near4 (id or identifier) near4 attack)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:42
S117	0	((operating adj2 system) or os) same tcp same mal\$ware same fingerprint)	US-PGPUB; USPAT	OR	ON	2013/08/31 15:48
S118	13	((operating adj2 system) or os) same tcp same mal\$ware)	USPAT	OR	ON	2013/08/31 15:48

EAST Search History (I nterference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S119	0	((operating adj2 system) or os) same tcp same mal\$ware same fingerprint)	USPAT; UPAD	OR	ON	2013/08/31 15:48

9/ 3/ 2013 3:31:25 PM
C:\ Users\ dnguyen18\ Documents\ EAST\ Workspaces\ 13083501.wsp

[IEEE.org](#) | [IEEE Xplore Digital Library](#) | [IEEE Standards](#) | [IEEE Spectrum](#) | [More Sites](#)



Access provided by:
United States Patent and
Trademark Office
[Sign Out](#)



SEARCH RESULTS

You searched for: **malware operating system identifier compare alert top**

1 Results returned

Exploring an open WiFi detection vulnerability as a malware attack vector on iOS devices

Spaulding, J. ; Krauss, A. ; Srinivasan, A.

Malicious and Unwanted Software (MALWARE), 2012 7th
International Conference on

Digital Object Identifier: 10.1109/MALWARE.2012.6461013

Publication Year: 2012 , Page(s) : 87 - 93

IEEE CONFERENCE PUBLICATIONS

[Sign In](#) | [Create Account](#)

IEEE Account

[Change Username/Password](#)

[Update Address](#)

Purchase Details

[Payment Options](#)

[Order History](#)

[Access Purchased Documents](#)

Profile Information

[Communications Preferences](#)

[Profession and Education](#)

[Technical Interests](#)

Need Help?

[US & Canada: +1 800 878 4333](#)

[Worldwide: +1 732 351 0000](#)

[Contact & Support](#)

[About IEEE Xplore](#) | [Contact](#) | [Help](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Site Map](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest professional association for the advancement of technology.

© Copyright 2013 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

+You Search Images Maps Play YouTube News Gmail More

Sign in

Google

malware detect operating system identifier tcp packet compare alert

Web Images Maps Shopping More Search tools

Page 2 of about 2,540,500 results (0.21 seconds)

Networking flashcards | Quizlet

quizlet.com/13087655/networking-flash-cards/

Aug 6, 2012 - What is the Ethernet frame type that is used by **TCP/IP**? ... In an IPv6 network for creating subnets when the prefix is /48 and the host ID is 64 bits? 16 ... One critical difference between a client **OS** and a server **OS** is the addition of ... What is a type of **malware** that is so difficult to **detect** and remove that most ...

Black Hat USA 2013 | Briefings

<https://www.blackhat.com/us-13/briefings.html>

Now the base **operating system** is the formerly off-the-shelf RTOS QNX, which ... is a new modulation mode and link-layer **packet** format defined in Bluetooth 4.0 ... Worse, they are often (mis)used to **compare** competing products to assess which one ... Regardless of the advances in **malware** and targeted attacks **detection** ...

Know your Enemy: Tracking Botnets - The HoneyNet Project

www.honeynet.org/book/export/html/50

Due to their immense size (tens of thousands of systems can be linked together), they ... sharing on machines running all versions of Microsoft's Windows **operating system** ... And finally, port 135/**TCP** is used by Microsoft to implement Remote ... this **malware** is harder since it includes functions to **detect** debuggers (e.g. ...

IPDEF: The User Agent Field: Analyzing and Detecting the ... - SANS Ins ...

www.sans.org/~user-agent-field-analyzing-detecting-abnormal-malicio...

shown **malware** using an HTTP client to beacon out to command and control systems. (Higgins, 2011) Sometimes a custom user agent helps in **identification**, as ... The device is possibly an iPad 1 as its running an early 3.2 **OS**, but it is ... **alert**. log tcp \$HOME_NET any <- any \$HTTP_PORTS (msg:"HTTP USER AGENT ...

SANS: Malware FAQ: Microsoft Windows UPnP vulnerabilities

www.sans.org/security-resources/malwarefaq/win_upnp.php

Implementation of UPnP functionality is provided through a set of **TCP/IP** services ... and Exposures database and assigned the **identifier** [CAN-2001-0721]. ... A self-described "Distributed Intrusion **Detection System**", the site is ... threat, **compared** to the severity of HTTP based attacks against Microsoft IIS, for example.

Information Security: Analysis of the FinFisher ... | SecurityStreet

<https://community.rapid7.com/community/infosec/blog/2012/.../finfisher>

Aug 8, 2012 - It's all over the news once again: lawful interception **malware** discovered in ... driver is sensibly bigger **compared** to the one from Bahrain), the execution flow is ... Supports most common **Operating Systems** (Windows, Mac OS X and Linux) ... **alert** tcp any any -> any any (msg:"FinFisher Malware Connection ...

