Filed on behalf of: GoSecure, Inc.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner,

v.

GOSECURE, INC.,
Patent Owner.

Case IPR2025-00070
Patent 9,954,872

DECLARATION OF JOSEPH GREENFIELD IN SUPPORT OF PATENT OWNER'S PRELIMINARY RESPONSE

GoSecure, Inc.
Exhibit 2001
CrowdStrike v. GoSecure
IPR2025-00070

Table of Contents

I. Introduction and Qualifications 2

II. Summary Of Materials Reviewed And Considered 4

III. Legal Standards 5

IV. Level of Skill in the Art 8

V. Claim Construction 9

VI. Overview of the '872 Patent 10

VII. The Claims of the '872 Patent Would Not Have Been Obvious in View of Petitioner's Prior Art 14

A. Overview of Capalik 14
B. Capalik Fails to Disclose or Render Obvious the "Transmitting" Limitation in Each Claim of the '872 Patent 18

VIII. Conclusion 26

I. Introduction and Qualifications

1. I, Joseph Greenfield, have been retained by GoSecure, Inc. ("Patent Owner") to provide my independent opinions concerning the validity of claims 1-21 of U.S. Patent No. 9,954,872 (the "'872 patent," Ex. 1001), in support of Patent Owner's Preliminary Response to the Petition for *Inter Partes* review of the '872 patent (IPR 2025-00070) filed by CrowdStrike, Inc. ("Petitioner") and accompanied by a Declaration of Dr. Markus Jakobsson (the "Jakobsson Declaration"), among other exhibits.

2. I am more than eighteen years of age, and I am a citizen of the United States, currently residing in the State of California.

3. In formulating my opinions, I have relied upon my knowledge, training, and experience in the relevant art including cybersecurity, digital forensics, and cyber incident response. My qualifications, along with a more detailed summary of my background and publications, are stated more fully in my *curriculum vitae*, which has been provided as Exhibit 2002. Here, I provide a brief summary of my qualifications.

4. I am the Vice President and Chief Forensic Examiner of Maryman & Associates Inc., a professional services firm specializing in computer forensics, cyber investigations, incident response and security consulting. I have over 18 years

of experience in conducting investigations, collecting evidence and analyzing digital evidentiary items.

5. In addition to my role at Maryman & Associates Inc., I am an Associate Professor of Information Technology Practice at the Viterbi School of Engineering at the University of Southern California (USC). I have been teaching cyber security and forensics at USC since 2006 and have developed ten courses in the fields of information security and digital forensics. During my time as a faculty member, I authored the first undergraduate cyber security program at USC, the undergraduate Minor in Applied Computer Security, in 2009. In 2012, I authored the minor in Computer & Digital Forensics. I also co-authored the interdisciplinary degree in Intelligence and Cyber Operations. In 2021, I received the Viterbi School of Engineering Dean's Award for Innovation in Teaching and Education.

6. I received my Bachelor's degree in Computer Engineering in 2005 and my Master's degree in Computer Science in 2006, both from the University of Sothern California.

7. I completed my Doctor of Philosophy (Ph.D.) in Computer Science at the University of Rhode Island in 2019, where my research focused on parallel processing of digital forensic artifacts during bitstream imaging. My thesis, entitled "SPARTA: System for Portable Acquisition with Real-Time Analysis" focused on

designing, developing, and testing a new portable system for digital forensics imaging with real-time analysis over every live file.

8. I have performed thousands of hours of computer forensic investigation including forensic data acquisition and analysis of an extensive variety of digital evidence items including electronic business records and computer files. I have been a presenter at local and national conferences on various topics in digital forensics.

9. I have testified as a digital forensics expert in California State Superior Court. I have had my deposition taken as a digital forensics expert in US Federal Court. I have testified as a digital forensics expert in a tribunal inquiry in India.

10. I have experience programming in programming and scripting languages including Python, C/C++, C#, Java, and PowerShell. My entire Ph.D. dissertation project was coded in Python without the use of Artificial Intelligence (AI) or Large Language Models (LLMs).

