

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

SECURITYPROFILING, LLC,
Patent Owner.

IPR2021-01242
Patent 9,100,431 B2

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

FENICK, *Administrative Patent Judge*.

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

I. INTRODUCTION

Cisco Systems, Inc. (“Petitioner”) filed a Petition (Paper 2, “Pet.”) requesting *inter partes* review of claims 1, 2, 4–12, and 14–20 of U.S. Patent No. 9,100,431 B2. Ex. 1001 (“the ’431 patent”). After the Petition was filed, SecurityProfiling, LLC (“Patent Owner”) filed a Statutory Disclaimer of claims 1, 2, 4–12, and 14–18. *See* Ex. 2002. Thus, claims 19 and 20

(“remaining challenged claims”) are the only challenged claims that remain for our consideration.¹ Patent Owner also filed a Preliminary Response opposing institution of review as to the remaining challenged claims 19 and 20. Paper 6 (“Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2021). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted “unless the Director determines . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.”

For the reasons that follow, we do not institute an *inter partes* review.

II. BACKGROUND

A. *Real Parties in Interest*

Petitioner identifies only itself as a real party in interest. Pet. 83. Patent Owner identifies only itself as a real party in interest. Paper 5 (Patent Owner’s Mandatory Notices), 2.

¹ See *Guinn v. Kopf*, 96 F.3d 1419, 1422 (Fed. Cir. 1996) (“A statutory disclaimer under 35 U.S.C. § 253 has the effect of canceling the claims from the patent and the patent is viewed as though the disclaimed claims had never existed in the patent.”); 37 C.F.R. § 42.107(e) (“The patent owner may file a statutory disclaimer under 35 U.S.C. [§] 253(a) in compliance with § 1.321(a) of this chapter, disclaiming one or more claims in the patent. No *inter partes* review will be instituted based on disclaimed claims.”); Patent Trial and Appeal Board, Consolidated Trial Practice Guide, at 52 (Nov. 2019) (“[A] patent owner may file a statutory disclaimer of one or more challenged claims to streamline the proceedings Where one or more challenged claims remain, the Board’s decision on institution would be based solely on the remaining claims.”).

B. Related Matters

Petitioner identifies two pending district court cases involving the '431 patent: *SecurityProfiling, LLC v. Cisco Systems, Inc.*, 6-21-cv00337 (W.D. Tx.); and *SecurityProfiling, LLC v. Trend Micro Incorporated*, 6-21-cv00330 (W.D. Tx.). Pet. 83. Patent Owner, in its Mandatory Notices filed October 25, 2021, identifies these cases as related as well, but notes that they are no longer pending. Paper 5, 2. In its Updated Mandatory Notices, filed October 26, 2021, Patent Owner identifies two cases filed on October 25, 2021 as related: *SecurityProfiling, LLC v. Cisco Systems, Inc.*, 6-21-cv-01106 (W.D. Tx.) and *SecurityProfiling, LLC v. Trend Micro Incorporated*, 6-21-cv-01105, (W.D. Tx.). Paper 7, 1.

Petitioner and Patent Owner both identify three other district court cases as related but no longer pending: *SecurityProfiling LLC v. Trend Micro America Inc.*, 3-17-cv-01484 (N.D. Tx.); *SecurityProfiling, LLC v. Trend Micro America, Inc.*, 6-16-cv-01165 (E.D. Tx.); *SecurityProfiling, LLC v. Intel Corporation*, 6-16-cv-01016 (E.D. Tx.). Pet. 83; Paper 5, 2.

Patent Owner additionally notes that a related patent, U.S. Patent No. 10,609,063, is the subject of a petition for *inter partes* review, IPR2021-01428. Paper 5, 2.

C. The '431 Patent

The '431 patent is titled "Computer Program Product and Apparatus for Multi-Path Remediation" and generally relates to management of security of computing devices. Ex. 1001, codes (54), (57), 1:18–20. The '431 patent describes the invention, in one embodiment, in relation to a

system including a networked system of computers, depicted in Figure 1, reproduced below. *Id.* at 1:39–40.

