UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner,

v.

GOSECURE, INC.,
Patent Owner.

IPR2025-00068
Patent 9,954,872 B2

Before NEIL T. POWELL, STACEY G. WHITE, and
GARTH D. BAER, *Administrative Patent Judges.*

POWELL, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background

CrowdStrike, Inc. ("Petitioner") filed a Petition for *inter partes* review of claims 1–21 of U.S. Patent No. 9,954,872 B2 (Ex. 1001, "the '872 patent"). Paper 1 ("Pet."). GoSecure, Inc. ("Patent Owner") filed a Preliminary Response. Paper 7 ("Prelim. Resp."). We authorized Petitioner to file a Preliminary Reply and Patent Owner to file a Preliminary Sur-Reply. Paper 9 ("Prelim. Reply"); Paper 10 ("Prelim. Sur-Reply").

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2024). To institute an *inter partes* review, we must determine that the information presented in the Petition and the Preliminary Response shows "a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a). For the reasons set forth below, we determine that there is a reasonable likelihood that Petitioner will prevail with respect to at least one challenged claim. We institute an *inter partes* review of claims 1–21 based on the grounds set forth in the Petition.

B. Related Proceedings

The parties note that the '872 patent is involved in *GoSecure Inc. v. CrowdStrike, Inc., and Crowdstrike Holdings, Inc.*, Case No. 24-cv-526 in the Western District of Texas, Austin Division. Pet. 81; Paper 5, 1. Additionally, Petitioner notes that it has filed another petition challenging claims of the '872 patent in IPR2025-00070.

C. The '872 Patent

The '872 patent "relates generally to systems and methods for protecting computer networks, including but not limited to systems and methods for analyzing malicious activities on a computer system in order to better protect the computer from future malicious activity." Ex. 1001, 1:44–48. The '872 patent discusses more details in connection with Figure 1, which is reproduced below.

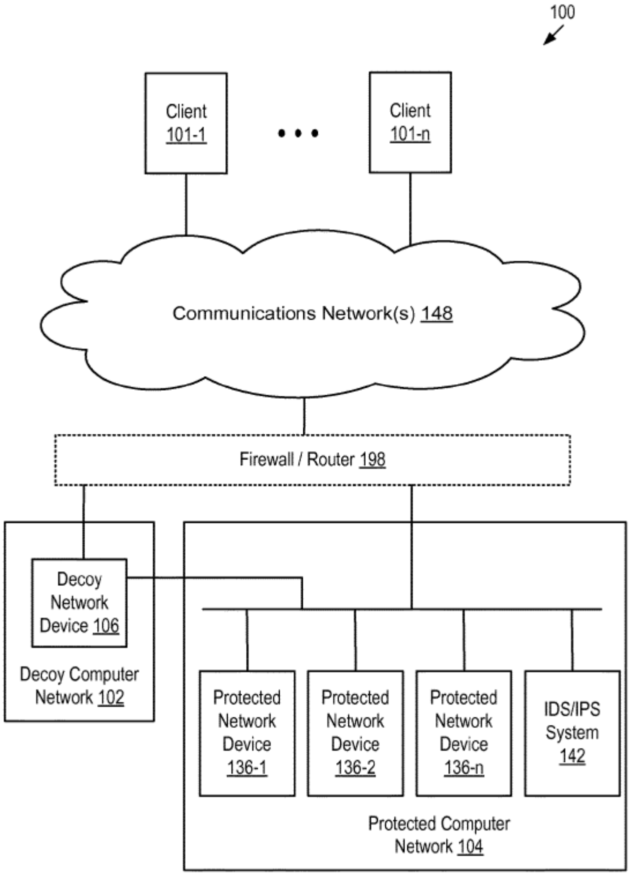
100
Client 101-1
Client 101-n
Communications Network(s) 148
Firewall / Router 198
Decoy Network Device 106
Decoy Computer Network 102
Protected Network Device 136-1
Protected Network Device 136-2
Protected Network Device 136-n
IDS/IPS System 142
Protected Computer Network 104

Figure 1

The '872 patent explains that "[Figure] 1 is a high-level block diagram illustrating an exemplary distributed computer system." Ex. 1001, 3:26–28.

More specifically, Figure 1 shows distributed computer system 100, which "includes a decoy computer network 102, a communications network 148, and protected computer network 104." Ex. 1001, 4:5–8. Additionally, client computers 101 may have access to decoy computer network 102 and protected computer network 104 via communications network 148. *Id.* at 4:13–24.

"Typically, the protected computer network 104 includes a firewall/router 198 to protect the protected network devices 136 and route network traffic to and from the protected network devices 136." Ex. 1001, 4:30–33. "In some embodiments, the protected computer network 104 also includes an IDS/IPS system 142 (intrusion detection and prevention system)." *Id.* at 4:37–39. IDS/IPS system 142 may use "fingerprints of unauthorized activities" to "prevent[] unauthorized activities matching the stored fingerprints by modifying the protected network devices 136 and/or the firewall/router 198." *Id.* at 4:39–47.

"The decoy computer network 102 includes one more decoy network device(s) 106. The decoy network device 106 is a decoy system that is monitored to collect fingerprint data of unauthorized activities." Ex. 1001, 4:57–60. "In some embodiments, the decoy network device 106 is intentionally kept vulnerable to unauthorized or malicious activities (e.g., known security weaknesses may be intentionally left unfixed or other security components (e.g., firewalls) are intentionally not installed)." *Id.* at 4:60–65. "The purpose of the decoy network device 106 is to allow attackers to attack the decoy network device 106, so that the pattern of attack can be monitored and analyzed to generate a fingerprint," which can be used to forestall similar future attacks. *Id.* at 5:3–9. Along with other components, decoy network device 106 may include at least one virtual machine. *Id.* at 5:31–32, 59–61, 6:6–9, 6:24–28, Fig. 2.

The '872 patent discusses a method that decoy network device 106 may perform in connection with Figures 6A–6C, which are reproduced below.