Sec midterm Flashcards

www.flashcardmachine.com/Flashcards

Oct 18, 2012 - An() _____ virus adds a program to the **operating system** that is a ... to identify vulnerabilities and **alert** network administrators to these problems. ... The signal from an ID badge is **detected** as the owner moves near a _____, which ... **TCP** is responsible for addressing **packets** and sending them on the correct ...

Configuring Intrusion Prevention: Astero Security Gateway - Sophos

www.sophos.com/en-us/support/knowledgebase/115154.aspx

May 21, 2012 - Terminate Connection: A terminating data **packet** (RST for **TCP** and ICMP ... **Operating system** specific attacks: Attacks trying to exploit **operating system** related weaknesses. ... **Malware**: Software designed to infiltrate or damage a computer ... **Alert**: Unlike the Drop setting, critical data **packets** are allowed to ...

Introduction to intrusion prevention systems - IBM

<https://www.ibm.com/developerworks/library/ee-intrusion/>

Mar 19, 2013 - If a threat is **detected**, the **system** is able to take defensive actions ... in a file, and an **alert** is sent to the **system** or network administrator. ... This pattern is treated as a baseline profile and **compared** against the real-time data stream patterns. ... For example, a **TCP** **packet** with only SYN and FIN flags on is a ...

Transport Layer Security - Wikipedia, the free encyclopedia

en.wikipedia.org/wiki/Transport_Layer_Security

In the **TCP/IP** model view, TLS and SSL encrypt the data of network ... 5.2.1 Handshake protocol; 5.2.2 **Alert** protocol; 5.2.3 ChangeCipherSpec protocol; 5.2.4 ... to **detect** any changes in the data between the time it was sent and the time it is ... **OS** X 10.8 on have SecureTransport support for TLS 1.1 and 1.2/DualyS SSL ...

Ads related to malware detect operating system identifier tcp ...

Malware Removal Tool

www.enigmasoftware.com/ ▼

Remove **Malware** to Clean, Secure & Speed Up Your PC. Free Scanner!

Webroot® Malware Removal 1 (855) 654 2144

www.webroot.com/malware-removal ▼

PC Mag Best of the Year Winner! Get \$10 Off - Limited Time Special

Rated **A+** – Better Business Bureau (BBB)

Webroot has 344 followers on Google+

Internet Security Special - Business Antivirus - #1 US Retail Security

Malware Reviews

www.ask.com/Malware+Reviews ▼

Search for **Malware** Reviews Look Up Fast Results now!

Ask.com has 6,668 followers on Google+

[Previous](#)

[1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#)

[Next](#)

[Advanced search](#)

[Search Help](#)

[Send feedback](#)

[Google Home](#)

[Advertising Programs](#)

[Business Solutions](#)

[Privacy & Terms](#)

[About Google](#)

+You Search Images Maps Play YouTube News Gmail More

Sign in

Google

malware detect operating system identifier tcp packet compare alert

Web Images Maps Shopping More Search tools

About 2,540,000 results (0.45 seconds)

ISA Server Network Protection: Protecting Against Floods and Attacks

technet.microsoft.com/en-us/library/bb794735.aspx

Simplified client IP **alert** pooling and connection quotas improve resiliency ...
Enhanced flood protection and intrusion **detection** features help block flood ... In a non-TCP DoS attack, malicious hosts send numerous non-TCP **packets** to a victim server. ... To enable the **operating system** mechanism, which is useful in server ...

Overview of intrusion detection - TechNet - Microsoft

technet.microsoft.com/en-us/library/cc935155.aspx

Overview of **malware** inspection ... By default, the intrusion **Detected alert** is reset automatically after one minute, during ... The attacker sends a TCP SYN **packet** with a spoofed source IP address that matches the IP ... which causes some older **operating systems** to fail when the datagram is received. ... Event ID, Message.

Free Tools | McAfee Downloads

www.mcafee.com/Business/Home/Products/Solutions/Downloads

McAfee GetSusp is intended for users who suspect undetected **malware** on ... Mac Stinger is a standalone utility used to **detect** and remove specific viruses on Mac OS X. ... McAfee Stinger **detects** and removes prevalent Fake Alert **malware** and ... Reports all open TCP and UDP ports and maps them to the owning process ...

PDF SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy

csrc.nist.gov/publications/nistpubs/800-41/Rev1/sp800-41-rev1.pdf

by K Scarfone - 2009 - Cited by 20 - Related articles
sensitive unclassified information in Federal computer **systems**. ... Such **identification** is not intended to imply recommendation or endorsement by ... In their most basic form, firewalls with **packet** filters **operate** at the network layer. ... A typical unified threat management (UTM) **system** has a firewall, **malware detection** and.

Results for similar searches

PDF Passive Operating System Identification From TCP/IP Packet

www.itl.mit.edu/mission/communications/istv/JG3_POSI_Lippmann.pdf

by R Lippmann - Cited by 29 - Related articles
alerts from intrusion **detection** systems. ... determined using passive OS analysis of TCP/IP **packet** ... compared to a database of exemplars containing stored.

