

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

SECURITYPROFILING, LLC,
Patent Owner.

IPR2022-00035
Patent 10,893,066 B1

Before DEBRA K. STEPHENS, TREVOR M. JEFFERSON, and
SHARON FENICK, *Administrative Patent Judges*.

STEPHENS, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314, 37 C.F.R. § 42.4

I. INTRODUCTION

A. *Background and Summary*

Cisco Systems, Inc. (“Petitioner”) filed a petition for *inter partes* review (Paper 2 (“Pet.” or “Petition”)) challenging claim 1 of U.S. Patent 10,893,066 B1 (Ex. 1001 (“’066 Patent”)). SecurityProfiling, LLC (“Patent Owner”) timely filed a Preliminary Response (Paper 6 (“Prelim. Resp.”)). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides as follows:

(a) THRESHOLD.—The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is 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)).

Petitioner challenges claim 1 as unpatentable under 35 U.S.C. § 103 (Pet. 11). Generally, Patent Owner contends that the Petition should be denied (*see* Prelim. Resp.). Based on our review of the record, we conclude that Petitioner is reasonably likely to prevail in demonstrating that at least one of the challenged claims is not patentable.

Our findings of fact and conclusions discussed below are based on the evidentiary record developed thus far. This Decision to institute trial is not a final decision as to the patentability of any challenged claim. Any final decision will be based on the full record developed during trial.

B. *Real Parties in Interest*

Patent Owner states that SecurityProfiling, LLC is the real-party-in-interest (Paper 5, 1).

Petitioner states that Cisco Systems, Inc. is the real-party-in-interest (Pet. 72).

C. Related Matters

Patent Owner and Petitioner indicate the '066 Patent was asserted in the following district court proceedings:

SecurityProfiling, LLC v. Cisco Systems, Inc., No. 6-21-cv-00337 (W.D. Tex.); and

SecurityProfiling, LLC v. Trend Micro Incorporated, No. 6-21-cv-00330 (W.D. Tex.) (Pet. 72.; Paper 5, 2). Patent Owner indicates neither of these litigations is pending (Paper 5, 2).

Patent Owner indicates the '066 Patent is presently involved in the following district court proceedings:

SecurityProfiling, LLC v. Cisco Systems, Inc., No. 6-21-cv-01106 (W.D. Tex.); and

SecurityProfiling, LLC v. Trend Micro Incorporated, No. 6-21-cv-01105 (W.D. Tex.)

Patent Owner further states that the '066 Patent is related to the following patents challenged in *inter partes* review:

U.S. Patent No. 9,100,431 B2 (“the '431 Patent” or “Oliphant '431”), which was challenged in IPR2021-01242 and

U.S. Patent No. 10,609,063 B1, which was challenged in IPR2021-01428 (*id.*).

Petitioner further states that the '066 Patent “is part of the same patent family” as U.S. Patent No. 8,984,644 B2 (“the '644 Patent” or “Oliphant '644 Patent”) “with both claiming priority to a common patent, US 9,117,069 (both claiming priority as continuations-in-part)” (Pet. 43).

Petitioner states Oliphant '644 Patent, was challenged in IPR2017-02192 (*id.*).

D. The '066 Patent

The '066 Patent, titled “Computer Program Product and Apparatus for Multi-Path Remediation,” issued January 12, 2021 (Ex. 1001, codes (45), (54)). The '066 Patent describes “remediation techniques that collectively remediate [a] plurality of [computing] device vulnerabilities” (*id.* at code (57)). The '066 Patent states that, “[i]n one embodiment, attacks are accurately identified and mitigated before they reach their targets, and targeted vulnerabilities may be remotely remediated” (*id.* at 1:46–48). Figure 1, reproduced below shows one embodiment on the invention, in

relation to a system including a networked system of computers (*id.* at 1:48–47, Fig. 1).

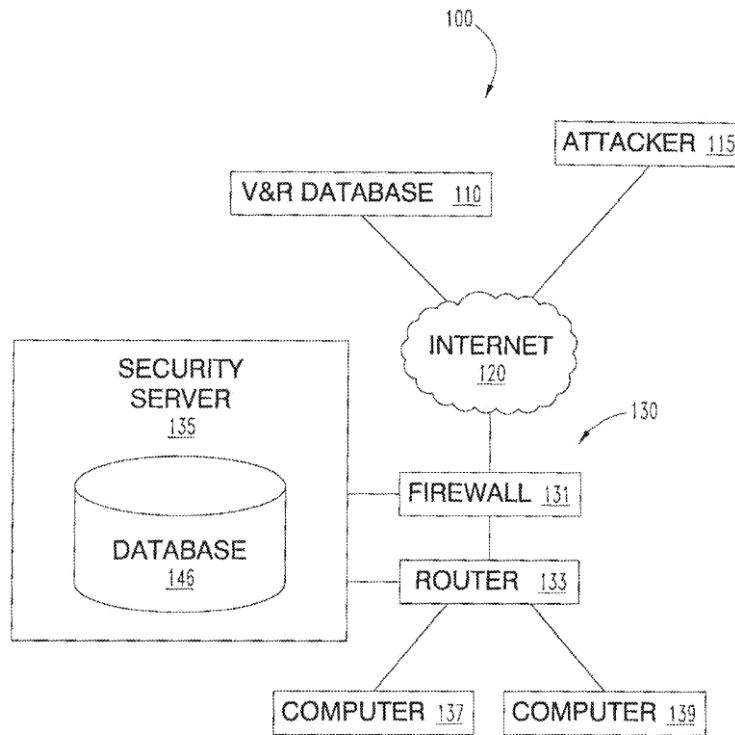


FIG. 1

As shown in Figure 1, subnet 130 is connected to the Internet 120 via included firewall 131, that serves as the gateway between the Internet 120 and the rest of subnet 130 (*id.* at 2:30–34, Fig. 1). Router 133 directs connections between computer 137 and other computers in the subnet 130 and those connected via the Internet 120 (*id.* at 2:34–36).

Also in subnet 130 is security server 135 that collects information from other devices in subnet 130, including information about software installed on the devices, the devices' configurations and policy settings, and patches that have been installed on those devices, and stores this information in database 146 (*id.* at 2:7–19, 2:36–38, 2:42–45, 3:37–40). Security server 135 additionally obtains from remediation database 110 “a regularly updated list of security vulnerabilities in software for a wide variety of operating

systems” and “a regularly updated list of remediation techniques that can be applied to protect a device from damage due to those vulnerabilities” (*id.* at 2:46–52).

Figure 3, reproduced below, traces signals that travel between the devices through the network shown in Figure 1 (*id.* at 1:51–53, Fig. 3).

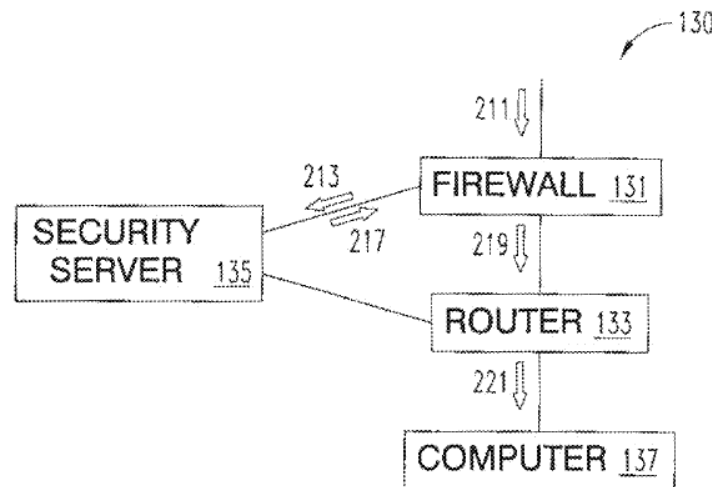


FIG. 3

As shown in Figure 3, “connection request 211 arrives at firewall 131 requesting that data be transferred to computer 137” (*id.* at 4:11–12, Fig. 3). That connection request may contain a payload designed to “takes advantage of a particular security vulnerability in a certain computer operating system” (*id.* at 4:13–15). Firewall 131 “sends a query 213 to security server 135” that uses information within the query to determine “whether connection request 211 is attempting to take advantage of a particular known vulnerability of destination machine 137” (*id.* at 4:15–24).