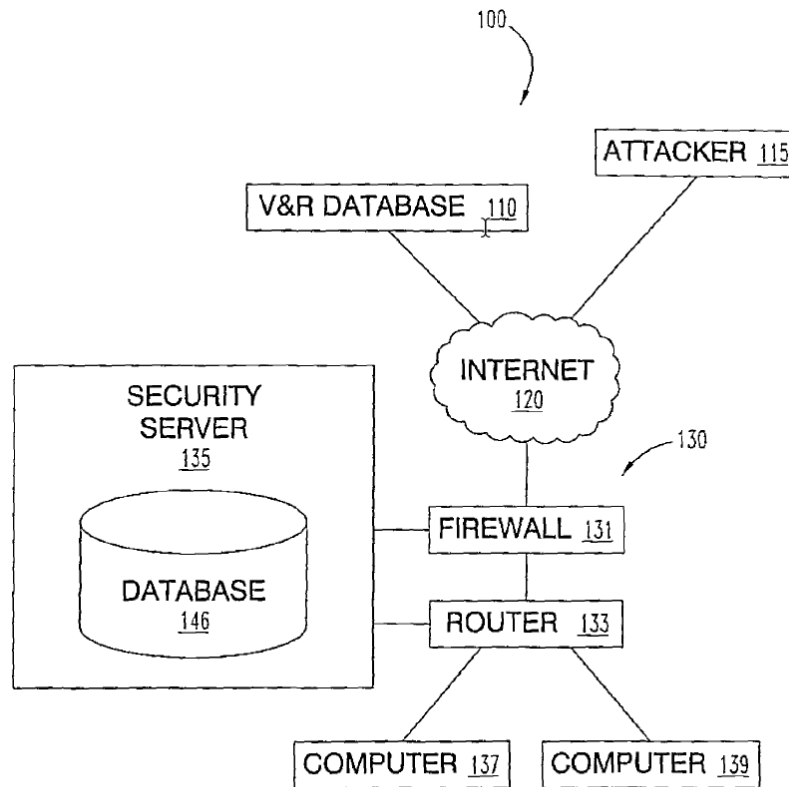


Fig. 1

As shown in Figure 1, subnet 130 is connected to the Internet 120 via included firewall 131, which serves as the gateway between the Internet 120 and the rest of subnet 130. *Id.* at 2:20–24. Router 133 directs connections between computer 137 and other computers in the subnet 130 and those connected via the Internet 120. *Id.* at 2:24–26.

Also in subnet 130 is security server 135, which 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 2:26–28, 2:32–35, 2:50–3:10, 3:17–23. 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 2:36–42.

Security server 135 determines, from a request received by firewall 131 via the Internet, directed to computer 137, whether that request is attempting to take advantage of a particular known vulnerability on that exists on computer 137. *Id.* at 3:60–4:12. Security server 135 uses information from database 146 to determine whether computer 137 has vulnerable software installed, whether the vulnerability has been patched, or whether computer 137 has been configured so as to be invulnerable to a particular attack. *Id.* Security server 135 sends a result signal back to firewall 131 with an indication as to whether the connection request should be granted or rejected. *Id.* at 4:13–21. Analogous operation allows computers within subnet 130 to protection from compromised devices within the subnet as well, with router 133 querying security server 135 before allowing one computer within subnet 130 to connect with another computer within the subnet. *Id.* at 4:22–40.

“[U]pon 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 4:41–47. The remediation technique may be applied only to the machine that was attacked, to all devices subject to the same vulnerability, or to all devices to which the remediation technique may be applied. *Id.* at 4:47–53.

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 4:54–58.

D. Illustrative Claims

Claim 19 depends from claim 14. Therefore we reproduce claim 14 here, along challenged claim 19. Bracketed claim numbering is added to correspond with the bracketing added by Petitioner and used by the parties.

14. A computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:

[14.1] code for:

accessing at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where:

[14.2] each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

[14.3] each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

[14.4] code for:

receiving information in connection with at least one of a plurality of devices; and

[14.5] identifying an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information;

[14.6] 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;

[14.7] wherein the computer program product is operable such that the effect of the attack is mitigated by preventing the attack from taking advantage of the at least one vulnerability;

[14.8] wherein the computer program product is operable such that one or more of the plurality of mitigation techniques is identified based on an identification of an operating system.