More results for

malware detect operating system identifier tcp packet compare alert

Chapter 8. Remote OS Detection - Nmap

nmap.org/book/osdetect.html

Reasons for OS **Detection** ... TCP ISN sequence predictability index (SP) - IP ID sequence generation algorithm (TI, CI, II) - Shared IP ID sequence Euclean ...

More results for

malware detect operating system identifier tcp packet compare alert

SANS: intrusion Detection FAQ: How can passive techniques be ...

www.sans.org/security-resources/ifaq/passive_vuln.php

Second, current **operating system identification** implementations using passive techniques are ... An **operating system** can be identified by comparing slight differences in the ... Notice the initial ICMP request and six **packets** with TCP flags set to SYN, ... **alert** tcp any -> \$HOME_NET any (msg:"queso scan", flags:21G, ack: 0).

More results for

malware detect operating system identifier tcp packet compare alert

Ads related to malware detect operating system identifier tcp ...

WebSense® DLP Product - Safeguard Your Data with WebSense®

www.websense.com/DLP

Free White Paper. Download Now

Malware Survival Kit

www.sourcesfire.com/incidentResponse

Find out what you need to defend against advanced **malware** attacks

Free Spyware Detection - Detect & Remove Spyware On Your PC

www.winzip.com/SpywareDetection

(Highly Recommended) Free Scan.

1 2 3 4 5 6 7 8 9 10 [Next](#)

[Advanced search](#) [Search Help](#) [Send feedback](#)

[Google Home](#) [Advertising Programs](#) [Business Solutions](#) [Privacy & Terms](#)
[About Google](#)

Search Notes

Application/Control No.

13/083,501

Examiner

DUSTIN NGUYEN

Applicant(s)/Patent under
Reexamination

MCNAMEE ET AL.

Art Unit

2446

SEARCHED

Class	Subclass	Date	Examiner
726	23, 24	9/3/2013	DN

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner
726	23, 24	9/3/2013	DN
709	224	9/3/2013	DN

**SEARCH NOTES
(INCLUDING SEARCH STRATEGY)**

	DATE	EXMR
update EAST search, IEEE, ACM and google	9/3/2013	DN
inventor search	9/3/2013	dn

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)

22511 7590 09/12/2013
OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010



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.

Patty Giebler (Depositor's name)
Patty Giebler (Signature)
12-5-13 (Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/083,501	04/08/2011	Kevin McNamee	37617/011002; 08917906US	8289

TITLE OF INVENTION: METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL UNDISCOUNTED	\$890 \$1780	\$300	\$0	\$1190 \$2080	12/12/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
NGUYEN, DUSTIN	2446	726-024000

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.

Osha Liang, L.L.P.
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)

ALCATEL LUCENT Paris, France

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 credit any overpayment, to Deposit Account Number 12-2325 (enclose an extra copy of this form).

12/11/2013 EEKUBAY2 00000041 122325 13083501

01 FC:1501 1780.00 DA
02 FC:1504 300.00 DA

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☒ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

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.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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 United States Patent and Trademark Office.

Authorized Signature

Patty Giebler

Date

12-5-13

Typed or printed name

Patty Giebler

Registration No.

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, 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.

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)

22511 7590 09/12/2013
OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010



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.

<i>Patty Giebler</i>	(Depositor's name)
<i>Patty Giebler</i>	(Signature)
<i>12-5-13</i>	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/083,501	04/08/2011	Kevin McNamee	37617/011002; 08917906US	8289

TITLE OF INVENTION: METHOD AND SYSTEM FOR OPERATING SYSTEM IDENTIFICATION IN A NETWORK BASED SECURITY MONITORING SOLUTION

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL UNDISCOUNTED	\$890 \$1780	\$300	\$0	\$1190 \$2080	12/12/2013
EXAMINER	ART UNIT	CLASS-SUBCLASS				
NGUYEN, DUSTIN	2446	726-024000				

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.

Osha Liang, L.L.P.

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)

ALCATEL LUCENT Paris, France

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 credit any overpayment, to Deposit Account Number *12-2325* (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

☐ Applicant asserting small entity status. See 37 CFR 1.27

☒ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

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.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

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 United States Patent and Trademark Office.

Authorized Signature

Patty Giebler

Date

12-5-13

Typed or printed name

Patty Giebler

Registration No.

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, 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.



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.
13/083,501	01/21/2014	8635697	37617/011002; 08917906US	8289

22511 7590 12/31/2013
OSHA LIANG L.L.P.
TWO HOUSTON CENTER
909 FANNIN, SUITE 3500
HOUSTON, TX 77010

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 209 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):

Kevin McNamee, Ottawa, CANADA;
Mike Pelley, Ottawa, CANADA;
Darren Deridder, Ottawa, CANADA;
Paul Edwards, Ottawa, CANADA;

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.