Query 213 includes information that security server 135 uses to determine (1) the intended destination of connection request 211, and (2) some characterization of the payload of connection request 211, such as a vulnerability identifier. Security server

135 uses this information to determine whether connection request 211 is attempting to take advantage of a particular known vulnerability of destination machine 137, and uses information from database 146 (see FIG. 2) to determine whether the destination computer 137 has the vulnerable software installed, and whether the vulnerability has been patched on computer 137, or whether computer 137 has been configured so as to be invulnerable to a particular attack

(*id.* at 4:17–29). Then, “security server 135 sends result signal 217 back to firewall 131 with an indication as to whether the connection request should be granted or rejected” (*id.* at 4:13–21). If result signal 217 “indicates that connection request 211 is to be rejected, firewall 133 drops or rejects the connection request 211” (*id.* at 4:35–38).

Further, “[a]nalogous operation[s] protect[] subnet 130 from compromised devices within the subnet 130 as well” (*id.* at 4:39–41). As an example, router 133 queries security server 135 before allowing one computer within subnet 130 to connect with another computer within the subnet to prevent a compromised computer 137 from taking advantage of a potential vulnerability in computer 139 (*id.* at 4:39–45; *see* Fig. 4). Again, in this case, based on security server 135’s response regarding device vulnerability, router 133 “determine[s] whether to allow the connection attempt” between devices of the subnet (*id.* at 4:54–57).

Furthermore, “upon a determination by security server 135 that a connection attempt or other attack has occurred against a computer that is vulnerable (based on its current software, patch, policy, and configuration status), security server 135 selects one or more remediation techniques from database 146 that remediate the particular vulnerability” (*id.* at 4:48–64).

Based on a prioritization previously selected by an administrator or the system designer, the remediation technique(s) are applied (1) to the machine that was attacked, (2) to all devices subject to

the same vulnerability (based on their real-time software, patch, policy, and configuration status), or (3) to all devices to which the selected remediation can be applied

(*id.* at 4:64–5:3). Remediation techniques may include: “the closing of open ports on the device; installation of a patch that is known to correct the vulnerability; changing the device’s configuration; stopping, disabling, or removing services; setting or modifying policies; and the like” (*id.* at 5:4–5:8; 5:58–60, 7:62–65).

E. Challenged Claims

Challenged claim 1 is the only challenged claim and is reproduced below.

1. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

said first vulnerability information generated utilizing the second vulnerability information, by:

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and

determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

identify an occurrence in connection with at least one of the plurality of devices;

determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being

taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices;

wherein the at least one configuration involves at least one operating system

(Ex. 1001, 31:50–32:48).

F. References Relied Upon

Petitioner relies upon the following prior art references:

Reference	Exhibit
Willebeek-LeMair, et al., US 7,359,962 B2, issued April 15, 2008 (“Willebeek-LeMair”)	1005
Gupta, et al., US 2003/0004689 A1, published Jan. 2, 2003 (“Gupta”)	1006
Graham, et al, US 7,237,264 B1, issued Jan. June 26, 2007 (“Graham”)	1007

(Pet. 11).

Petitioner also relies on the Declaration of Narasimha Reddy, Ph.D.

(Ex. 1003).

Patent Owner relies on the Declaration of Dr. Michael Smith

(Ex. 2001).

G. Prior Art and Asserted Grounds

Petitioner asserts that claim 1 is unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1	103	Willebeek-LeMair
1	103	Gupta, Graham

(Pet. 11).

II. ANALYSIS

A. Legal Standards

A patent claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains (*KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007)). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) when in evidence, objective evidence of nonobviousness (*Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966)).¹

“In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable” (*Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring *inter partes* review petitions to identify “with particularity . . . the evidence that supports the grounds for the

¹ Patent Owner does not present arguments or evidence of secondary considerations in its Preliminary Response. Therefore, secondary considerations do not constitute part of our analysis herein.

challenge to each claim’’)). This burden of persuasion never shifts to Patent Owner (*see Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (discussing the burden of proof in *inter partes* review)).

B. Level of Ordinary Skill in the Art

The level of skill in the art is a factual determination that provides a primary guarantee of objectivity in an obviousness analysis (*Al-Site Corp. v. VSI Int’l Inc.*, 174 F.3d 1308, 1324 (Fed. Cir. 1999) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966); *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991))).

Petitioner asserts that a person of ordinary skill in the art (“POSITA”) in July 2003 would have had a working knowledge of the network communications art that is pertinent to the ’066 Patent, including network security. A POSITA would have had a bachelor’s degree in computer science, computer engineering, or an equivalent, and two years of professional experience relating to network communications. Lack of professional experience can be remedied by additional education, and vice versa (Pet. 9 (citing Ex. 1003 ¶¶ 17–19)).

Patent Owner agrees with Petitioner’s assertion and further asserts a “higher level of education (e.g., a Master’s degree) may make up for less work experience, and additional work experience may make up for less education” (Prelim. Resp. 14 (citing Ex. 2001 ¶¶ 14–22)).

The prior art itself demonstrates the level of ordinary skill in the art at the time of the invention (*see Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (explaining that specific findings regarding ordinary skill level are not required “where the prior art itself reflects an appropriate level and a need for testimony is not shown”) (quoting *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 163 (Fed. Cir. 1985))).

Based on the present record including the disclosure in the '066 Patent, we adopt Petitioner's articulation of the level of ordinary skill in the art with some modifications, which is consistent with the '066 Patent and the asserted prior art, as modified by Patent Owner's assertion. In particular, we determine a POSITA would have had (i) a working knowledge of the network communications art pertinent to the '066 Patent, including network security and (ii) (a) a bachelor's degree in computer science, computer engineering, or an equivalent and two years of professional experience relating to network communications, (b) a higher relevant level of education (e.g., a Master's degree) with less professional experience or, (c) more professional experience and less education.

We apply this determination in our obviousness evaluations below.

C. Claim Construction

In interpreting the claims of the '066 patent, we “us[e] the same claim construction standard that would be used to construe the claim[s] in a civil action under 35 U.S.C. [§] 282(b)” (*see* 37 C.F.R. § 42.100(b) (2019)). The claim construction standard includes construing claims in accordance with the ordinary and customary meaning of such claims as would have been understood by one of ordinary skill in the art and the prosecution history pertaining to the patent (*see id.*; *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–14 (Fed. Cir. 2005) (*en banc*)).

“Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification” (*Phillips*, 415 F.3d at 1312). An inventor may rebut that presumption by providing a definition of the term in the specification with

reasonable clarity, deliberateness, and precision (*In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994)). In the absence of such a definition, limitations are not to be read from the specification into the claims (*In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993)).

Petitioner states that “for purposes of this proceeding and the analysis presented herein, no claim term requires express construction” (Pet. 9–10). Petitioner does identify a previous *inter partes* review of related patent U.S. 8,984,644 that previously construed certain terms, but notes that a different claim construction standard was used and that Petitioner was not a party in that *inter partes* review (*id.* at 10 n.1).

Patent Owner does not expressly include a claim construction section in its Preliminary Response (*see generally* Prelim. Resp.), but in its discussion of Petitioner’s challenges, effectively asserts a construction for the limitation reciting “instructions that . . . cause the one or more processors to . . . cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices” (*see id.* 14–28).