19. The computer program product of claim 14, wherein the computer program product is operable such that the at least one first mitigation technique of the first mitigation type and the at least one second mitigation technique of the second mitigation type utilize different underlying security technology types that are both supported by a same system component that is capable of identifying the attack and preventing the attack from taking advantage of the at least one vulnerability after the at least two mitigation techniques are automatically applied.

E. Prior Art and Asserted Grounds

Petitioner asserts that remaining challenged claims 19 and 20 would have been unpatentable on the following grounds:

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
19, 20	103	Willebeek-LeMair ²

With respect to the statutes to be applied, the Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), amended 35 U.S.C. §§ 102 and 103 for applications filed on or after March 16, 2013. Petitioner, citing the ’431 patent’s priority claim to a provisional application filed in 2003, argues that the pre-AIA version of the statutes apply in this case, but that Willebeek-LeMair would qualify as prior art under either pre- or post-AIA versions of 35 U.S.C. §§ 103. Pet. 10, 12 &

² Willebeek-LeMair et al., U.S. Patent 7,359,962 B2, iss. Apr. 15, 2008.

n.2; see Ex. 1001, code (60). Patent Owner does not comment on this issue. See Prelim. Resp.

Because the '431 patent was filed as a continuation-in-part application after March 16, 2013, any determination of which version of §§ 102 and 103 applies hinges on a determination of whether the application contains or contained at any time a claim to a claimed invention having an effective filing date on or after March 16, 2013. Ex. 1001, code (63); see MPEP 2159.02. As it appears on the present record that Willebeek-LeMair would be prior art under either the pre- or post-AIA versions of 35 U.S.C. §§ 102 and 103, and as we do not institute even considering Willebeek-LeMair as prior art, we do not make a determination as to whether pre- or post-AIA versions apply.

III. ANALYSIS

A. *Legal Standards*

“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 challenge to each claim”)). This burden never shifts to Patent Owner. See *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review).

Furthermore, Petitioner must explain with particularity how the prior art would have rendered the challenged claims unpatentable. 35 U.S.C.

§ 312(a)(3); 37 C.F.R. § 42.104 (“The petition must specify where each element of the claim is found in the prior art patents or printed publications relied upon.”).

A claim is unpatentable under 35 U.S.C. § 103 if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which said subject matter pertains. *See 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 skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

B. Level of Ordinary Skill in the Art

Relying on the testimony of its expert, Dr. A.L. Narasimha Reddy, Petitioner contends that, as of July 2003, a person of ordinary skill in the art “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” and that “[l]ack of professional experience can be remedied by additional education, and vice versa.” Pet. 10 (citing Ex. 1003 ¶¶ 17–19). Patent Owner, relying on the testimony of its expert, Dr. Michael Smith, largely agrees with this assessment, with the addition of examples for “[additional] education” and “additional work experience.” Prelim. Resp. 11–12 (citing Ex. 2001 ¶ 16).

For purposes of this Decision on Institution, we adopt Petitioner’s proposed level of ordinary skill in the art. This level of skill comports with the teachings of the ’431 patent and the asserted prior art.

Each of Petitioner and Patent Owner appear to agree that the knowledge of one of ordinary skill should be analyzed as of July 2003, the date of the provisional application to which the application that issued as the '431 patent claimed priority. Ex. 1001, code (60); Pet. 10; Ex. 1003 ¶¶ 18, 19; Ex. 2001 ¶ 16. As previously discussed (*supra* at II.E), whether pre- or post-AIA 35 U.S.C. § 103 should apply affects whether we should consider obviousness to one of ordinary skill in the art at the time the invention was made (pre-AIA § 103) or at the time of the effective filing date (AIA § 103). On the present record, the parties appear to agree that the relevant date is July 2003; we analyze Petitioner's arguments as presented.

C. Claim Construction

In an *inter partes* review, claims are construed using the same claim construction standard that would be used to construe the claims in a civil action under 35 U.S.C. § 282(b), including construing the claims in accordance with the ordinary and customary meaning of such claims as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. 37 C.F.R. § 42.100(b) (2020). We apply the claim construction standard as set forth in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Claim terms are generally given their ordinary and customary meaning as would be understood by one with ordinary skill in the art in the context of the specification, the prosecution history, other claims, and even extrinsic evidence including expert and inventor testimony, dictionaries, and learned treatises, although extrinsic evidence is less significant than the intrinsic record. *Phillips*, 415 F.3d at 1312–17. Usually, the specification is dispositive, and it is the single best guide to the meaning of a disputed term. *Id.* at 1315.