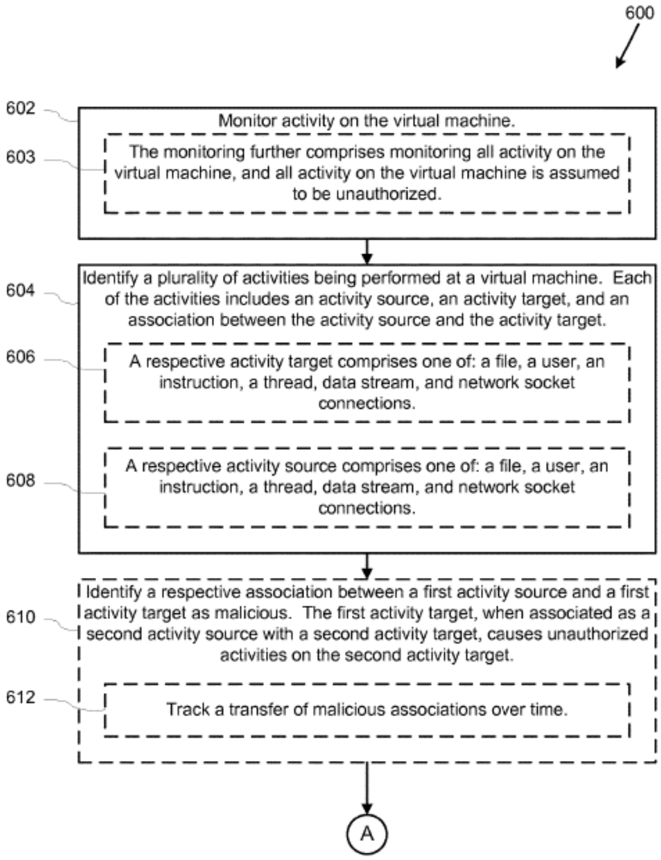
600
602
Monitor activity on the virtual machine.
603
The monitoring further comprises monitoring all activity on the virtual machine, and all activity on the virtual machine is assumed to be unauthorized.
604
Identify a plurality of activities being performed at a virtual machine. Each of the activities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

Figure 6A

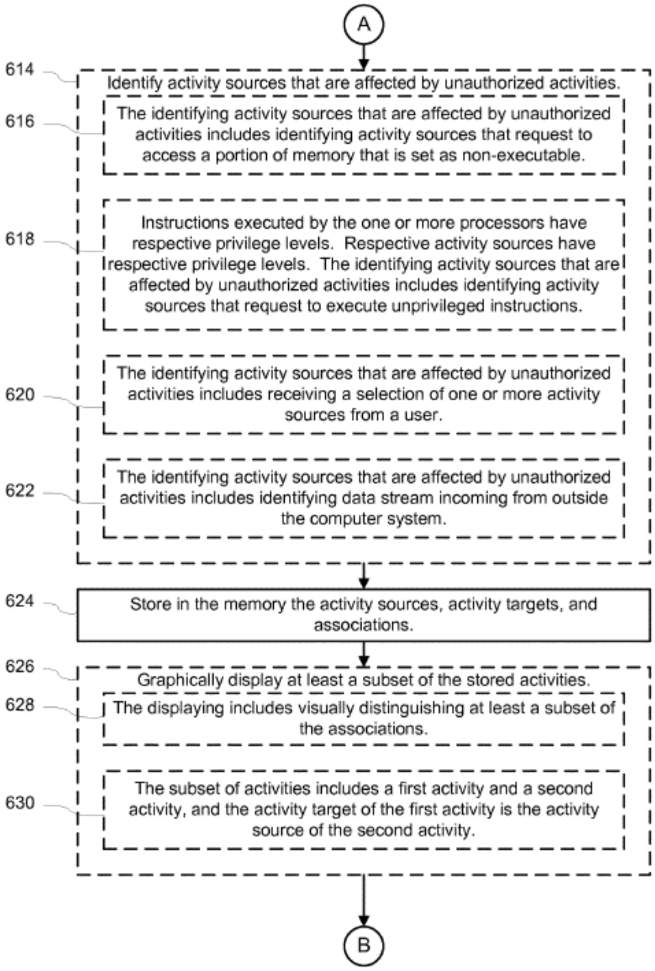
A
614
Identify activity sources that are affected by unauthorized activities.
616
The identifying activity sources that are affected by unauthorized activities includes identifying activity sources that request to access a portion of memory that is set as non-executable.
618
Instructions executed by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

Figure 6B

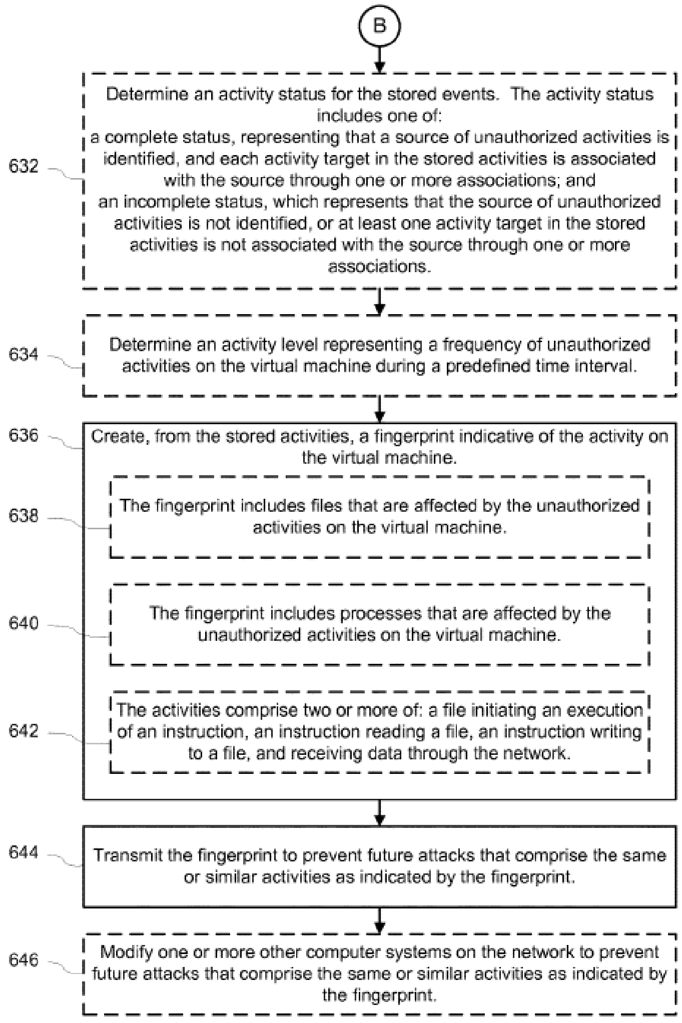
B
Determine an activity status for the stored events. The activity status includes one of:
a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations; and
an incomplete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

Figure 6C

The ’872 patent explains that “[Figures] 6A-6C are flowcharts representing a method of identifying unauthorized activities on a computer system.” Ex. 1001, 3:47–49.