11. I am a listed inventor and author of patent number 20110029881, Devices and Methods For Providing Software Programs Compatible With A Computer System For Download By A User.

II. Summary Of Materials Reviewed And Considered

12. All of the opinions contained in this Declaration are based on the documents I reviewed and my knowledge and professional judgment. In forming

the opinions expressed in this Declaration, while drawing on my experience, I reviewed the following documents in addition to the Petition itself:

Ex.	Description
1001	United States Patent No. 9,954,872 ("the '872 patent")
1002	File History for United States Patent No. 9,954,872 ("'872 FH")
1003	Declaration of Dr. Markus Jakobsson
1004	U.S. Application Publication No. 2008/0016570 to Capalik ("Capalik")

13. My opinions are additionally guided by my appreciation of how a person of ordinary skill in the art ("POSITA") would have understood the claims of the '872 patent at the time of the invention, which I have been asked to assume is June 24, 2010.

III. Legal Standards

14. I am not an attorney. However, I have been informed by counsel of certain legal standards and have applied those standards, described below, to formulate my opinions.

15. I understand that the claims of a patent define the limits of a patentee's exclusive rights. I understand that to determine the scope of the claimed invention, courts may construe claim terms, the meaning of which the parties may dispute. I understand that claim terms should generally be given their ordinary and customary meaning as understood by a POSITA in the context of the entire patent at the time of filing of the patent application.

16. I understand that claims must be construed in light of and consistent with the intrinsic evidence. In this context, I understand that intrinsic evidence includes the claims themselves, the written disclosure in the specification, and the patent's prosecution history. I understand that the specification is always highly relevant to the claim construction analysis and often is the single best guide to the meaning of a disputed term. I understand that extrinsic evidence may also be considered when construing claims and may include, for example, technical dictionaries, technical publications and books, treatises, and expert testimony, though the intrinsic record will be more persuasive as to the meaning of a particular term.

17. I understand that one or more prior art references can render a patent claim obvious to a person of ordinary skill in the art if the differences between the subject matter set forth in the patent claim and the prior art are such that the subject matter of the claim would have been obvious at the time the claimed invention was made. In analyzing obviousness, I understand that it is important to consider the scope of the claims, the level of skill of a person of ordinary skill in the relevant art, the scope and content of the prior art, the differences between the prior art and the claims, and "secondary considerations" of non-obviousness, which I also understand can include, for example, evidence of commercial success of the invention, evidence

of a long-felt need that was solved by an invention, evidence that others copied an invention, or evidence that an invention achieved an unexpected result.

18. I understand that the claimed subject matter can be obvious when a person of ordinary skill in the art would have been motivated to combine pre-existing elements, and that combination yields no more than what a person of ordinary skill in the art would have expected. I also understand that, in assessing whether a claim is obvious, one must consider whether the claimed improvement is more than the predictable use of prior art elements according to their established functions. I understand that there need not be a precise teaching in the prior art directed to the specific subject matter of a claim because one can take account of the inferences and creative steps that a person of ordinary skill in the art would employ. However, I further understand that obviousness cannot be based on the hindsight combination of components selectively culled from the prior art.

19. I understand that for a reference to qualify as a relevant prior art reference in an obvious analysis, the reference must be "analogous"—meaning it is from the same field of endeavor as the patented technology, and if not, then the reference must be reasonable pertinent to the particular problem facing the inventors of the patent at issue. I also understand that a reference is reasonably pertinent if a person of ordinary skill in the art would have reasonably consulted those references and applied their teachings in seeking a solution to the problem facing the inventors.

IV. Level of Skill in the Art

20. I understand that certain issues relating to validity must be judged from the perspective of a POSITA. I further understand that factors that may be considered in determining the level of skill of a person of ordinary skill in the art include, but are not limited to, (1) the type of problems encountered in the art; (2) prior art solutions to those problems; (3) rapidity with which innovations are made; (4) sophistication of the technology; and (5) the educational level of active workers in the field.