Only those terms that are in controversy need be construed, and only to the extent necessary to resolve the controversy. *Nidec Motor Corp.*, 868 F.3d at 1017 (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

Neither Petitioner nor Patent Owner explicitly requests claim construction. Pet. 10–11; *see* Prelim. Resp. Patent Owner's Preliminary Response raises certain implicit claim construction issues. Additionally, we acknowledge that, in a related litigation, a district court has issued a Markman order construing certain claims of the '431 patent. Ex. 1016. However, in this instance, no resolution of claim construction issues is necessary to resolve the controversy, and thus, we do not construe any claim terms. *See Nidec Motor Corp.*, 868 F.3d at 1017.

D. Ground 1

Petitioner argues that claims 19 and 20 would have been obvious over Willebeek-LeMair. Pet. 13–36. Patent Owner presents arguments relating to these contentions. Prelim. Resp. 2, 8–26. For the reasons discussed below, we determine that Petitioner has not shown a reasonable likelihood that the Petitioner would prevail with respect to these claims.

1. Willebeek-LeMair

Willebeek-LeMair is titled “Network Security System Integration” and relates to network discovery, intrusion detector, and firewalling functionality in a network security system. Ex. 1005, codes (54), (57). 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.

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.

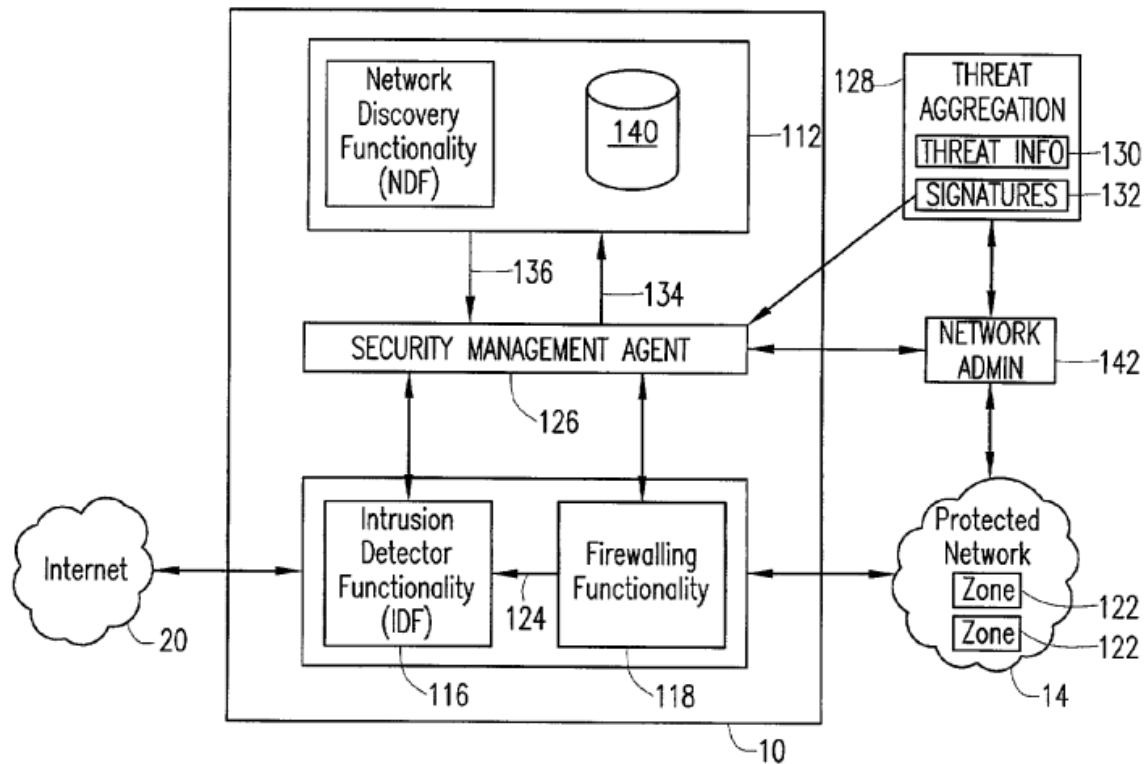


FIG. 2

As seen in Figure 2, network defense system 10 may include intrusion detector functionality 116 that analyzes network traffic to identify traffic that is potentially harmful to the network. *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. This is done by instantiating detection signatures to intrusion detector functionality 116 and firewalling functionality 118 tailored to perceived threats to network 14. *Id.* at 9:45–56. This occurs in an automated manner when security management agent 126 response 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.