In this method, “[t]he decoy network device monitors (602) activity on the virtual machine.” Ex. 1001, 15:7–8. Additionally, “[t]he decoy network device identifies (604) a plurality of activities being performed at the virtual machine.” *Id.* at 15:25–26. “In some embodiments, the decoy network device identifies (610) a respective association between a first activity source and a first activity target as unauthorized.” *Id.* at 15:48–50.

Later, "[t]he decoy network device stores (624) the activity sources, activity targets, and associations in its memory." *Id.* at 16:56–57. The decoy network device also "creates (636) a fingerprint indicative of the activity on the virtual machine from the stored activities." *Id.* at 18:4–6. The decoy network device may share the fingerprint:

> The decoy network device transmits (644) the fingerprint to one or more protected network devices 136 to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the decoy network device transmits the fingerprint to the IDS/IPS system 142 to prevent future attacks that comprise the same or similar activities on one or more protected network devices 136.
>
> In some embodiments, one or more other computer systems (e.g., protected network devices 136) on the network are modified (646) to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (e.g., in FIG. 1A, the IDS/IPS system modifies at least one of the protected network device(s) 136 to prevent future attacks that comprise the same or similar activities).

Ex. 1001, 18:44–58.

D. Illustrative Claims

Of the challenged claims, claims 1, 20, and 21 are independent. Each of claims 2–19 depends, directly or indirectly, from independent claim 1. Claim 1 is illustrative for our analysis herein and is reproduced below with certain reformatting:[1]

> 1. [1(pre)] A computer implemented method of identifying unauthorized activities on a first computer system attached to a computer network, wherein the first computer system comprises one or more processors and memory, the method comprising:
>
> [1(a)] monitoring activity on the first computer system;

[1] We have added the same labels that Petitioner uses to identify portions of claim 1. *See, e.g.*, Pet. 18–45.

> [1(b)] identifying a plurality of activities being performed at the first computer system, wherein each of the activities includes an activity source, an activity target, and an association between the activity source and the activity target;
>
> [1(c)] storing in the memory a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and
>
> [1(d)] transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

Ex. 1001, 19:39–59.

E. ASSERTED GROUNDS

Petitioner asserts that claims 1–21 would have been unpatentable on the following grounds (Pet. 8):

Ground	Claim(s) Challenged	35 U.S.C. §	References
1	1–12, 14–16, 18–21	103	Capalik[2], King[3]
2	13	103	Capalik, King, Pike[4]
3	17	103	Capalik, King, Farley[5]

[2] Alen Capalik, United States Patent Application Publication No. 2008/0016570 A1, published Jan. 17, 2008 (Ex. 1004, "Capalik").
[3] Samuel T. King, "*Analyzing Intrusions Using Operating System Level Information Flow*" (Ex. 1006, "King").
[4] Geoffrey Pike et al., U.S. Patent No. 8,819,822 B1, issued Aug. 26, 2014 (Ex. 1007, "Pike").
[5] Timothy P. Farley et al., U.S. Patent No. 7,089,428 B2, issued Aug. 8, 2006 (Ex. 1008, "Farley").

In support of its challenges, Petitioner also relies on the Declaration of Markus Jakobsson, Ph.D. Ex. 1003. Patent Owner supports its Preliminary Response with a Declaration of Joseph Greenfield, Ph.D. Ex. 2001.

II. DISPUTE REGARDING MULTIPLE PETITIONS

In addition to challenging the claims of the ’872 patent with the instant Petition, Petitioner filed a petition in IPR2025-00070, which also challenged claims of the ’872 patent. IPR2025-00070, Paper 1 (“the ’70 Petition”). Petitioner ranked the ’70 Petition first and the instant Petition second. Paper 3, 5.

Petitioner explained that it filed two petitions because it is unsure whether Patent Owner may argue for a broad or narrow interpretation of the term “association” in limitation 1(b) of challenged claim 1 of the ’872 patent. Paper 3, 1–2. Given this and the “complexity of the subject matter and the number of claims challenged,” Petitioner argued that two petitions are warranted. *Id.* at 3–4. Petitioner stated, however, that it would be appropriate for us to institute the ’70 Petition and deny the instant Petition if Patent Owner conceded that the broader interpretation of “association” is correct. *Id.* at 5.

Patent Owner argued that we should not institute both petitions. Paper 8, 1–5. Patent Owner argued that the challenged claims are not long and Petitioner’s concerns about the construction of “association” in limitation 1(b) are “contrived.” *Id.* at 1. Patent Owner contends that Petitioner could have addressed all of the challenged claims in one petition. *Id.* Noting that both the ’70 petition and the instant Petition challenge all claims of the ’872 patent, Patent Owner argued that the number of claims challenged does not necessitate multiple petitions. *Id.* at 2–3. Patent Owner also argued that Petitioner could have waited until closer to the statutory due date for filing the Petition to see how Patent Owner might have construed the claim language "association" in the related district court proceeding. *Id.* at 4–5.