Patent Owner argues that this limitation should be construed to exclude “mitigation techniques [that] are caused to be utilized (applied) ‘WITHIN the . . . network defense system’” based on our Decision Denying

Institution in IPR2021-01242 (Prelim. Resp. 27, 34 (*citing* Ex. 2006,² 22)).

The claim at issue in IPR2021-01242, claim 14³, recites limitation:

code for:

automatically applying at least two of the plurality of mitigation techniques including at least one first mitigation technique of a first mitigation type and at least one second mitigation technique of a second mitigation type to the at least one device, for mitigating an effect of the attack on the at least one device that takes advantage of the at least one vulnerability;

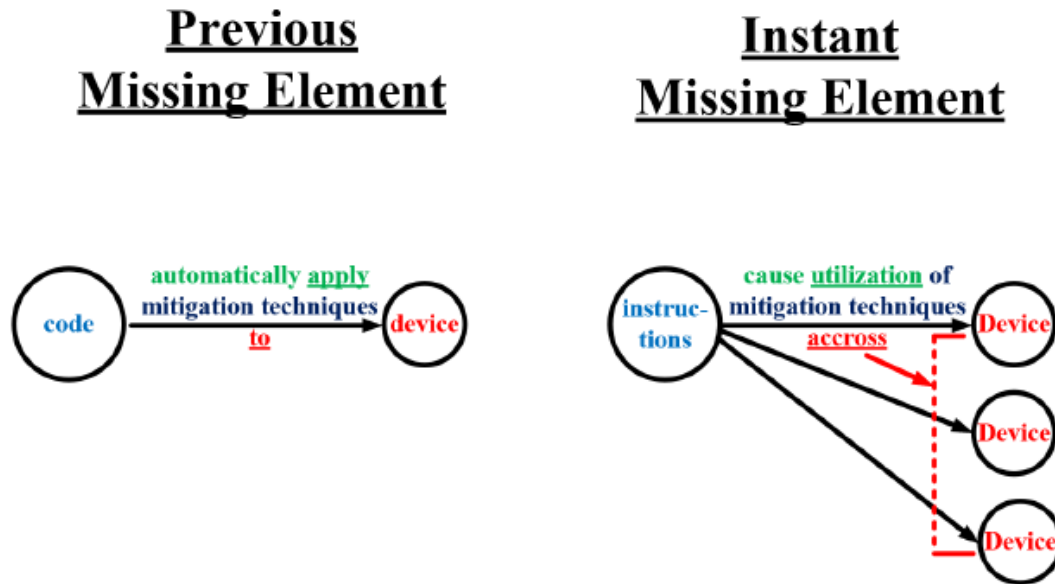
Patent Owner bases its construction argument on its assertion that “instructions that . . . cause the one or more processors to . . . cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types . . . across the plurality of devices,” as recited in the sole claim at issue here, is “nearly identical” to a limitation recited in claim 14 of the ’431 Patent, challenged in IPR2021-01242 (Prelim. Resp. 16).

Based on this assertion, Patent Owner argues the limitation in question here should be construed to exclude “mitigation techniques [which] are caused to be utilized (applied) “WITHIN [a] network defense system” (i.e. in itself)” (*id.* at 27 (*citing* Ex. 2006, 22) (emphasis omitted)). Patent Owner provides a diagram illustrating its construction of claim 14 of the

² Exhibit 2006 is our Decision Denying Institution in IPR2021-01242 (Paper 8).

³ The claim challenged in IPR2021-01242 was claim 19 which depends from claim 14 and thus, the analysis in IPR2021-01242 included analysis of claim 14 (IPR2021-01242 (Paper 8)).

'431 Patent, and claim 1 of the '066 Patent, which we reproduce below (Prelim. Resp. 20).



Patent Owner diagrams the “Previous Missing Element” directed to claim 14 of the '431 Patent including an arrow between code and device labeled “automatically apply mitigation techniques to” indicated (*id.*). Patent Owner’s depiction of the “Instant Missing Element” directed to claim 1 of the '066 Patent illustrates an arrow between Instructions and three devices labeled “cause utilization of mitigation techniques across” (*id.*).

Patent Owner asserts that the claim element before us is narrower than the element previously analyzed (Prelim. Resp. 17–20). More specifically, Patent Owner argues “[f]irst, both the Previous [and] Instant Missing Elements require software (e.g., ‘code,’ ‘instructions’) for causing multiple actions to/across at least one device” (*id.* at 17). Patent Owner next asserts that the term “utilization” recited in challenged claim 1 and the term “applying” recited in claim 14 of the '431 Patent (IPR2021-01242) are “equivalent” (*id.* at 17–18). Lastly, Patent Owner argues the term “across”

here in the '066 Patent and “to” in the '431 Patent (IPR2021-01242) are “equivalent” (*id.* at 18), and “across the plurality of devices” here is narrower than the term “to the at least one device” in the '431 Patent (IPR2021-01242) because “it requires multiple objects” (*id.* at 18–19).

Patent Owner argues the Board previously construed the recitation to exclude mitigation techniques implemented in a separate network defense system providing firewall functionality, as shown on the rightmost diagram — as opposed to mitigation techniques implemented in a device identified as the vulnerable or attacked device, as shown in the leftmost and center diagrams (*see id.* at 23–24, 26–27).

We disagree with Patent Owner’s construction. Patent Owner’s arguments ignore significant claim language of claim 1 that contradicts Patent Owner’s proposed construction, instead focusing on tying to equate broad, ordinary terms — “utilization” with “applying” and “across” with “to” (*see id.* at 16–21). In particular, Patent Owner ignores the portion of the limitation which recites “cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, *including a firewall-based occurrence mitigation type* and a other occurrence mitigation type, across the plurality of devices” (emphasis added). To aid in understanding the meaning of “a firewall-based occurrence mitigation type,” we turn to the disclosure of the '066 Patent (*see Ex. 1001*). The '066 Patent includes a detailed disclosure which contradicts Patent Owner’s argument that the limitation at issue excludes mitigation actions of a network defense system providing firewall functionality.

Initially, we note claim 1 recites “instructions that, when executed by one or more processors, cause the one or more processors to . . . cause

utilization of different occurrence mitigation actions” (Ex. 1001, 31:60–32:48). The claim does not recite where this “processor” is located.

Additionally, Figure 3 of the ’066 Patent shows computer 137 — a device targeted for an attack from connection request 211 — and shows firewall 131 as a separate networking device (Ex. 1001, 4:9–14, 4:21–24).

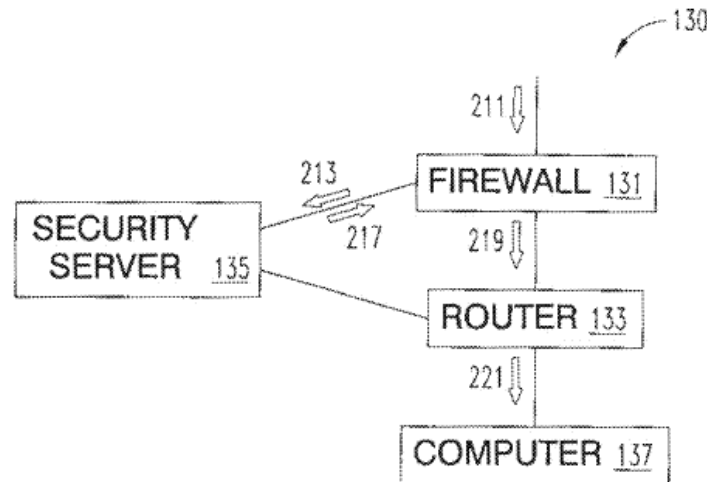


Figure 3 “trace[s] signals that travel through the system” of “a networked system of computers” (*id.* at 1:47–53). Figure 3 shows a security server 135 which sends a query to firewall 131 which then sends request 219 to router 133 which sends a request 221 to computer 137 (*id.* at 4:9–38). The ’066 Patent discloses that if computer 137 is vulnerable to an attack from connection request 211 sent to the firewall 131, “firewall 133 drops or rejects the connection request 211” to computer 137 (*id.* at 4:21–39). Thus, we determine, based on the current record, the support in the disclosure of the ’066 Patent for protecting a vulnerable or attacked device using “a firewall-based occurrence mitigation type” includes mitigation in a network defense system’s firewall functionality, which may be separate from the vulnerable or attacked device, as supported in Figures 1 and 3 and the related disclosure.