21. I have been informed and understand that a POSITA is a hypothetical person who is presumed to be aware of all pertinent prior art, thinks along conventional wisdom in the art, and is a person of ordinary creativity. I understand that this hypothetical person is of ordinary skill in the art to which the claimed subject matter pertains.

22. In his declaration, Dr. Jakobsson contends that a POSITA in the field of the '872 patent as of June 24, 2010 would have been knowledgeable regarding the field of software security analysis and dynamic malware analysis. Dr. Jakobsson further notes that most workers of ordinary skill in the art as of June 24, 2010, would have had a bachelor's degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and would have had a working knowledge of software security analysis and dynamic malware analysis.

Dr. Jakobsson further notes that a person with less relevant practical experience but with additional education could also have qualified as a POSITA in the field of the '872 patent. Ex. 1003 ¶ 41.

23. For the purposes of this Declaration, I agree with and have adopted Dr. Jakobsson's definition of a POSITA. Based on Dr. Jakobsson's definition, I qualified as a POSITA as of June 24, 2010. As of June 24, 2010, I held a Bachelor's Degree in Computer Engineering and a Master's Degree in Computer Science. I had been working as a consultant in the field of cybersecurity and digital forensics with four years of industry experience, along with my four years of teaching experience at USC. I have applied Dr. Jakobsson's perspective of a person of ordinary skill in the art, as of June 24, 2010, in forming and expressing my opinions. Unless otherwise stated, my testimony below refers to the knowledge of one of ordinary skill in the art at that relevant time.

V. Claim Construction

24. In my analysis, I have applied the plain and ordinary meanings of the claim terms in the '872 patent, as a person of ordinary skill in the art would have understood them in the context of that patent in approximately June 2010. And it is my opinion that the prior art set forth in the Petition fails to disclose or render obvious the subject matter of the challenged claims under any reasonable construction and interpretation of the '872 patent's claims.

VI. Overview of the '872 Patent

25. The '872 patent is entitled "System and method for identifying unauthorized activities on a computer system using a data structure model," and it is directed to "systems and methods for analyzing malicious activities on a computer system in order to better protect the computer system from future malicious activity." '872 patent at 1:44-48.

26. The specification of the '872 patent explains that "networked computers are … vulnerable to attacks, unwanted intrusions, and unauthorized access" by malicious computer programs such as malware. '872 patent at 1:53-57. The specification highlights that prior anti-malware and network security systems—such as firewalls—suffered significant drawbacks because they focused on stopping known threats by matching "low-level IP data packets" against a preexisting database of "malware fingerprints." '872 patent at 1:58-2:8. Relying on a library of "malware fingerprints" in connection with "low-level IP data packets" left conventional techniques for preventing attacks using intrusion detection systems ("IDS") and intrusion prevention systems ("IPS") vulnerable to previously unknown threats: "A critical threat to computer networks is the so-called zero-day attack that exploits security vulnerabilities previously unknown …." '872 patent at 2:9-11. Likewise, because conventional IDS/IPS solutions relied on "match[ing]" fingerprints, they were vulnerable to slight modifications in the packaging of

malicious code, which could suffice to avoid signature-based detection while still exploiting the same or similar security vulnerabilities. '872 patent at 2:5-8. According to the '872 patent, there was "a great need for efficient methods of identifying fingerprint data for previously unknown types of malicious and/or unauthorized activities." '872 patent at 2:20-23. However, as the patent acknowledges, "identifying the fingerprints of malicious activities in the middle of numerous other non-malicious processes is not a trivial task." '872 patent at 2:17-19.

27. The '872 patent solves these technological problems with specific techniques to prevent unauthorized activities by "monitoring and identifying associations between activity sources and activity targets without using pre-determined fingerprints" and propagating information to other computing devices that were to be protected in the network. '872 patent at 3:11-16.