Considering the facts holistically, we determine the totality of the circumstances here supports Petitioner's position that two petitions are warranted. Petitioner has challenged a large number of claims directed to complex subject matter. And the task of challenging those claims is complicated by the potential for Patent Owner to argue for a narrow construction of "association" in limitation 1(b). Patent Owner's suggestion that Petitioner would not have needed to file multiple petitions if it had waited longer to file a petition is not persuasive. Paper 8, 4–5. Patent Owner does not explain why a petitioner should be encouraged to delay the filing of its petition. *See id.* And the parties appear to agree that Patent Owner has not weighed in on whether "association" should be interpreted narrowly or broadly. Prelim. Reply. 8; Prelim. Sur-Reply 8. The present circumstances, considered as a whole, warrant two petitions challenging the claims of the '872 patent.

III. ANALYSIS

A. Level of Ordinary Skill

Petitioner explains the applicable level of skill in the art as follows:

> As of June 24, 2010, a person of ordinary skill in the art (POSITA) would be a person having a bachelor's degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience. A POSITA would also have had a working knowledge of software security analysis and dynamic malware analysis. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education.

Pet. 7 (Ex. 1003 ¶¶ 41–43). Patent Owner does not dispute Petitioner's explanation of the level of skill in the art. *See* Prelim. Resp. 13.

At this stage of the proceeding and on the present record, we adopt Petitioner's uncontested proposed level of ordinary skill in the art, which we find consistent with the level of ordinary skill in the art reflected by the '872 patent and the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995); *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978).

B. Claim Construction

In an *inter partes* review, we apply the same claim construction standard as would be used by a district court to construe a claim in a civil action involving the validity or infringement of a patent. 37 C.F.R. § 42.100(b). Under that standard, claim terms are given their ordinary and customary meaning, as would have been understood by a person of ordinary skill in the art at the time of the invention, in light of the language of the claims, the specification, and the prosecution history of record. *Id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–19 (Fed. Cir. 2005) (en banc); *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365–66 (Fed. Cir. 2012).

Additionally, only terms that are in controversy need to be construed, and these need be construed only to the extent necessary to resolve the controversy. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) ("The Board is required to construe 'only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

The parties' arguments raise one claim-construction dispute that warrants detailed discussion at this stage of the proceeding, specifically the parties' dispute regarding the scope of limitation 1(d):

> transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

Ex. 1001, 19:53–59.

The parties do not agree about where information must be transmitted in order to perform the claimed step. *E.g.*, Prelim. Reply 1–3; Prelim. Sur-Reply 1–3. Petitioner contends that transmitting information to a "protected network, including protected endpoint devices and the IDS/IPS" falls within the scope of the claimed step. *E.g.*, Prelim. Reply 2. Patent Owner contends that the claimed step requires transmitting the information "to 'protected network device' that are actually the subject of future attacks." *E.g.*, Prelim. Sur-Reply 3. According to Patent Owner, this does not encompass transmitting the information to an IDS/IPS. *Id.* at 1.

Weighing the parties' arguments and evidence, we determine Petitioner has shown a reasonable likelihood of prevailing on this claim-construction dispute. In particular, we determine there is a reasonable likelihood of Petitioner demonstrating that limitation 1(d) encompasses transmitting the information to a group of components that includes components subject to future attacks, such as a protected network. *E.g.*, Prelim. Reply 2–3. The arguments and evidence currently of record do not support a conclusion that limitation 1(d) narrowly requires transmitting the recited "information" specifically to "protected network devices," as Patent Owner contends. Prelim. Resp. 24; Prelim. Sur-Reply 3.

We first look to the claim language itself. It recites "transmitting to one or more computer *systems*," not transmitting to "devices." Ex. 1001, 19:53. Although the claim language "one or more computer systems" may encompass "protected network devices," we do not see a reason that its plain meaning would be limited to network devices, much less protected network devices.

Nor do we see a reason that the plain meaning of "one or more computer systems" is limited to protected network devices to the exclusion of a network that includes protected network devices and one or more other components. In support of its suggestion that the claim language "one or more computer systems" excludes a combination of protected network devices and one or more other components, Patent Owner cites the claim language "for preventing future attacks, to the one or more computer systems." Prelim. Resp. 20–24; Prelim. Sur-Reply 1–2. But Patent Owner does not provide reasoning or evidence persuading us to read the claim language more narrowly than its plain meaning, which encompasses preventing future attacks to a computer system that includes both protected network devices and one or more other components.

When discussing attack-prevention, the Specification discloses transmitting a fingerprint to protected network devices 136 or to IDS/IPS system 142. Ex. 1001, 18:44–58. Patent Owner argues that limitation 1(d) is limited to transmitting information to protected network devices. Prelim. Sur-Reply 3. But Patent Owner does not provide persuasive reasoning or evidence that the claims do not also encompass the disclosed approach of transmitting to a protected network by transmitting to the network's IDS/IPS, which protects other devices on the network.

Patent Owner argues that the Specification supports its construction, but Petitioner more persuasively argues that the Specification supports its construction. Prelim. Sur-Reply 2–3; Prelim. Reply 2–3. Both parties cite the following passage:

> The decoy network device transmits (644) the fingerprint to one or more protected network devices 136 to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint. In some embodiments, the decoy network device transmits the fingerprint to the IDS/IPS system 142 to prevent future attacks that comprise the same or similar activities on one or more protected network devices 136.
>
> In some embodiments, one or more other computer systems (e.g., protected network devices 136) on the network are modified (646) to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint (e.g., in FIG. 1A, the IDS/IPS system modifies at least one of the protected network device(s) 136 to prevent future attacks that comprise the same or similar activities).

Ex. 1001, 18:44–58.

Patent Owner suggests that this discloses two embodiments: one embodiment involving transmitting the fingerprint to the IDS/IPS and a different embodiment involving transmitting the fingerprint to protected network devices. Prelim. Sur-Reply 3. According to Patent Owner, "[o]nly the latter is claimed." *Id.* Patent Owner does not persuasively support this position. Indeed, Patent Owner does not clearly explain its basis for this position.

To the extent Patent Owner's position stems from a belief that the '872 patent uses the language "computer system" to mean only protected endpoint devices, the Specification does not support Patent Owner's position. Rather, consistent with Petitioner's arguments, the Specification repeatedly uses the term "computer system" to refer to things that are not limited to protected endpoint devices. Prelim. Resp. 2–3. For instance, the Specification refers to "one or more other computer systems (e.g., protected network devices 136)." Ex. 1001, 18:52–53. Thus, the Specification lists "protected network devices 136" as only an example of "other computer systems," demonstrating that "computer systems" refers to things other than protected network devices.