Patent Owner’s argument that we should “abide by the principle of collateral estoppel and conclude consistently” the limitation at issue here excludes mitigation techniques implemented in a separate network defense system because the limitation at issue here is “nearly-identical” to the limitation at issue in IPR2021-01242 (Prelim. Resp.21 (emphasis omitted), 1–2, 15) is unavailing. First, as discussed above, the limitations are not “nearly-identical.” Indeed, Patent Owner fails to address significant language recited by the claim at issue here while focusing on broad terms in isolation, e.g., equating the terms “utilization” with “applying” and “across” with “to” (*see id.* at 16–21).

Based on the record before us and the context of the claims and disclosure in the ’066 Patent, we are not persuaded the terms are equivalent. More specifically, although Patent Owner asserts that “the definition of ‘across’ incorporates and includes the preposition (e.g. ‘to’)” (Prelim. Resp. 18 (citing Ex. 2004)), Patent Owner ignores another applicable definition that does not use the proposition “to,” i.e., “throughout” (Ex. 2004). Even further, the claim at issue in IPR2021-01242 uniquely recites that “each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option” (Oliphant ’431, 33:65–67). Patch, policy setting, or configuration option mitigation types are described as implemented in a vulnerable or attacked device (*see id.* at 4:8–12, 5:53–56, 6:20–22), and so suggests that the mitigation types in the claim at issue in IPR2021-01242 occur in the vulnerable or attacked device. Patch, policy setting, or configuration option mitigation types, however, may be contrasted with a “firewall-based occurrence mitigation type,” which the ’066 patent discloses can be implemented in a network defense system separate from the vulnerable or attacked device (*see above*).

Even further, although Patent Owner discusses IPR2021-01242 to argue its claim construction in this *inter partes* review, we determine notably more similar claim language in IPR2017-02192 cited by Petitioner (*see* Pet. 43). As Petitioner points out (Pet. 45), claim 1 of the '066 Patent (the subject of this *inter partes* review) and claim 1 of the '644 Patent (the subject of IPR2017-02192) share claim language squarely at issue here: “utiliz[ing] different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type . . . across the plurality of devices for occurrence mitigation” (*compare* Ex. 1001, 32:48–52 *with* Oliphant '644 Patent, 31:52–57). The Final Written Decision in IPR2017-02192 construed that limitation as “selecting for use one or more actions of different types that mitigate exploitation of the vulnerability . . . *an occurrence mitigation action performed by generic firewall technology* (such as blocking an attempted connection) and/or a generic intrusion prevention system technology (such as dropping an existing connection),” in which “at least one of the devices of a plurality of devices is capable of using at least two different ‘occurrence mitigation actions’” (Paper 31, 22–23 (citing Paper 7, 15–18) (emphasis added)). Further, in IPR2017-02192, Patent Owner conceded that prior art disclosing “firewall techniques” describes “that a user may select what could be termed a ‘firewall-mitigation option’” (Paper 19, 53). Indeed, Patent Owner argued “deployment of mitigation strategies at a firewall” was a feature problematically lacking by asserted prior art (*id.* at 48). As such, the analysis of the claim in IPR2017-02192 further supports the interpretation that the limitation in question here includes a mitigation type implemented in a network defense system which provides firewall functionality and may be

separate from a vulnerable or attacked device. Our interpretation is consistent with IPR2017-02192.

Accordingly, for purposes of institution, we determine that the meaning of “instructions that . . . cause the one or more processors to . . . cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices,” as recited in claim 1, includes network defense systems which provide firewall functionality. We do not exclude those other mitigation types that may be separate from a vulnerable or attacked device.

D. Asserted Obviousness Over Willebeek-LeMair

Petitioner contends claim 1 is obvious over Willebeek-LeMair (Pet. 14–41).

1. Willebeek-LeMair (Ex. 1005)

Willebeek-LeMair is a US patent titled “Network Security System Integration,” and issued April 15, 2008 (Ex. 1005, codes (45), (54)). Willebeek-LeMair describes a unified network defense system with reference to Figure 1 of Willebeek-LeMair, reproduced below, which shows

the network defense system acting between a protected network and the wider Internet (*id.* at 4:35–8:36).

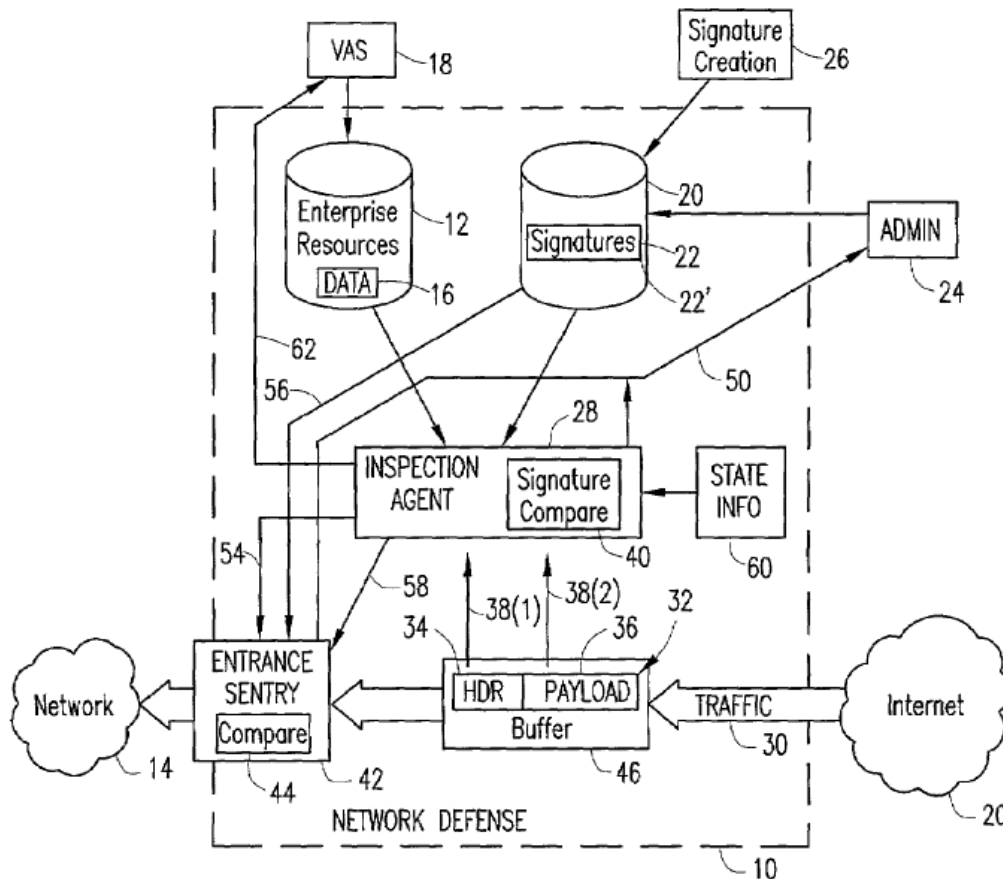


FIG. 1

As seen in Figure 1, traffic 30 from Internet 20 is intercepted en route to protected network 14 by network defense system 10, whereby traffic 30 is inspected by inspection agent 28 (*id.* at 5:37–58). Inspection agent 28 receives features 38(1), 38(2) extracted from traffic 30 (*id.* at 5:41–49). These features 38(1), 38(2) are compared to detection signatures 22 obtained from database 20 to detect a potential threat to network 14 posed by traffic 30 (*id.* at 5:50–58, 13:18–29, 14:48–52). Detection signatures 22 comprise, for example, security rules, policies and algorithms designed to mitigate or avert network damage from detected vulnerabilities (*id.* at 5:20–36, 10:53–67, 11:56–64).