28. For example, the '872 patent describes monitoring activity directly on a computer system (e.g., an endpoint device such as a laptop, desktop, or server) using a module that is integrated with the operating system. '872 patent at 4:15-21, 6:35-43. The focus of malware detection in this way is shifted away from relying on libraries of fixed signatures that reside at the gateway to a network (i.e., "low-level IP data packets") to instead monitoring activity directly on endpoint devices. That is, rather than relying on conventional techniques in which an "IDS or IPS

examines the low-level IP data packets and compares them to its library of fingerprints for a match" whenever "a connection is attempted to a network port" ('872 patent at 2:2-5), the '872 patent provides techniques for identifying and responding to malware that infiltrated a host computing device undetected by the IDS/IPS. *See* '872 patent at 2:37-46 ("The fingerprint is transmitted to one or more other computer systems on the network to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint.").

29. Similarly, the patent describes identifying activities based on "an activity source, an activity target, and an association between the activity source and the activity target." '872 patent at 15:25-33. By focusing on significant events and chains of activities (as defined by associations between activity sources and activity targets), the invention takes a dynamic, behavior-based approach to addressing threats, as opposed to the conventional approach of comparing inbound network data packets to fixed signatures. '872 patent at 1:58-2:31, 19:24-30. For example, the '872 patent recognized the need to distinguish between read-only operations and operations that modified a target file, recognizing that the latter posed a greater threat for purposes of propagating malware through a system. '872 patent at 17:42-50. And in order to process and utilize the vast amounts of data generated by monitoring such activity directly on the computer system, the '872 patent discusses the use of

"time or sequence-based filters" in conjunction with the behavior-based approach described above. '872 patent at 16:5-7.

30. The patent also discusses storing the monitored activities in a specific data structure that identifies the activity sources, the activity targets, and the associations. For example, Figure 5A provides an example of such a data structure in which "unauthorized activity entries are grouped into one or more sets (e.g., 504) based on time (e.g., time when the entries are recorded or time window of recorded activity), association types (e.g., malicious associations v. benign associations), source types, target types, and other characteristics of the unauthorized activities." '872 patent at 12:50-55. Each set in FIG. 5A includes a "status 506," a "frequency 508," a "global time stamp 510," and "one or more unauthorized activity entries 505." '872 patent at 12:56-13:64.

31. Lastly, and most importantly, the patent describes sharing the newly-created security information with other computer systems "to prevent future attacks on the computer system or other computer systems, by blocking activity sources that match a pattern of unauthorized activities." '872 patent at 14:43-50. The patent explains, for example, that the "decoy network device transmits (644) the fingerprint to one or more protected network devices (136) to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint." '872 patent at 18:44-47.

VII. The Claims of the '872 Patent Would Not Have Been Obvious in View of Petitioner's Prior Art

32. In its Petition and the supporting Jakobsson Declaration, Petitioner argues that the claims of the '872 patent would be obvious over various combinations of references, each relying on Capalik (Ex. 1004). Pet. 9. I disagree. Petitioner and Dr. Jakobsson fundamentally misunderstand Capalik's disclosure in arguing that Capalik discloses the final limitation of each independent claim in the '872 patent, which states: "transmitting to one or more computer systems other than the first computer system information … for preventing attacks to the one or more computer systems."[1]

A. Overview of Capalik

33. Capalik, entitled "System and method for analyzing unauthorized intrusion into a computer network," is directed to "methods and systems that adequately protect networks from new and undefined attacks and that allow for real-time updates to a network's library of attack signatures." Capalik at Cover, [0007].

34. Capalik's invention "comprises a modular decoy network appliance" that includes: 1) "front-end fully functional operating system modules" and 2) "a separate processing back-end module." Capalik [0008]. Capalik's "front-end