2. *Analysis of Claim 19*

Petitioner’s analysis of claim 19 necessarily begins with arguments relating to the asserted obviousness of claim 14, from which claim 19 depends. Pet. 33 (referencing Pet. 14–33). Petitioner then proceeds to analyze the additional limitations of claim 19. Pet. 33–35.

a) *Preamble and Limitations 14.1, 14.2, and 14.3 of Claim 14*

With respect to the preamble of claim 14, reciting “[a] computer program product embodied on a non-transitory computer readable medium,” while not addressing whether the preamble is limiting, Petitioner argues that Willebeek-LeMair teaches an appliance with hardware and software,

including “a security application functionality . . . that is implemented as the unified network defense system.” Pet. 14–15 (citing Ex. 1005, 16:1–5, 16:11–15; Ex. 1003 ¶¶ 38–40). Petitioner argues that it would have been obvious to one of skill in the art to store the security application on a non-transitory computer readable medium. *Id.* (citing Ex. 1003 ¶ 40).

With respect to limitations 14.1, 14.2, and 14.3 (“code for: accessing at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, where: each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option”), Petitioner argues that the “data structure” is taught or suggested by Willebeek-LeMair’s database of signatures inside its network defense system or the “threat aggregation functionality” which stores signatures separately from the network defense system. Pet. 16–18, 19 (citing Ex. 1005, 5:20–27, 8:39–42, 10:36–52, Fig. 1 (element 20), Fig. 2 (element 128); Ex. 1003 ¶¶ 42–45). Petitioner further argues that the mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities are taught or suggested by Willebeek-LeMair’s signatures, because they are data structures designed to mitigate or avert network damage from detected vulnerabilities, and include responses to take in response to detected threats. *Id.* at 18–20 (citing Ex. 1005, 5:20–24, 5:59–65, 7:4–9, 9:45–55, 10:54–60; Ex. 1003 ¶¶ 46–48, 50–52).

Petitioner further argues that Willebeek-LeMair’s teachings regarding accessing the signatures in their storage locations to find one associated with a discovered vulnerability teaches or suggests the accessing of the data structure as recited in limitation 14.1 to obtain a signature describing actions

to perform in response to the associated vulnerability. Pet. 20 (citing Ex. 1005, 5:50–53, 10:50–52, 10:58–60, 13:25–35; Ex. 1003 ¶¶ 53–55). These actions, according to Petitioner, teach or suggest that the signatures (mitigation techniques) are capable of mitigating the effect of an attack taking advantage of a discovered vulnerability, thus teaching or suggesting limitation 14.2. *Id.* at 21–22 (citing Ex. 5:20–27 (detection signatures including “security rules, policies and algorithms . . . designed to mitigate or avert network damage from detected vulnerabilities); 10:46–52, 10:58–60, 11:56–64, 14:46–15:6, 15:37–43; Ex. 1003 ¶¶ 59–64).

Petitioner argues that Willebeek-LeMair teaches each mitigation type mentioned in limitation 14.3. Willebeek-LeMair describes dropping or rejecting a connection request in response to a detected attack, which Petitioner argues teaches or suggest a policy setting and a configuration option. *Id.* at 22–23 (citing Ex. 1005, 9:31–35, 10:58–60; Ex. 1003 ¶¶ 66–73. Petitioner argues that blocking traffic from a specific IP address as described in Willebeek-LeMair teaches a policy setting mitigation type. *Id.* at 24 (citing Ex. 1005, 14:46–15:8; Ex. 1003 ¶¶ 75–77). Petitioner contends that Willebeek-LeMair’s description of the configuration of firewall and intrusion detector to be responsive to attacks teaches or suggests configuration options. *Id.* at 24–25 (citing Ex. 1005, 12:33–43; Ex. 1003 ¶¶ 78–79). And Petitioner argues that Willebeek-LeMair teaches the claimed patch mitigation type in the description of “vendor patches” which can be installed. *Id.* at 25 (citing Ex. 1005, 14:38–45; Ex. 1003 ¶ 81).