When a threat is detected by inspection agent 28, a number of actions (specified by the relevant detection signature 22) may be performed by network defense system 10 (*id.* at 5:53–63, 13:25–42, 14:54–15:8). An alarm report may be issued to administrator 24 (*id.* at 5:63–65). The traffic may be blocked and discarded through a command to entrance sentry 42, which is an in-line component of network defense system 10 through which all traffic 30 must pass to network 14 (*id.* at 5:67–6:2, 6:21–39).

Detection signatures 22 may be applied by inspection agent 28 without alteration or change (*id.* at 6:5–7). Alternatively, detection signatures 22 may be tailored by inspection agent 28 and optimized to the needs and configuration of network 14 (*id.* at 6:7–15, 7:16–34). Enterprise resources database 12 contains enterprise-specific data 16 that identifies machines/hosts in the network 14, services provided by the hosts, and potential computer system and network device vulnerabilities associated with the machines and services in the network configuration (*id.* at 5:9–15). Agent 28 uses enterprise-specific data 16 from enterprise resources database 12 when instantiating detection signature 22 so that the signature minimizes the likelihood that false positive alarms will be generated (*id.* at 6:11–20).

More than one action may be undertaken when a threat has been detected, for example, an alarm may be issued and the session associated with the threatening traffic terminated (*id.* at 7:4–15).

Figure 2 of Willebeek-LeMair, reproduced below, depicts a block diagram for an architecture of network defense system 10

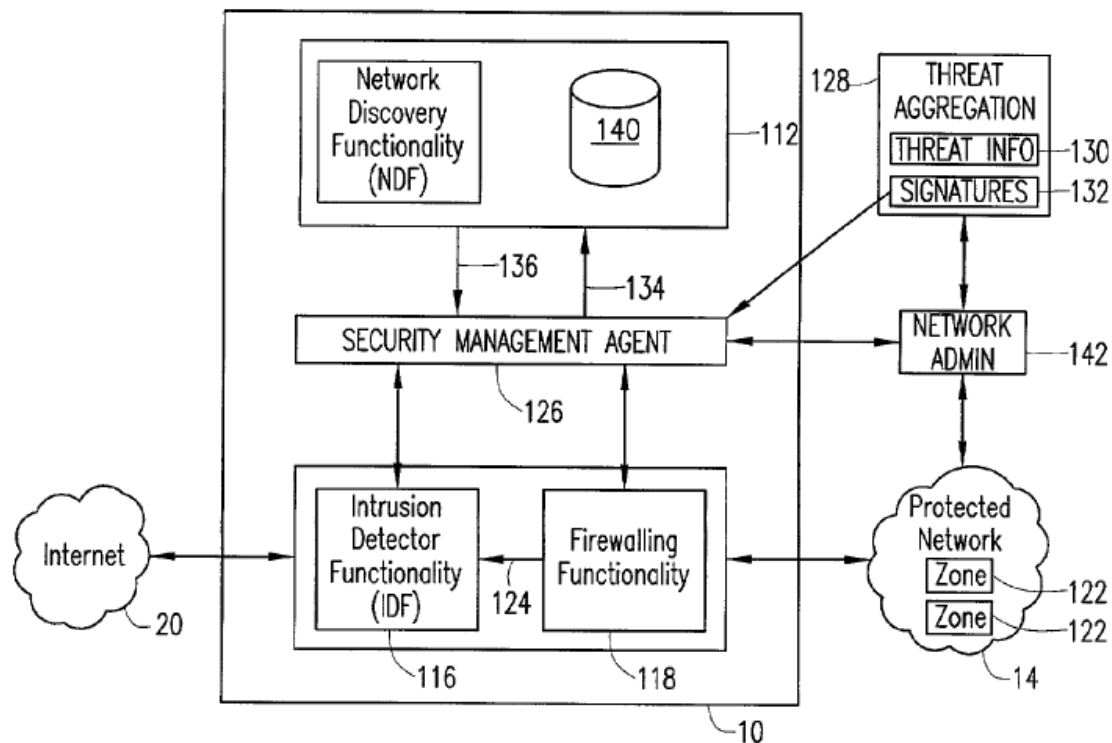


FIG. 2

As seen in Figure 2, network defense system 10 may include “intrusion detector functionality (IDF) 116 that continuously analyzes network traffic to identify content that is potentially harmful to the network 14” (*id.* at 8:54–62). Network defense system 10 may also include in-line firewalling functionality 118 that inspects traffic and makes decisions concerning accepting, denying, or tapping the traffic (*id.* at 8:63–9:14, 9:21–35). Detection signatures are instantiated to intrusion detector functionality 116 and firewalling functionality 118, tailored to perceived threats to the network and including a set of criteria to compare to traffic, and response instructions to follow if a match is detected (*id.* at 9:36–56, 14:54–15:8). Security management agent 126 configures, tunes, and monitors operation of intrusion detector functionality 116 and firewalling

functionality 118, “specifying what they should be on the look out for and what should be done when it is detected” (*id.* at 9:36–45). Security management agent 126, in network defense system 10, “instantiates detection signatures to the intrusion detector functionality 116 and the firewalling functionality 118 tailored to a certain perceived threat to the network 14” (*id.* at 9:45–48; *see id.* at 14:54–15:8). This occurs in an automated manner when security management agent 126 responds to continuing assessments of the network 14 by network discovery functionality 112 (*id.* at 9:57–10:19).

In summary, the agent 126 operates to assess changes to the network 14 detected by the network discovery functionality 112, confirm their validity, and inform the intrusion detector functionality 116 to tune its operation so that false alerts are not generated when the new, but nonetheless valid, information types are encountered in the network traffic content. Additionally, the agent 126 can . . . adapt the firewalling functionality 118 to block access to the network 14 from another network that could be trying to exploit a scanning functionality 112 recognized vulnerability. . . [T]he threat detection (IDF) and threat suppression (fire walling) capabilities of the system 10 are continually being optimized . . . in response to continuous threat assessment ([network discovery functionality]) analysis (*id.* at 10:20–35).

Furthermore, “threatened portions of the network” are protected using a tailored action set “so that the actions taken responsive to the detection of the attack are appropriate” (*id.* at 12:33–37). “The agent 126 may establish a block action to be taken by the firewalling functionality 118 to block the attack-related traffic, and a terminate action to be taken by the intrusion detector functionality 116 to terminate any session associated with a possible attack” (*id.* at 12:39–43).

2. Independent Claim 1

Petitioner contends claim 1 is obvious over Willebeek-LeMair (Pet. 14–41).

a) “utilization of . . . mitigation actions”

Petitioner contends Willebeek-LeMair teaches cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices, as recited in claim 1 (Pet. 37–40; Ex. 1005, 17:31–62). In particular, Petitioner asserts that Willebeek-LeMair’s “‘block’ action ‘taken by the firewalling functionality 118’ is an example of ‘a *firewall-based occurrence mitigation type*’” and that its “‘terminate action (to terminate the session) ‘taken by the intrusion detector functionality 116’ is an example of ‘a other occurrence mitigation type’” (Pet. 37–38 (citing Ex. 1005, 12:28–43; Ex. 1003 ¶¶ 95)). Petitioner argues that, as such, Willebeek-LeMair “teaches causing several different actions to occur in response to detecting a threat in traffic” (*id.* at 38 (citing Ex. 1003 ¶ 97)). Further, Petitioner asserts that Willebeek-LeMair’s intrusion detector functionality 116 and firewalling functionality 118, i.e., the block and terminate actions, are “located at the network edge” via an “in-line” component and, so, “any mitigation actions apply ‘*across a plurality of devices*’” (*id.* at 38–39 (citing Ex. 1005, 6:26–29, 9:27–31; Ex. 1003 ¶ 98)).