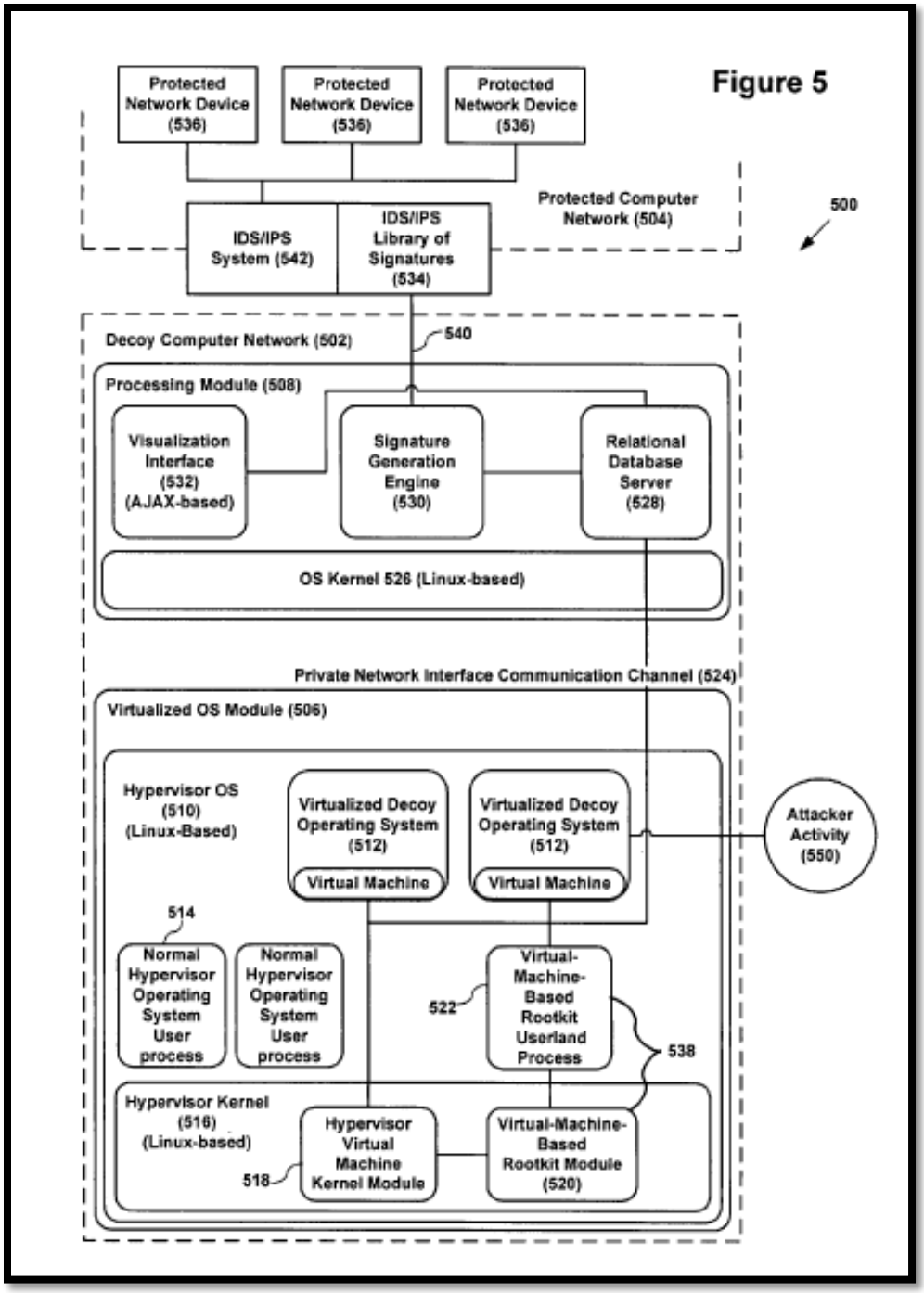
[1] I reserve the right to express additional opinions regarding why the claims of the '872 patent are not obvious in the event this proceeding is instituted, but for purposes of this Declaration, have limited my analysis to this issue.

presents a standard fully functional operating system … that returns a standard operating system fingerprint when it is scanned by tools that attackers typically use to identify vulnerable systems" such that an "attacker is thus lured into accessing the identified operating system and running custom or known exploits on that system." Capalik [0009]. More specifically, "[w]hen an attacker connects to a port, and begins interacting with decoy operating system 32, sentinel 34 monitors and captures information from the connection including port numbers, data streams, keystrokes, file uploads and any other data transfers." Capalik [0027].