Consistent with this, as Petitioner notes, the Specification uses the language "distributed computer system" when referring to numerous components, including "protected network devices" and an "IDS/IPS system." Ex. 1001, 3:26–28; Prelim. Reply 2. This demonstrates that, contrary to Patent Owner's arguments, a "computer system" (1) can include components other than protected endpoint devices, and (2) can include an IDS/IPS system. *See, e.g.*, Prelim. Sur-Reply 2 ("[T]he specification repeatedly distinguishes IDS/IPS and computer systems.").

Patent Owner argues that the '872 patent "distinguishes between" a "computer system" and a "distributed computer system." Prelim. Sur-Reply 3. This argument does not support a narrow construction of the "one or more computer systems" recited in limitation 1(d). The Specification's use of "distributed computer system" to refer to a particular type of computer system does not support a narrow understanding of the language "computer system." Logically, although the language "distributed computer system" refers to a particular type of computer system, the language "computer system" omits the modifier "distributed" and thus, refers to all types of computer systems, including distributed computer systems.

Moreover, to the extent Patent Owner's claim construction stems from a belief that "protected network devices" constitute the only thing that can be protected from the "future attacks" recited in limitation 1(d), Patent Owner does not provide persuasive evidence or reasoning for such a position. For example, Patent Owner does not provide persuasive reasoning or evidence that the claim language "preventing future attacks, to the one more computer systems" would only mean preventing attacks that harm every part of a computer system, as opposed to also preventing attacks that harm only parts of the computer system.

In sum, as noted above, based on all of the evidence and arguments of record, we find a reasonable likelihood of Petitioner demonstrating that limitation 1(d) encompasses transmitting the information to a group of components that includes components subject to future attacks, such as a protected network.

C. Prior Art References

1. Capalik

Capalik "relates to the field of methods and systems for protecting computer networks." Ex. 1004 ¶ 2. Capalik discusses an embodiment in connection with Figure 5, which is reproduced below.

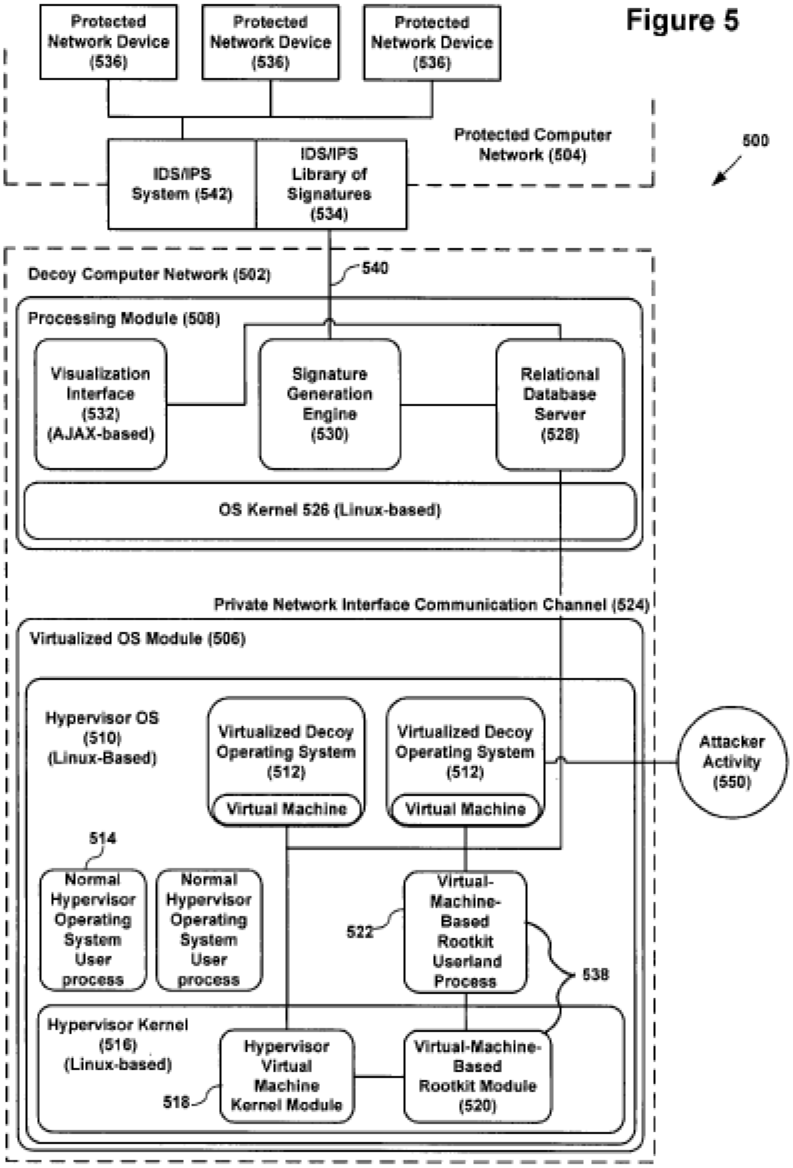
Figure 5
Protected Network Device (536)
Protected Network Device (536)
Protected Network Device (536)
Protected Computer Network (504)
500
IDS/IPS System (542)
IDS/IPS Library of Signatures (534)
Decoy Computer Network (502)
540
Processing Module (508)
Visualization Interface (532) (AJAX-based)
Signature Generation Engine (530)
Relational Database Server (528)
OS Kernel 526 (Linux-based)
Private Network Interface Communication Channel (524)
Virtualized OS Module (506)
Hypervisor OS (510) (Linux-Based)
Virtualized Decoy Operating System (512)
Virtual Machine
Virtualized Decoy Operating System (512)
Virtual Machine
Attacker Activity (550)
514
Normal Hypervisor Operating System User process
Normal Hypervisor Operating System User process
522
Virtual-Machine-Based Rootkit Userland Process
538
Hypervisor Kernel (516) (Linux-based)
518
Hypervisor Virtual Machine Kernel Module
Virtual-Machine-Based Rootkit Module (520)

Figure 5 is a block diagram showing "a system for analyzing and preventing unauthorized intrusion into a computer network." Ex. 1004 ¶¶ 20, 37.