Patent Owner contends Petitioner fails to show Willebeek-LeMair teaches “utilization of . . . mitigation actions . . . across the plurality of

devices” (Prelim. Resp. 14–28). In particular, Patent Owner asserts that Willebeek-LeMair’s “system applies ‘different ... mitigation actions’ (techniques) in itself, and not ‘across [i.e. to] the plurality of devices,’ as claimed” (*id.* at 25 (emphasis omitted)). That is, Patent Owner argues that because Willebeek-LeMair’s block and terminate actions “are ‘located’ and ‘applied’ ‘at network edge,’” those actions are not “across the plurality of devices” (*id.* at 27).

Willebeek-LeMair teaches, as shown in Figure 4, step 310, “the intrusion functionality 116 detects . . . an attempt from outside the network 14 to exploit [a] noted vulnerability (for example, a certain IP address is noted as being a source of traffic relating to the IIS buffer overflow vulnerability as detected by the code red signature)” (Ex. 1005, 14:59–64; *see* Pet. 37). Willebeek-LeMair further teaches, in step 312, “[t]his is reported back to the agent 126” which “responds in step 314 by reporting . . . that an attempt to exploit has occurred” (Ex. 1005 14:64–67; *see* Pet. 37). Willebeek-LeMair discloses the agent 126 additionally “instructs the firewalling functionality 118 in step 316 to drop the packet traffic relating to the attempted exploitation” and “in step 318 instruct[s] the firewall to block all traffic originating from the noted IP address of the attacker” (Ex. 1005 14:67–15:6, 1:7–10; *see* Pet. 37).

Thus, because Willebeek-LeMair discloses a firewalling functionality, at this juncture, we determine Willebeek-LeMair teaches the recited “firewall-based occurrence mitigation type.” Additionally, because Willebeek-LeMair discloses instructing the firewall to block all traffic from the attacker (an occurrence mitigation action), based on the record before us, we determine Willebeek-LeMair teaches the recited “firewall-based occurrence mitigation type,” as recited in claim 1.

Willebeek-LeMair further teaches, intrusion detector functionality, and specifically, “a terminate action [] taken by the intrusion detector functionality 116 to terminate any session associated with a possible attack” (Ex. 1005, 12:40–43; *see* Pet. 38). Willebeek-LeMair also teaches the intrusion detector functionality generates alerts from its analysis of the network traffic content (Ex. 1005, 9:34–27, 1:7–10; *see* Pet. 38). Based on the record before us, we determine this intrusion detector functionality is an occurrence mitigation action that is different than the firewall-based occurrence mitigation type. Accordingly, based on the record before us, we determine Willebeek-LeMair teaches the recited “a other occurrence mitigation type,” as recited in claim 1. In combination of these two functionalities, we determine on the current record, Willebeek-LeMair teaches the recited “cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-base occurrence mitigation type and a other occurrence mitigation type” (*see* Pet. 38 (citing Ex. 1003 ¶ 97)).

Willebeek-LeMair additionally teaches a “defense system” that includes the intrusion detector functionality and a firewalling functionality to automate threat detection and threat response (Ex. 1005, 3:22–29, 4:65–5:2; *see* Pet. 12). As shown in Figure 1, Willebeek-LeMair teaches the defense system 10 is positioned between the Internet 20⁴ and the Network 14 (Ex. 1005, Figs. 1–2). As noted by Petitioner (Pet. 38), Willebeek-LeMair describes the defense system 10 is located at the network edge. In particular, Willebeek-LeMair discloses “[r]esponsive to [] alerts [generated by the

⁴ We note two different elements are labeled with the numeral “20” in Figure 1: signature database 20 and Internet 20 (Ex. 1005, 5:20, Fig. 1).

intrusion detector functionality,] the firewalling functionality . . . stops malicious traffic at the edge of the network 14 before it can enter, infect and debilitate the network systems” (Ex. 1005, 9:27–31; *see* Pet. 39).

Willebeek-LeMair additionally describes the defense “system 10 further includes a gatekeeping functionality performed by an entrance sentry 42 . . . [,] an in-line component of the system (*id.* at 6:24–27, Fig. 1; *see also* Fig. 2 (element 126); *see* Pet. 39). “[I]n-line” as described by Willebeek-LeMair, means “all traffic 30 must pass through entrance sentry 42 before entering the protected network” (Ex. 1005, 6:27–29, Fig. 1; *see also* Fig. 2 (element 126); *see* Pet. 39). Willebeek-LeMair describes that “the elements of the protected network 14 may include: a router; special server types . . . ; an intranet; personal computers; and network zones” (Ex. 1005, 15:59–63). Thus, on the record before us, we determine Willebeek-LeMair discloses a plurality of devices in the protected network 14. Because Willebeek-LeMair teaches the defense system, positioned between the internet and the network, causes utilization of different occurrence mitigations actions and the different occurrence mitigation actions and the network includes a plurality of devices, based on the current record, we determine this teaching of Willebeek-LeMair discloses the recited “cause utilization of different occurrence mitigation actions . . . across the plurality of devices for occurrence mitigation,” as recited in claim 1.

Moreover, Willebeek-LeMair further discloses “the firewalling functionality 118 may be independently tuned to provide threat protection on a zone-by-zone basis” (Ex. 1005, 9:8–14, Fig. 2; Pet. 39). Willebeek-LeMair describes

[t]he tuning operation that is performed by the agent 126 further occurs in a manner that is optimized to the network 14 being

protected. To that end, the agent 126 confers with the network discovery functionality 112 to ensure that the detection signatures supplied to the intrusion detector functionality 116 and firewalling functionality 118 are tailored to the collected enterprise (i.e., network 14) specific data. More specifically, the enterprise specific data is considered by the agent when issuing a detection signature so that the signature (either through its criteria or its response instructions) is designed in a way that minimizes the likelihood that false positive alarms will be generated. This cooperative defense effort between the network discovery functionality 112, intrusion detector functionality 116 and firewalling functionality 118, through the agent 126 tailoring the detection signatures based on enterprise specific data, effectuates a self-hardening system 10

(Ex. 1005, 10:3–19; *see* Pet. 39–40). Willebeek-LeMair additionally describes in Figure 4, step 300, “the network discovery functionality 112 scans the network 14 and discovers a certain vulnerability relating to a web server in the network [which] is reported to the agent 126 in step 302” (Ex. 1005, 14:48–52; *see* Pet. 37). Thus, based on the record before us, we determine Willebeek-LeMair teaches actions being taken based on detection signatures supplied that are tailored “based on enterprise specific data” (Ex. 1005, 10:3–19; *see* Pet. 39–40). Accordingly, we determine at this juncture, Willebeek-LeMair teaches preventing advantage being taken of vulnerabilities. Because Willebeek-LeMair describes “the enterprise specific data is considered . . . [to] minimize[] the likelihood that false positive alarms will be generated,” based on the record before us, we determine Willebeek-LeMair is determining actual vulnerabilities. On the record before us, we determine Willebeek-LeMair teaches identifying the vulnerabilities and taking steps to “prevent[] advantage being taken of actual vulnerabilities,” as recited in claim 1.