35. "The captured information, or attack-identifying information, is then sent for processing to processing module 40." Capalik [0028]. "The processing module is used to generate an attack signature by analyzing all the data passed through the socket," which includes "analyzing the attack payload including the keystrokes or transferred bytes and any files uploaded to the client operating system of an ASCII or binary nature." Capalik [0013].

36. Lastly, "the signature may be sent from the back end processing module 40 to IDS/IPS 62 through a second connection which is used by the processing module 40 to directly interact with IDS/IPS 62." Capalik [0028]. By "applying the generated signature to the IDS/IPS library of signatures to update the information contained in the library of signatures," Capalik thereby seeks "to prevent the attacker from accessing the primary network with a zero-day attack." Capalik [0033].

37. Capalik's system is further explained with reference to Figure 5 (copied below for ease of reference), which includes "a decoy computer network 502" and a "protected computer network 504." Capalik [0038]. Capalik's "protected computer network 504 includes an IDS/IPS library of signatures 534 and an IDS/IPS system 542 coupled to multiple protected network devices 536." Capalik [0053].



38. When an attacker "connects to a virtualized decoy operating system 512 through an open port, the attacker sees a fully-functional standard operating system fingerprint," such that "[t]he instigator of the attack 550 is [] lured into accessing the

decoy 512." Capalik [0045]. By interacting with decoy 512, "the attacker provides decoy 512 with the data used to obtain control of the decoy 512." Capalik The "captured information … is then sent from introspection module 538," which resides within virtualized operating system module 506, to the other component of decoy computer 512: processing module 508. Capalik [0048]. Within processing module 508, "signature generation engine 530 then uses this forensic data to generate a signature of the attack." Capalik [0052]. Once generated, the signature is sent "from the back-end processing module 508 to the intrusion detection and/or prevention (IDS/IPS) signature library 534." Capalik [0054]. "The generated attack signature is thus applied to the IDS/IPS library of signatures 534, thereby updating the information contained in the signature library and preventing the attacker from accessing the protected network 504." Capalik [0059].

B. Capalik Fails to Disclose or Render Obvious the "Transmitting" Limitation in Each Claim of the '872 Patent

39. Each independent claim in the '872 patent requires "transmitting to one or more computer systems other than the first computer system information … for preventing attacks, to ***the*** one or more computer systems." I understand that the emphasized "the" above indicates that the "one or more computer systems" that are protected from attacks are the same as the "one or more computer systems" that receive the information. That is, each claim requires transmitting information to a computer to protect that specific computer from an attack.

40. Capalik does not disclose this limitation. As Petitioner recognizes (Pet. 33-34), Capalik is focused on sending signatures to an IDS/IPS so that the IDS/IPS can prevent attacks on other computers within a network, not attacks on the IDS/IPS itself. Capalik [0059]. That is a fundamental difference between Capalik and the claims of the '872 patent that Petitioner and Dr. Jakobsson do not address.

41. In its analysis of this limitation, Petitioner argues that the ***specification*** of the '872 patent provides an example in which "the decoy network device transmits the fingerprint to the IDS/IPS system 142 …" Pet. 33 (quoting '872 patent at 18:47-51). But that is not what the ***claims*** say, and I understand that the claims define the scope of the invention. That is, I understand that the proper comparison is between the prior art and the claims, not the prior art and the specification. As discussed above, every independent claim requires "transmitting to one or more computer systems other than the first computer system information … for preventing attacks, to the one or more computer systems." A POSITA would have understood this claim language to be describing transmitting information to one or more user devices (e.g., "endpoint" devices) that are the subject of future attacks, not transmitting information to an "IDS/IPS" so that the IDS/IPS can use it to protect a network of devices. The specification of the '872 patent specifically distinguishes between these two use cases. '872 patent at 18:45-51:

> The decoy network transmits (644) the fingerprint to one or more protected network devices 136 to prevent future

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

42. Specifically, and as discussed above, Capalik employs a "honeypot" to attract attacks. Capalik [0025]. By showing an attacker an intentional vulnerability in the network (e.g., a decoy operating system accessible through an open port), Capalik discusses luring the attacker into accessing the decoy. Capalik [0045]. Then, Capalik teaches generating "an attack signature by analyzing all data" passed through the open port, or "socket." Capalik [0013]. Once generated, the signature is sent to an IDS/IPS, which uses it to "prevent[] the attacker from accessing the protected network." Capalik [0059].

43. Transmitting a signature to an IDS/IPS is different from transmitting information to a device that is sought to be protected, as claimed in the '872 patent. That is, a POSITA would have understood that Capalik's IDS/IPS is a separate physical network device and not in the category of protected network devices, such as workstations and servers. This is consistent with Capalik itself. For example, Capalik specifically illustrates and discusses the IDS/IPS (542) as being a separate component from the protected network devices (536). *See, e.g.,* Capalik at Figure 5, [0053]-[0054]. Consistent with this separation, Capalik also lists several

"[s]uitable IDS/IPS systems" that can be used in implementing its disclosure, including "Cisco Systems' IPS 4200 Series, Juniper's IDP 200, and Enterasys' Dragon IDS Network Sensor." Capalik [0053]. Each of these systems is a standalone hardware device that is intended to protect other computer systems. For example, the Cisco IPS 4200 Series is described as a device to "stop malicious attacks, worms, and application abuse before they affect your data and resources" and includes its own separate hardware. Ex. 2003. As shown in the drawing on the Cisco IPS 4200 Series page, the IPS sensors are separate from, for example, the protected network devices of the Public Services Segment.

44. Continuing the example above, the Cisco IPS 4200 Series operates on the Cisco Internetwork Operating System (IOS). Ex. 2009. This operating system is not one of those listed as a virtual operating system that would be exposed in Capalik. To the contrary, Capalik describes exposing a virtual operating system that is typically used by users, such as Windows, or servers, such as Linux or Solaris (Capalik [0009]), and sending attack signatures to a dedicated network device, which typically operates a dedicated network device operating system, such as the Cisco Integrated Operating System (IOS) (Capalik [0053]). This is fundamentally different from the claims of the '872 patent which requires providing attack signatures to other endpoints, which would only make sense if the endpoints were running the same (or similar) operating system configurations.

45. Dr. Jakobsson concedes that an IDS/IPS is different from a protected network device, and seems to concede that Capalik's transmission of information to the IDS/IPS, by itself, does not meet the claims' requirement of transmitting information to devices for preventing attacks on those devices. This is why he must argue that a POSITA "would have understood that signatures updated in the signature library are ***also*** transmitted to the multiple protected network devices 536 coupled to the IDS/IPS system." Ex. 1003 ¶ 143 (emphasis added). But this additional transmission is not disclosed or suggested by Capalik, which does not discuss the protected network devices 536 receiving signatures. Thus, while he correctly acknowledges that the IDS/IPS is distinct from the network devices themselves, Dr. Jakobsson provides no support for his opinion that a POSITA would have understood that the signatures generated in Capalik are "also transmitted to the multiple protected network devices." Ex. 1003 ¶ 143. That lack of support is unsurprising because Dr. Jakobsson's opinion is inconsistent with how typical enterprise computer network security systems operated in 2010 coupled with a POSITA's understanding of the relevant technology at the time of the '872 patent.

46. As discussed above, Capalik is focused on identifying attacks on a network. Capalik does so by directing attacks away from a protected network to a honeypot. Capalik [0025]. One common example of a network attack is a denial of service ("DOS") attack, where an attacker floods a target network with traffic (e.g.,

authentication requests with invalid return addresses), effectively overwhelming the network's capacity and preventing it from performing its intended operation. In order to identify and respond to such an attack, Capalik teaches implementing a network-based IDS/IPS to detect malicious packets in network traffic and block potential attacks. Capalik [0013] ("The processing module is used to generate an attack signature by analyzing all the data passed through the socket."). Likewise, Petitioner's own documents provide an example of a network-centric protection system using Snort, which is described as an open-source network IDS/IPS that monitors network traffic and compares it against configurable rules (e.g., analogous to Capalik's "signatures"). Ex. 2004.