Specifically, Figure 5 shows system 500, which comprises decoy computer network 502 and protected computer network 504. Ex. 1004 ¶ 38. "The decoy computer network 502 includes a virtualized operating system module 506 for monitoring the decoy network 502, and a processing module 508 for obtaining, analyzing, and responding to exploits." *Id.* "The 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." *Id.* ¶ 53.

"In use, attacker activity 550 is directed at the decoy computer network 502 through one more ports . . . that are left open as a gateway for attacker activity." Ex. 1004 ¶ 44. When an attacker connects to an open port, decoy computer network 502 "monitors and captures information from the connection, including port numbers, data streams, file uploads, keystrokes, ASCII or binary files, malicious payloads, memory manipulation attempts, and any other data transfers or malicious attempts." *Id.* ¶ 49. If the interaction warrants creating an attack signature, decoy computer network 502's processing module 508 may generate an attack signature. *Id.* ¶¶ 52, 59. The attack signature may be sent "to the intrusion detection system (IDS) or intrusion prevention system (IPS) for the protected network 504." *Id.* ¶ 59.

2. King

King notes that "[m]odern computer systems are under attack." Ex. 1006, 9.[6] With this background, King "propose[s] using operating-system-level (OS-level) information-flow graphs to highlight the activities of an attacker." *Id.* at 11. King notes that "[i]nformation-flow graphs can be used to describe behavior on a computer system":

> A graph of *known-good* behavior defines how a service interacts with the system and how information flows between components, any deviations from this graph of known-good behavior may indicate potentially suspicious activity. In addition, a graph of *known-bad* behavior defines known

[6] We cite to the page numbers in the lower, righthand corner of King, rather than King's native page numbers.

> malicious activities, acting as a signature for an intrusion detection system.

Ex. 1006, 64.

D. GROUND 1 – ALLEGED OBVIOUSNESS OVER CAPALIK AND KING

In asserting obviousness of claims 1–12, 14–16, and 18–21 over Capalik and King, Petitioner cites Capalik as teaching most of the challenged claims' limitations. Pet. 18–69. Petitioner relies on King when addressing limitation 1(b) of challenged claim 1. *Id.* at 27–40. Noting that Patent Owner may argue that limitation 1(b)'s "claimed ***association*** requires classifying or characterizing the individual activities as authorized or unauthorized (i.e., benign or malignant)," Petitioner argues that "*King* teaches a computer monitoring process similar to *Capalik's*, but additionally teaches that each individual activity related to an attack is classified as benign or malignant before generating a signature indicative of the attack." *Id.* at 27–28. Petitioner further argues that "[a person of ordinary skill in the art] would have been motivated to modify *Capalik* per *King's* teachings to identify, store, and graphically display attack activities including the activity sources, activity targets, and associations between them (i.e., benign and malignant activities)." *Id.* at 38.

At this stage, Patent Owner disputes Ground 1 two ways. Patent Owner argues that "Petitioner failed to establish that King (Ex. 1006)—part of every ground in the Petition—was publicly accessible before the critical date of the '872 patent." Prelim. Resp. 1. Patent Owner also argues that Petitioner has not shown Capalik teaches limitation 1(d). *Id.*

Having reviewed all of the parties' arguments and evidence, we determine Petitioner has demonstrated a reasonable likelihood of establishing that at least claim 1 of the '872 patent would have been obvious over Capalik and King. Pet. 8–14, 18–49; Prelim. Resp. 20–37; Prelim. Reply 1–7; Prelim. Sur-Reply 1–8. We turn now to detailed discussions of the two disputes raised by Patent Owner's arguments.

1. Whether King Was Publicly Accessible Before the '872 Patent's Critical Date

Patent Owner disputes Petitioner's position that King was publicly accessible before the '872 patent's critical date. Pet. 11–12; Prelim. Resp. 28–37; Prelim. Reply 4–8; Prelim. Sur-Reply 4–8. At this stage, Petitioner does not dispute Patent Owner's contention that June 24, 2010, which is the filing date of the earliest provisional application to which the '872 patent claims priority, is the '872 patent's critical date. *E.g.*, Prelim. Resp. 28; Pet. 3.

"A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art[,] exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)). "When a reference is uploaded to a website or deposited in a library, the fact that the reference is indexed or cataloged in some way can indicate that it is publicly accessible." *Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019). "[A]t the institution stage, the petition must identify, with particularity, evidence sufficient to establish a reasonable likelihood that the reference was publicly accessible before the critical date of the challenged patent and therefore that there is a reasonable likelihood that it qualifies as a printed publication." *Hulu v. Sound View*

Innovations, LLC, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential).

In support of its contention that King "qualifies as prior art under 35 U.S.C. § 102(b)," Petitioner contends that King was publicly available soon after November 28, 2006:

> *King* was submitted to the University of Michigan library in partial fulfillment of the requirements for the degree of Doctor of Philosophy (Computer Science and Engineering) of Samuel T. King. *See King* (Ex. 1006). The University of Michigan library first acquired *King* as of November 28, 2006, and it was made publicly available shortly after its initial acquisition date. *See Munford Dec.*, (Ex. 1009). Therefore, *King* qualifies as prior art under 35 U.S.C. § 102(b) (pre-AIA). *Id.*

Pet. 11–12.

In its Preliminary Response, Patent Owner counters that Petitioner "failed to establish that King—part of every ground in the Petition—was publicly accessible before the critical date of the '872 patent (i.e., June 24, 2010)." Prelim. Resp. 28. Noting that Petitioner supports its assertion of King's public accessibility with a declaration of Ms. June Ann Munford, Patent Owner argues that "Ms. Munford's declaration is fatally deficient for at least two reasons. First, Ms. Munford fails to identify any specific date on which King was allegedly made publicly available, much less any evidence that King was publicly available before the critical date of the '872 patent." *Id.* at 30. Patent Owner elaborates that "[n]either Ms. Munford nor Petitioner provides any evidence that the library's catalog (or a substantially similar one) existed on or before the critical date (e.g., via archived versions of the catalog)." *Id.*

"Second, even if King were technically available to the public, Petitioner fails to explain how an interested party would have located King in 2010," Patent Owner argues. Prelim. Resp. 30. Patent Owner asserts that "[n]either Ms. Munford nor Petitioner explains why an interested party, in 2010, would have known: (1) to search the University of Michigan's library; and (2) to search Michigan's library catalog using every word of King's ***title***." Prelim. Resp. 33.

