

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioner,

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00678
Patent 8,117,645 B2

Before CHRISTOPHER M. KAISER, JOHN A. HUDALLA, and
AARON W. MOORE, *Administrative Patent Judges*.

Opinion for the Board filed by *Administrative Patent Judge*
JOHN A. HUDALLA.

Dissenting Opinion filed by *Administrative Patent Judge*
AARON W. MOORE.

HUDALLA, *Administrative Patent Judge*.

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

Cisco Systems, Inc. and Fortinet, Inc. (collectively, “Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1, 2, 5, and 6 (“the challenged claims”) of U.S. Patent No. 8,117,645 B2 (Ex. 1301, “the ’645 patent”). Petitioner filed a Declaration of Henry Houh, Ph.D. (Ex. 1303) with its Petition. InfoExpress, Inc. (“Patent Owner”) filed a Preliminary Response (Paper 7¹, “Prelim. Resp.”), along with declarations of Dr. Eric Cole (Ex. 2001) and Hugh Smith, Ph.D. (Ex. 2007). With our authorization (Paper 9), Petitioner also filed a Preliminary Reply (Paper 11, “Pet. Prelim. Reply”) and Patent Owner filed a Preliminary Sur-reply (Paper 12, “PO Prelim. Sur-reply”) directed to Patent Owner’s attempt to antedate the asserted references.

We have authority to determine whether to institute an *inter partes* review. See 35 U.S.C. § 314 (2018); 37 C.F.R. § 42.4(a) (2023). Under 35 U.S.C. § 314(a), we may not authorize an *inter partes* review unless the information in the petition and the preliminary response “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.” For the reasons that follow, we do not institute an *inter partes* review.

¹ Paper 7 was filed with its availability restricted to “Filing Party and Board.” Patent Owner filed a public version of the Preliminary Response as Paper 8.

I. BACKGROUND

A. *Real Parties-in-Interest*

Petitioner identifies Cisco Systems, Inc. and Fortinet, Inc. as the real parties-in-interest. Pet. 1. Patent Owner identifies InfoExpress Inc. as the real party-in-interest. Paper 5, 1 (Patent Owner’s Mandatory Notices).

B. *Related Matters*

As required by 37 C.F.R. § 42.8(b)(2), the parties identify the following district court cases as related matters:

InfoExpress Inc. v. Fortinet, Inc., No. 4:23-cv-04389 (N.D. Cal. filed Aug. 25, 2023); and

InfoExpress Inc. v. Cisco Systems, Inc., No. 4:23-cv-02698 (N.D. Cal. filed May 31, 2023).

Pet. 1; Paper 5, 1. Patent Owner additionally identifies the following *inter partes* review proceedings as being related: IPR2024-00539, IPR2024-00540, IPR2024-00676, and IPR2024-00677. Paper 5, 1–2

C. *The ’645 Patent*

The ’645 patent is titled “Systems and Methods of Controlling Network Access” and is directed to “[a] new approach to network security.” Ex. 1301, codes (54), (57). The ’645 patent describes “[s]everal approaches to controlling external access to computing networks” that serve the goals of “limiting access to authorized users and assuring that computing devices employed by these users do not include malicious computing code.” *Id.* at 1:24–29. “A first level of access control is achieved by requiring authentication of a user.” *Id.* at 1:33–34. “A greater level of access control may be achieved by including a gatekeeper between the secure network and

the access device.” *Id.* at 1:55–57. Figure 1 of the ’645 patent depicts such a gatekeeper and is reproduced below.