Willebeek-LeMair teaches a detection signature 132, associated with a discovered vulnerability, is activated in the intrusion detector functionality 116 which detects attempts from outside the network 14 to exploit the noted vulnerability (Ex. 1005, 14:54–61; *see* Pet. 37). “The detection signature 132 specifies block and terminate actions to be taken. In implementing these actions, the agent 126 may establish a block action to be taken by the firewalling functionality 118 to block the attack-related traffic, and a terminate action to be taken by the intrusion detector functionality 116 to terminate any session associated with a possible attack” (Ex. 1005, 12:34–43; *see* Pet. 38).

Thus, on the record before us, we determine Willebeek-LeMair teaches difference occurrence mitigation actions — blocking all traffic or dropping the packet traffic — and diverse occurrence mitigation types — intrusion detector functionality and firewalling functionality. Therefore, on this record, we determine Willebeek-LeMair teaches “difference occurrence mitigation actions of the diverse occurrence mitigation types.”

Accordingly, on the current record, we are persuaded Petitioner has made a sufficient showing that Willebeek-LeMair teaches

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices,

as recited in claim 1 (Ex. 1005, 17:31–62).

b) Remaining Limitations

Petitioner relies on Willebeek-LeMair to teach

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to (Pet. 14–16 (citing Ex. 1005, 16:1–5, 16:11–19, Figs. 1–2, 6; Ex. 1003 ¶¶ 37–42; Ex. 1018, Abstract, 4:20–43)):

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities (Pet. 16–28 (citing Ex. 1005, 5:20–36, 5:50–53, 6:5–7, 6:54–58, 8:7–11, 9:37–48, 10:9–14, 10:36–46, 11:1–29, 13:8–11, 13:27–35, 16:2–5, Figs. 1, 2, 6; Ex. 1003 ¶¶ 43–47, 52–63));

said first vulnerability information generated utilizing the second vulnerability information, by (Pet. 28 (citing Ex. 1003 ¶ 63)):

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device (Pet. 28–32 (Ex. 1005, 5:15–24, 8:54–58, 10:3–19, 12:9–33, 12:44–13:7, Figs. 1–2; Ex. 1003 ¶¶ 64–74)), and

determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities (Pet. 32–34 (citing Ex. 1001, 46:5–6; Ex. 1005, 8:54–58, 8:66–9:3, 10:3–19, 10:40–42, 11:12–29, 12:15–33, 12:44–13:17, 15:24–26; Ex. 1003 ¶¶ 75–81));

identify an occurrence in connection with at least one of the plurality of devices (Pet. 34–37 (citing Ex. 1005, 3:41–49, 5:37–41; Ex. 1003 ¶¶ 82–86));

determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first

vulnerability information (Pet. 35–37 (citing Ex. 1005, 5:39–41, 5:50–63, 8:54–58, 10:3–19, 13:30–39; Ex. 1003 ¶¶ 87–92)) and

wherein the at least one configuration involves at least one operating system (Pet. 40–41 (citing Ex. 1005, 12:44–61; Ex. 1003 ¶¶ 105–107)).

Patent Owner does not offer any arguments specific to these claim limitations, for consideration (*see generally* Prelim. Resp.). Upon review of the recitations and relied-upon teachings, we are persuaded, based on the record before us, that Petitioner has made a sufficient showing that Willebeek-LeMair teaches the remaining limitations recited in claim 1.

3. Conclusion

Based on the record before us, we determine Petitioner’s offered arguments, evidence, and supporting testimony establish a reasonable likelihood that Petitioner would prevail in showing that Willebeek-LeMair teaches the recited invention of claim 1.

E. Asserted Obviousness over Gupta and Graham

Petitioner contends claim 1 is obvious over Gupta and Graham (Pet. 41–59).

1. Gupta

Gupta is a US patent application publication titled “Hierarchy-Based Method and Apparatus for Detecting Attacks on a Computer System,” and published January 2, 2003 (Ex. 1006, codes (43), (54)). Gupta describes “provisioning a computer against computer attacks” by “constructing a hierarchy characterizing different computer attacks and counter measures, and traversing this hierarchy to identify computer attacks and counter measures relevant to a target platform” (*id.* ¶ 8, Abstract). Gupta explains that its system provides “security operations” via network security sensors

22 in a “computer network 20 incorporating network security devices and processes associated with the invention” (*id.* ¶ 30; *see id.* Fig. 1). Network security sensors include a “memory 50, which includes primary and/or secondary memory” and “memory 50 stores a set of executable programs utilized to implement functions of the invention” (*id.* ¶¶ 36–37; *see id.* Fig. 2). Further, “memory 50 also stores a classification and pattern-matching module 68” which “has an associated set of intrusion signatures 70” (*id.* ¶ 42) and those intrusion signatures 70 are stored in an “attack file” which “specifies attacks and counter measures” (*id.* ¶ 151). For example, in one embodiment, a hierarchical attack categorization module 150

initially constructs a hierarchy characterizing different computer attacks and countermeasures (block 160) . . . The hierarchy is then traversed to identify computer attacks and countermeasures relevant to the target platform (block 162). Detection and protection measures for the target platform are then collected (block 164). This can result in an attack file 149. A sensor is then supplied, through a download, with the protective software (e.g., the attack file) for the target platform (block 166).

(*id.* ¶ 164; *see id.* fig. 17).

To detect an attack, a “signature processing system . . . look[s] for signatures that are specific combinations of patterns (e.g., numerical field values, string matches, and the like) existing in monitored network traffic” (*id.* ¶ 83). When an attack is found, “response processor 54 . . . attempts to prevent the attack. Short-term responses include terminating TCP connections. Long-term responses include packet logging for further analysis to improve detection and response” (*id.* ¶ 87).

2. *Graham*

Graham is a US Patent titled “System and Method for Preventing Network Misuse,” and issued June 26, 2007 (Ex. 1007, codes (45), (54)). Graham explains that its system is designed for “analyzing and preventing unauthorized use of data network resources” by “evaluat[ing] potential network misuse signatures” to make a “misuse determination” (*id.* at 1:7–10, 2:51–56). For example, “several successive transmissions of an invalid user ID or password from a suspect node to a target may indicate that an unauthorized user is attempting to gain access to [a] target” (*id.* at 4:40–43). If Graham’s system “determines that the target is vulnerable” to potential misuse, the system “may take certain precautionary measures . . . For example, at this stage the system may attempt to block incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so)” (*id.* at 7:61–67; *see id.* at 7:48–57).

3. *Independent Claim 1*

Petitioner contends claim 1 is obvious over Gupta and Graham (Pet. 41–59).

a) “*utilization of . . . mitigation actions*”

Petitioner contends the combination of Gupta and Graham teaches cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices,

as recited in claim 1 (Pet. 56–58 (citing Ex. 1006 ¶¶ 87, 136, 143, 160; Ex. 1007, 7:58–67; Ex. 1003 ¶¶ 157–161); Ex. 1001, 31:60–32:48)).

In particular, Petitioner asserts that “Gupta discloses providing one or more options to selectively utilize different occurrence mitigation actions, including terminating TCP connections, which a POSITA would understand to be an intrusion prevention system-based occurrence mitigation technique as recited in this claim (*id.* at 57 (citing Ex. 1006 ¶ 87; Ex. 1003 ¶¶ 158–159)). Petitioner further asserts that “Graham also discloses providing occurrence mitigation actions, including disclosing the user of techniques known in the art, including firewall techniques,” and, in particular “block[ing] incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so)” (*id.* at 57–58 (citing Ex. 1007, 7:58–67)). Based on Gupta and Graham’s disclosures, Petitioner argues that “the combined teachings of Gupta and Graham disclose this limitation” (*id.* at 58).