In its Preliminary Reply, Petitioner asserts that "[t]he existing record demonstrates that King was publicly available before the priority date and that a fully developed record is at least reasonably likely to prove this." Prelim. Reply 4. Petitioner likens its evidence of public accessibility to the facts of other proceedings in which a document was found to be publicly accessible. *Id.* at 4–6. For example, Petitioner argues that "King's MARC record contains a Field 005 entry, indicating that all listed indexing occurred as of August 30, 2007. The Board has relied on Field 005 to establish public accessibility." *Id.* at 5–6 (citing *Kinaxis Inc. v. Blue Yonder Group, Inc.*, IPR2021-01205, Paper 16, 12–15 (PTAB Jan. 19, 2022)). Petitioner adds that "[n]ewly introduced here, responsive to the [Preliminary Response], Dr. Samuel T. King's declaration further confirms that King was publicly accessible before 2010." *Id.* at 6 (citing Ex. 1028).

In its Preliminary Sur-Reply, Patent Owner maintains that its "Preliminary Response established that Petitioner's evidence and arguments in support of King's alleged public availability were woefully deficient." Prelim. Sur-Reply 4. Patent Owner argues that Petitioner's Preliminary Reply does not salvage Petitioner's case. *Id.* at 4–8. For example, Patent Owner asserts that "Petitioner also argues that the '005' field, which indicates the last modification to a MARC record, within King's MARC record, supports its contentions. But again, that is not sufficient on this record. At best, Petitioner's arguments go to 'technical accessibility.'

Petitioner has still failed to show public accessibility, for which more is required." *Id.* at 6. Patent Owner also argues that Dr. King's declaration evidences "[e]fforts to disseminate his 'research,'" but does not show public availability of King, specifically. *Id.* at 7.

Considering the totality of the evidence and arguments presently of record, we find Petitioner has demonstrated a reasonable likelihood of establishing that King was publicly accessible before 2010. Patent Owner does not dispute Petitioner's evidence that the University of Michigan library acquired King *over three years before* 2010, specifically on November 28, 2006. Ex. 1009 5, 22; Pet. 12; Prelim. Resp. 28–37; Prelim. Reply 6; Prelim. Sur-Reply 4–8. Nor does Patent Owner dispute Petitioner's evidence that the University of Michigan library's catalog enabled Ms. Munford to locate King in 2024. Ex. 1009, 3–4; Prelim. Resp. 28–37; Prelim. Reply 4; Prelim. Sur-Reply 4–8. But Patent Owner suggests that Petitioner's evidence does not show sufficiently if or when King become discoverable to interested persons, as opposed to merely showing "technical accessibility" of King. Prelim. Resp. 30–34; Prelim. Sur-Reply 4–8.

Viewed as a whole, Petitioner's evidence demonstrates a reasonable likelihood of establishing that interested persons exercising reasonable diligence could have found King at the University of Michigan library before 2010. Petitioner provides evidence tending to show that King was available at the University of Michigan library "shortly after" its acquisition on November 28, 2006, as Ms. Munford testifies. Pet. 11–12 (citing Ex. 1009); Prelim. Reply 4–7 (citing Ex. 1009; Ex. 1028). For example, Patent Owner does not dispute Petitioner's contention that in King's MARC record, Field 005 lists August 30, 2007, which is the last modification date of the MARC record. Prelim. Reply 5; Ex. 1009, 22; Prelim. Sur-Reply 6.

This tends to show availability of King in the University of Michigan library's catalog as of August 30, 2007.

Additionally, contrary to Patent Owner's objections, Petitioner provides evidence that an interested person exercising reasonable diligence could have found King. For example, Petitioner provides significant evidence of pre-2010 public information that interested persons would have had about Mr. King's work generally, as well as King specifically. Prelim. Reply 6–7; Ex. 1028. For instance, Patent Owner does not dispute Petitioner's assertion that Dr. King's "thesis advisor, Dr. Peter Chen, . . . maintained a publicly accessible University of Michigan website," "including a description and direct link to King." Prelim. Reply 7; Ex. 1028, 4–5, 41; Prelim. Sur-Reply 4–8.

2. Limitation 1(d)

As noted above, limitation 1(d) recites the following:

> transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources, the activity targets, and the associations for preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.

Ex. 1001, 19:53–59.

Addressing this limitation, Petitioner cites Capalik's disclosure of transmitting an attack signature generated at decoy computer network 502 to protected computer network 504. Pet. 48 (citing Ex. 1004 ¶¶ 53, 59, Fig. 5; Ex. 1003 ¶¶ 157–158). Petitioner argues that Capalik "teaches that once the attack signature is generated, it can be sent 'to the intrusion detection system (IDS) or intrusion prevention system IPS) for the protected network 504.'" *Id.* (citing Ex. 1004 ¶¶ 53, 59; Ex. 1003 ¶¶ 157–158). Petitioner contends that "a [person of ordinary skill in the art] would have understood that *Capalik* transmits the fingerprint, including information identifying one or more of the activity sources, the activity targets, and the associations to prevent future attacks that comprise the same or similar activities as indicated by the fingerprint." *Id.* at 49 (citing Ex. 1003 ¶¶ 157–158). Petitioner further argues that "[a person of ordinary skill in the art] would have further understood that *Capalik* transmits this information to a computer system other than computer decoy 502 since the signature is sent 'through a standard network connection' to IDS/IPS 534 of protected network 504." *Id.* (citing Ex. 1004 ¶ 59, Fig. 5; Ex. 1003 ¶ 158).