47. Petitioner's document makes no mention of sending these configurable rules to the endpoint devices (which are analogous to Capalik's protected network devices 536) themselves, nor would doing so make sense. As one issue, the data used to configure Snort or one of the example IDS/IPS devices provided by Capalik (e.g., the Cisco device detailed above) would be unusable by a typical endpoint device that does not have IDS/IPS functionality. It would not be expected for an endpoint device to have such functionality, as the entire point of a hardware IDS/IPS is to separate that functionality into a device dedicated to protecting the network and eliminate the need for the endpoint devices to do protection. And, continuing with the DOS example above, the entire point of the attack is to overwhelm endpoint

devices (e.g., servers) by flooding a network with traffic. The IDS system would block this network traffic from being sent to the endpoints, so there would be no reason to send the same rules to the endpoints, overburdening them with rules that would never have to be checked. Even assuming that the endpoint devices could implement the configurable rules (which Dr. Jakobsson does not establish about Capalik's protected network devices 536), requiring the endpoint device to apply the configurable rules to detect the attack would serve no purpose. Thus, Dr. Jakobsson's opinion that in Capalik signatures are "also transmitted to the multiple protected network devices" is not only conclusory, but also inconsistent with Capalik and the knowledge of a POSITA.

48. In sum, not only would a POSITA in June 2010 not have seen any benefit to sending Capalik's signature to the actual devices to be protected (given that the entire purpose of a separate IDS/IPS is to monitor network traffic without burdening endpoint devices), doing so would have imposed a significant burden on the endpoint devices themselves by requiring them to perform redundant security-related tasks on network traffic that would never reach the systems in the first place. Also, transmitting Capalik's signature to the actual devices to be protected would have caused a burden on the network itself by occupying a portion of the network's finite bandwidth. A POSITA would have wanted to avoid such additional burdens,

given that a concern at the time was the high resource utilization of non-business essential software, including security software.

49. Additionally, Dr. Jakobsson's unsupported opinion fails to consider the security implications associated with sharing the attack information with potentially vulnerable endpoint devices. Indeed, Capalik specifically discusses only sharing the signature information via a "private and secure [virtual local area network (VLAN)]" so that the attacker cannot know that it is being monitored. Capalik [0011]. Creating a singular VLAN to connect the IDS/IPS to all endpoints, as suggested by Dr. Jakobsson, for the purpose of distributing attack signatures, would create an insecure flat network without proper system segregation. In short, a POSITA would not have read Capalik to disclose sending the signatures to endpoint devices; to the contrary, a POSITA would have considered doing so to be antithetical to Capalik's focus on stealthily capturing and sharing signatures in a way that does not alert the attacker that it is being monitored.

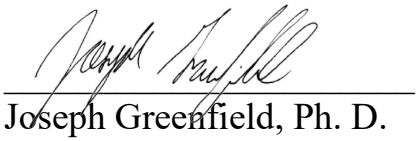
50. Accordingly, for the reasons above, Capalik does not disclose, teach, or suggest "transmitting to one or more computer systems other than the first computer system information … for preventing attacks to ***the*** one or more computer systems," as recited in the independent claims of the '872 patent.

VIII. Conclusion

51. For the foregoing reasons, it is my opinion that claims 1-21 of the '872 patent would not have been obvious over the prior art in Petitioner's Petition for *inter partes* review.

All statements made herein of my own knowledge are true, and all statements made on information and belief are believed to be true. Further, I am aware that these statements are 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. I declare under the penalty of perjury that the foregoing is true and correct.

Executed on February 2, 2025 in Los Angeles, California.



Joseph Greenfield, Ph. D.