Patent Owner contends “neither Gupta nor Graham even suggest ‘instructions that . . . cause the one or more processors to . . . cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types . . . across the plurality of devices,’ in the specific context claimed” (Prelim. Resp. 28–35 (emphasis omitted)). In particular, Patent Owner argues that Gupta “providing ‘the ability to select...actions’ does not rise to the level of specificity embodied in the claimed instructions to cause utilization of such actions ‘across the plurality of devices,’ in the specific context claimed” (*id.* at 31–32).

Additionally, Patent Owner argues that Gupta’s “actions are simply caused to be utilized by the response processor 54 which is part of the memory where the instructions are stored (and not across (to) the plurality of

devices)” (*id.* at 32). Similarly, Patent Owner argues that “Graham, like Gupta[,] . . . fails to meet the claims, since each merely discloses ‘in-line’ system instructions to cause utilization of actions in itself (the ‘in-line’ system), contrary to what is claimed” (*id.* at 34).

Gupta teaches

[t]he response processor 54 responds to AIDs [(AttackID) 26]. The response processor 54 generates alerts that provide notification of an attack. The response processor 54 also attempts to prevent the attack. Short-term responses include terminating TCP connections. Long-term responses include packet logging for further analysis to improve detection and response.

(Ex. 1006 ¶ 87; *see* Pet. 57). On the record before us, we determine Gupta teaches occurrence mitigation techniques — the attempts to prevent the attack, including short-term responses and long-term responses.

Gupta describes a subscriber is able to manage and monitor the virtual intrusion detection system (VIDS) provisioning module 110 (Ex. 1006 ¶¶ 131, 143; *see* Pet. 56). In particular, Gupta teaches

[t]he VIDS provisioning module 130 facilitates protection for multiple traffic streams for different subscribers using a Single Sensor platform while maintaining Security separation. The module 130 supports different security policies, protection objectives, and Security management preferences effectively and efficiently.

(Ex. 1006 ¶ 136; *see* Pet. 56–57).

At this juncture, we determine Gupta discloses “utilization of occurrence mitigation actions.” We determine, because Gupta utilizes these security polices such as alerts or terminating TCP connections to prevent attacks (through use of AIDs responses), on this record, Gupta further teaches utilizing the occurrence mitigation to “prevent[] advantage being taken of actual vulnerabilities utilizing the difference occurrence mitigation

actions of the diverse occurrence mitigation types.” Gupta also describes the occurrence mitigation actions are facilitated by the VIDS provisioning module that “facilitates protection for multiple traffic streams for different subscribers” (Ex. 1006 ¶ 136; *see* Pet. 56–57). We determine, at this juncture, Gupta teaches the different subscribers teach the “plurality of devices.” Additionally, in light of our discussion regarding “across the plurality of devices” *supra* and, because the mitigation actions are facilitated by the VIDS provisioning module, on the record before us, we determine Gupta teaches “utilization of . . . occurrence mitigation actions . . . across the plurality of devices,” as recited in claim 1.

Graham teaches providing different occurrence mitigation actions:

If the system determines that the target is not vulnerable, one embodiment of the system generates a low-level alert and/or simply logs the event signature (or may take no action whatsoever, depending on the configuration). If the system determines that the target is vulnerable, however, then one embodiment will generate an alert condition (or increase a preexisting alert level) and/or may take certain precautionary measures (at 235)

(Ex. 1007, 7:58–65; *see* Pet. 57–58). Graham provides an example — “the system may attempt to block incoming data transmissions form the suspect node (e.g., by commanding the firewall to do so)” (Ex. 1007, 7:65–67; *see* Pet. 58). Graham continues that a factor considered by the system is “the target’s response to the detected data signature to further evaluate the probability of network misuse” (*id.* at 8:3–5). Thus, we determine, at this juncture, Graham teaches occurrence mitigation actions, one of which is a firewall-based occurrence mitigation type — the firewall blocking incoming data transmission from a suspect node (*id.* at 7:65–67; *see* Pet. 58).

Thus, we determine, based on the current record, Gupta teaches “a other occurrence mitigation type” and Graham teaches “a firewall-based occurrence mitigation type.” Moreover, on this record, we determine both Gupta and Graham teach “caus[ing] utilization” of different occurrence mitigation actions.

Based on the record before us, we further determine, in combination, Gupta and Graham teach “cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type,” as recited in claim 1. Moreover, we are persuaded, on the record before us, Petitioner has made a sufficient showing that the combination of Gupta and Graham teaches

cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices,

as recited in claim 1 (Ex, 1001, 31:60–32:48). In addition, Petitioner provides articulated reasoning with some rational underpinning to support the combination of Gupta and Graham (Pet. 58).

b) Remaining Limitations

Petitioner relies on Gupta to teach

A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to (Pet. 47 (citing Ex. 1006 ¶¶ 30, 36–37, 130, Fig. 2; Ex. 1003 ¶¶ 17–21, 122–124)):

receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities (Pet. 48–50 (citing Ex. 1006 ¶¶ 151, 154, 164–165; Ex. 1003 ¶¶ 125–132));

said first vulnerability information generated utilizing the second vulnerability information, by (Pet. 51 (citing Ex. 1003 ¶ 133));

identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device (Pet. 51–52 (citing Ex. 1006 ¶¶ 32, 57, 68, 160, 164–165; Ex. 1003 ¶¶ 134–140)), and

determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities (Pet. 52–53 (citing Ex. 1006 ¶¶ 154, 164; Ex. 1003 ¶¶ 141–144));

identify an occurrence in connection with at least one of the plurality of devices (Pet. 53–54 (citing Ex. 1006 ¶¶ 31, 83; Ex. 1003 ¶¶ 146–150));

determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information (Pet. 54–56 (citing Ex. 1006 ¶¶ 83, 86, 154, 164–166; Ex. 1003 ¶¶ 151–156)); and

wherein the at least one configuration involves at least one operating system (Pet. 58–59 (citing Ex. 1006 ¶ 160; Ex. 1003 ¶¶ 162–164)).

Patent Owner does not offer any arguments specific to these limitations (*see generally* Prelim. Resp.). Upon our review of Petitioner’s asserted contentions, we are persuaded based on the record before us, Petitioner has made a sufficient showing that the combination of Gupta and

Graham teaches the limitations as recited in claim 1. In addition, Petitioner provides articulated reasoning with some rational underpinning to support the combination of Gupta and Graham (Pet. 42–43 (citing Ex. 1006 ¶¶ 151, 154, 164–165; Ex. 1007, 1:7–10, 7:58–67; Ex. 1003 ¶¶ 113–116), 58).

4. Conclusion

Based on the record before us, we determine Petitioner’s arguments, evidence, and supporting testimony establish a reasonable likelihood that Petitioner would prevail in showing that the combination of Gupta and Graham teaches the recited invention of claim 1.

III. CONCLUSION

For the foregoing reasons, on the record before us, we are persuaded that the Petition establishes a reasonable likelihood that Petitioner would prevail in showing that claim 1 of the ’066 Patent is unpatentable.

IV. ORDER

For the reasons given, it is:

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* is *instituted* on all the sole challenged claim with respect to all grounds set forth in the Petition; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(a), *inter partes* review of the ’066 Patent is instituted commencing on the entry date of this Order, and pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is given of the institution of a trial.

IPR2022-00035
Patent 10,893,066 B1

FOR PETITIONER:

Theodore Faster
David McCombs
Adam Fowles
Clint Wilkins
HAYNES AND BOONE, LLP
Ipr.theo.foster@haynesboone.com
David.mccombs.ipr@haynesboone.com
Adam.fowles.ipr@haynesboone.com
Clint.wilkins.ipr@haynesboone.com

FOR PATENT OWNER:

George Gordon
ANDREW GORDON LAW FIRM PLLC
andrew@agordonlawfirm.com