In each instance, Petitioner cites a teaching of Willebeek-LeMair with respect to a mitigation that is performed at the intrusion detector functionality 116 or firewalling functionality 118. *Id.* at 23–25.

b) Limitations 14.4 and 14.5 of Claim 14

With respect to limitations 14.4 and 14.5 (“code for: receiving information in connection with at least one of a plurality of devices; and identifying an attack on the at least one device that takes advantage of at least one of the vulnerabilities, based on the information”), Petitioner argues that these limitations are also taught by Willebeek-LeMair’s network defense system. Pet. 26–27.

Petitioner contends that Willebeek-LeMair’s system receives information regarding vulnerabilities of devices in the protected network (element 14), including during a network discovery process. Pet. 26 (citing Ex. 1005, 5:9–19, 8:39–53, 14:48–51; Ex. 1003 ¶¶ 85–87). Additionally, Petitioner argues that Willebeek-LeMair’s system includes an inspection agent which extracts features from entering traffic to the protected network. *Id.* (citing Ex. 1005, 3:41–44, 5:37–41; Ex. 1003 ¶ 88).

Petitioner further contends Willebeek-LeMair’s system identifies an attack based on this information. *Id.* at 27. Petitioner cites Willebeek-LeMair’s comparison of extracted features from the traffic to detection signatures (which relate to identified vulnerabilities) to identify an attack on a device. *Id.* (citing Ex. 1005, 5:50–6:20, 7:17–34, 8:39–53, 14:46–64; Ex. 1003 ¶¶ 92–94).

c) Limitations 14.6 and 14.7 of Claim 14

With respect to limitations 14.6 and 14.7 (“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; wherein the computer

program product is operable such that the effect of the attack is mitigated by preventing the attack from taking advantage of the at least one vulnerability”), Petitioner argues that these limitations are also taught by Willebeek-LeMair’s network defense system. Pet. 28–32.

Petitioner contends that Willebeek-LeMair’s system teaches the application of multiple mitigation techniques to mitigate an effect of an attack that takes advantage of an identified vulnerability. *Id.* at 28–30. Petitioner cites Willebeek-LeMair’s disclosure of applying multiple detection signatures (with different actions in each) and also of allowing multiple actions to be present in a given action set of a detection signature. *Id.* As Petitioner argues, Willebeek-LeMair discloses automatic application of actions in the description of the dropping of a packet related to an attack and the blocking of traffic from the attacker’s address without user interaction. *Id.* at 28–30 (citing Ex. 1005, 14:46–15:21; Ex. 1003 ¶¶ 98, 103, 107–108).

With respect to multiple signatures being applied, Petitioner argues that Willebeek-LeMair discloses this in its disclosure that upon detecting vulnerability, “the correlated one (or ones) of the signatures” are retrieved and instantiated. *Id.* at 28–29 (citing Ex. 1005, 9:45–48; Ex. 1003 ¶¶ 101–102). Petitioner argues that Willebeek-LeMair teaches that the multiple mitigation techniques applied are of at least a first and a second type because, for example, firewalling functionality and intrusion detection functionality in Willebeek-LeMair’s network defense system would deploy different types of techniques, a blocking action by the firewall and a terminating or reporting action by an intrusion detector. *Id.* at 29–30 (citing Ex. 1005, 12:28–43, 14:59–15:2; Ex. 1003 ¶¶ 103–105).

Petitioner argues that Willebeek-LeMair teaches that the effect of the identified attack would be mitigated by preventing the attack from taking advantage of the vulnerability. Willebeek-LeMair teaches, for example, that its “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 (quoted at Pet. 31). Petitioner contends that one of ordinary skill would have recognized that the actions taught in Willebeek-LeMair would mitigate the effect of an attack by preventing it from taking advantage of the vulnerability associated with the signature including these actions. Pet. 31–32 (citing Ex. 1005, 9:21–35, 12:28–43, 14:67–15:8; Ex. 1003 ¶¶ 113–116).

d) Analysis

As with its arguments with respect to limitations 14.1–14.3, in each example relating to Willebeek-LeMair’s teachings of limitation 14.6 of claim 14, Petitioner cites mitigations performed by the intrusion detector functionality 116 or firewalling functionality 118. *Id.* at 28–30 (describing a block action taken by the firewalling functionality and a terminate action being taken by the intrusion detector functionality, also describing an example relating to the firewalling functionality dropping packet traffic relating to an attempted exploitation of a vulnerability (*see* Ex. 1005, 14:59–15:2)).