Patent Owner counters that Capalik does not disclose limitation 1(d). Prelim. Resp. 20–28. According to Patent Owner, limitation 1(d) "expressly requires that the attack-identifying information ultimately reach one or more protected network devices." *Id.* at 24. Capalik's disclosure of transmitting information to the IDS/IPS does not meet this requirement, Patent Owner argues. *Id.* at 21–24. Patent Owner argues that Capalik's "IDS/IPS is a distinct component of Capalik's system from the protected network devices themselves." *Id.* at 21–22. Patent Owner argues that Capalik's IDS/IPS does not need protection but provides protection for other devices. *Id.* at 22.

In its Preliminary Reply, Petitioner counters that Patent Owner's argument "turns entirely on whether the claimed 'computer systems' should be construed narrowly to mean the individual endpoint themselves—as PO contends—or more broadly to capture the protected network, including protected endpoint devices and the IDS/IPS—as Petitioner contends." Prelim. Reply 2. Petitioner argues that Patent Owner errs in asserting that "'sending the information to the IDS/IPS is not enough,' even where the

IDS/IPS is coupled to protected endpoint devices in a protected network." *Id.* at 2.

In its Preliminary Sur-Reply, Patent Owner maintains that the proper interpretation of limitation 1(d) requires "transmitting [the information] to 'protected network devices' that are actually the subject of future attacks." Prelim. Sur-Reply 3. And Patent Owner reiterates that Capalik does not teach the disputed limitation because "Capalik only discloses transmitting information from a 'decoy' system to an IDS/IPS." *Id.* at 1.

Additionally, Patent Owner suggests that Capalik's IDS/IPS cannot be considered part of the same "computer system" as protected network devices 536 but separate from decoy computer network 502:

> if Petitioner's argument—that "computer systems" encompass Capalik's IDS/IPS because the IDS/IPS is coupled to the endpoints (Reply 2)—were correct (it is not), then Petitioner has utterly failed to show that Capalik's IDS/IPS is the claimed "computer system[] ***other than the first computer system***." Capalik's IDS/IPS is also coupled to its decoy computer (Ex. 1004, Figure 5), which Petitioner maps as the "first computer system" (Pet. 19-20). But Petitioner fails to explain why, under its claim interpretation, the IDS/IPS is not "the first computer system."

Prelim. Sur-Reply 2 (alteration in original).

Weighing all of the parties' arguments and evidence, we determine Petitioner has demonstrated a reasonable likelihood of establishing that Capalik discloses limitation 1(d). For the reasons discussed above in Section III.B, contrary to Patent Owner's argument that the claim requires transmitting information to "protected network devices," the record evidence demonstrates a reasonable likelihood of Petitioner establishing that the claim encompasses transmitting the information to a group of components that includes components subject to future attacks, such as an IDS/IPS connected to endpoint devices.

Additionally, Petitioner demonstrates a reasonable likelihood of establishing that Capalik discloses such an approach. Capalik discloses that IDS/IPS system 542 and protected network devices 536 are components of protected computer network 504. Ex. 1004 ¶ 53. Capalik does not disclose that decoy computer network 502 is part of protected computer network 504. *See, e.g.*, *id.* ¶ 38, Fig. 5. Given this, we find a reasonable likelihood of Petitioner demonstrating Capalik's decoy computer network 502 corresponds to the claimed "first computer system" and protected computer network 504 corresponds to the claimed "one or more computer systems other than the first computer system." *E.g.*, Pet. 20 ("[A person of ordinary skill in the art] would have understood that the Decoy Computer 502 is a first computer system."), 48 (citing IDS/IPS of protected network 504 as recipient of transmitted signature). And Patent Owner does not dispute Petitioner's argument that Capalik discloses transmitting a fingerprint from decoy computer network 502 to computer network 504's IDS/IPS. Pet. 48–49; Prelim. Resp. 20–28; Prelim. Reply 1; Prelim. Sur-Reply 1–3. Moreover, Petitioner's evidence tends to show that Capalik transmits the fingerprint from decoy computer network 502 to computer network 504's IDS/IPS for preventing future attacks to computer network 504. Pet. 48–49 (citing Ex. 1004 ¶¶ 52, 53, 59, Fig. 5); Ex. 1003 ¶¶ 157–158.

In sum, the evidence of record demonstrates a reasonable likelihood of Petitioner establishing that Capalik discloses transmitting the fingerprint from a first computer system (decoy computer network 502) to one more computer systems other than the first computer system (protected computer network 504) for preventing future attacks to the one or more computer systems. Accordingly, Petitioner demonstrates a reasonable likelihood of establishing that Capalik discloses limitation 1(d).

E. Grounds 2 and 3

Petitioner's Grounds 2 and 3 build from Ground 1, citing additional prior art to address certain limitations added by dependent claims 13 and 17. Pet. 69–77. At this stage, Patent Owner does not dispute Grounds 2 and 3 separately from its arguments directed toward Ground 1. *See generally* Prelim. Resp. In view of our determination that Petitioner has demonstrated a reasonable likelihood of prevailing on its Ground 1 assertion that claim 1 would have been obvious over Capalik and King, we will institute *inter partes* review for all Petitioner's challenges, including Grounds 2 and 3. *See SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1354, 1359–60; *PGS Geophysical AS v. Iancu*, 891 F.3d 1354, 1360 (Fed. Cir. 2018); 37 C.F.R. § 42.108(a) ("When instituting *inter partes* review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.").

IV. ORDER

It is:

ORDERED that *inter partes* review of claims 1–21 of the '872 patent is instituted on all grounds presented in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial; the trial will commence on the entry date of this decision.

FOR PETITIONER:

Paul R. Hart
Adam P. Seitz
ERISE IP, P.A.
paul.hart@eriseip.com
adam.seitz@eriseip.com
ptab@eriseip.com

FOR PATENT OWNER:

S. Giri Pathmanaban
Clement Naples
CLEARY GOTTLIEB STEEN & HAMILTON LLP
gpathmanaban@cgsh.com
cnaples@cgsh.com

Raghav Bajaj
Daniel S. Todd
Steven W. Peters
LATHAM & WATKINS LLP
raghav.bajaj@lw.com
daniel.todd@lw.com
steven.peters@lw.com