However, unaddressed is the claim’s requirement that each of the two of the plurality of mitigation techniques be automatically applied “**to the at least one device.**” Throughout the discussion of the limitations of claim 14, and again with respect to remaining challenged claim 19, Petitioner only describes the mitigation techniques to be taught by the application of signatures to the intrusion detector functionality and the firewalling

functionality of Willebeek-LeMair, which are included within the network defense system. However, Petitioner also asserts that the “plurality of devices” of the claim are the devices within the network being protected. *See* Pet. 26 (in arguing that Willebeek-LeMair teaches “code for: receiving information in connection with at least one of a plurality of devices,” (14.4) citing network discovery functionality to discover vulnerabilities in a scan of “machines” in protected network 14). Thus, Petitioner fails to show how Willebeek-LeMair teaches or suggests “automatically applying at least two of the plurality of mitigation techniques . . . **to the at least one device**,” that is, to a device in network 14.

Additionally, with respect to claim 19, Petitioner again uses the example, for teaching a first and second mitigation technique, of the intrusion prevention functionality and the firewalling functionality as the first and second mitigation techniques. Pet. 33–34 (citing Ex. 1005, 9:51–55, 12:28–43, 14:59–15:2; Ex. 1003 ¶¶ 126–128).

Patent Owner argues that the claims of the ’431 Patent require a server-client model for application of mitigation techniques in which mitigation techniques are applied to a client agent and contends that:

In sharp contrast, and as acknowledged by Petitioner at Page 39 of its petition, [Willebeek-LeMair] merely discloses an “in-line component” that sits at a “boundary” of a network of computers (“As an in-line component, [Willebeek-LeMair]’s integrated system 10 exists at the boundary of the protected network such that “all traffic 30 must pass through the entrance sentry 42 *before* entering the protected network 14.” [Pet. 39] - emphasis added). Thus, there is no similar client-server model disclosed by [Willebeek-LeMair] where “signatures” are applied to an endpoint device by communicating such “signatures” from server “code” to a client agent on such device.

Prelim. Resp. 23. Petitioner cites mitigation techniques applied only within the network defense system of Willebeek-LeMair, which as Patent Owner argues, appears to be an “in-line” or “boundary” system for network 14. While not specifically identified by the Patent Owner, the requirement in the claim that mitigation techniques be “automatically appl[ied]” “to the at least one device” that had been identified as the object of an attack is one which is neither addressed nor clearly shown as taught or suggested by the citations in the Petition to Willebeek-LeMair’s mitigation techniques applied within the network defense system, rather than to the devices in the protected network which have been identified as vulnerable.

For this reason, Petitioner has not shown a reasonable likelihood prevailing in showing that claim 19 is obvious over Willebeek-LeMair.

3. *Analysis of Claim 20*

Petitioner argues that claim 20, which depends from claim 19, incorporates Petitioner’s arguments with respect to claim 19. Pet. 35–36. Thus, for the same reasons given above, Petitioner has not shown a reasonable likelihood prevailing in showing that claim 20 is obvious over Willebeek-LeMair.

IV. CONCLUSION

Based on the arguments and evidence presented in the Petition, we conclude Petitioner has not demonstrated a reasonable likelihood that Petitioner would prevail in showing at least one of the challenged claims of the ’431 patent is unpatentable based on any asserted ground of unpatentability. Therefore, we do not institute an *inter partes* review with respect to any of the challenged claims of the ’431 patent.

V. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is denied, and no *inter partes* review is instituted.

IPR2021-01242
Patent 9,100,431 B2

FOR PETITIONER:

Theodore M. Foster
David L. McCombs
Adam C. Fowles
Clint S. 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:

G. Andrew Gordon
ANDREW GORDON LAW FIRM, PLLC
andrew@agordonlawfirm.com