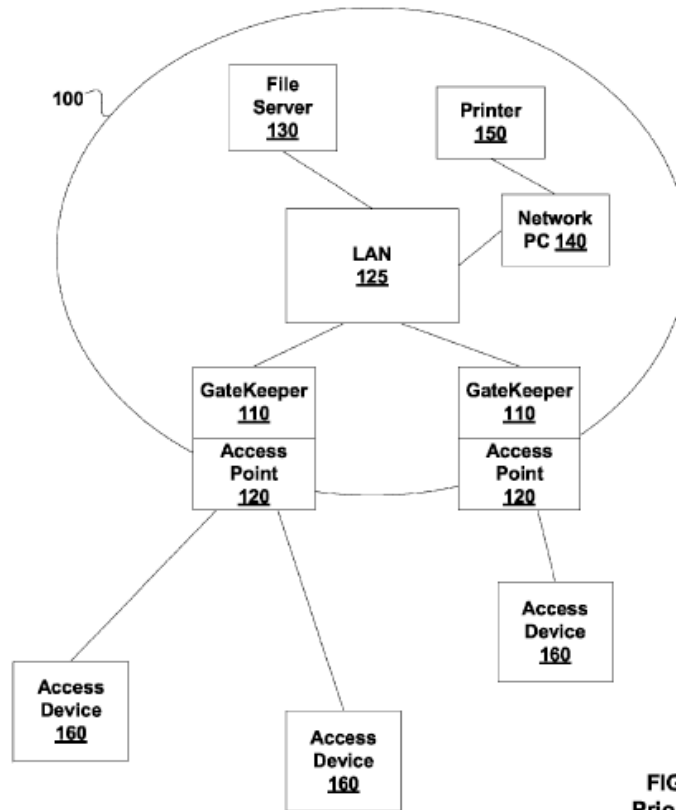


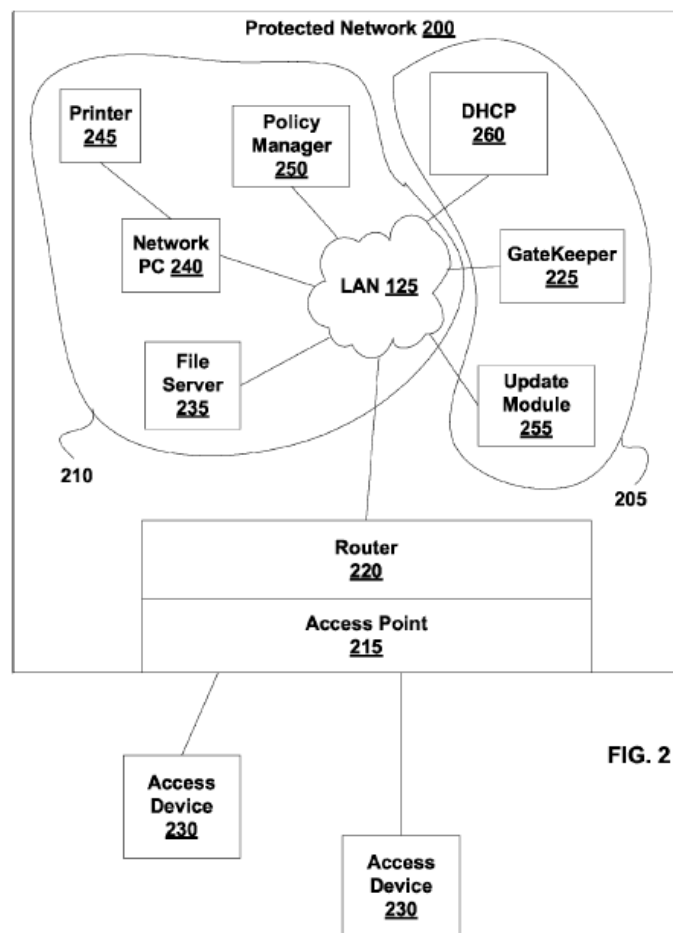
FIG. 1
Prior Art

Id. at Fig. 1. In Figure 1, access devices 160 communicate with access points 120, each of which connects with LAN 125 within secure network 100 through gatekeeper 110. *Id.* at 1:59–2:15. “A disadvantage of the use of GateKeeper 110, as practiced in the prior art, is that all communications between Access Device 160 and LAN 125 pass through GateKeeper 110,” which “can be a significant burden.” *Id.* at 2:28–33. The ’645 patent seeks to remove this disadvantage using “a protected network physically or logically divided into a restricted subset and one or more less-restricted subsets.” *Id.* at 2:50–52. “Requests from an access device for access to the less-restricted subset are first passed to the restricted subset,” and the gatekeeper is “then used to apply security policies to the

access device and if [the] security policies are satisfied, the access device is granted access to a less-restricted subset of the protected network.” *Id.*

at 2:52–58. “To grant access, the gatekeeper sends commands to the access point in order to reconfigure a communication port to which the access device is connected.” *Id.* at 3:22–24. “The reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN.” *Id.* at 3:24–27.

Figure 2 of the ’645 patent depicts “a protected network, according to various embodiments of the invention.” Ex. 1301, 5:4–5. That figure is reproduced below.



Id. at Fig. 2. “Protected Network 200 is either physically or logically divided into a Restricted Subset 205 and a Less-Restricted Subset 210.” *Id.* at 5:56–58. Access devices 230 can connect to the protected network “through an Access Point 215 . . . and an optional Router 220.” *Id.* at 5:59–61. “[T]his access is under the control of a GateKeeper 225,” which is located within restricted subset 205 and which “is configured to enforce a security policy against” the access device. *Id.* at 5:61–64, Fig. 2.

D. Illustrative Claim

Of the challenged claims, claim 1 is independent. Claims 2, 5, and 6 depend from claim 1. Claim 1 is illustrative of the challenged claims and recites:

1. A network access control system, comprising:
 - an authentication module stored in memory and executable by a processor to authenticate a device seeking network access based at least on authentication information received from the device;
 - a gatekeeper stored in memory and executable to:
 - formulate an audit request,
 - send the audit request to the device,
 - evaluate device information received from the device in response to the audit request, and
 - approve the device based on evaluation of the device information; and
 - an extensible authentication protocol (EAP) server layer (SL) stored in memory and executable to:
 - receive the authentication information from the device using an EAP encryption protocol, and

configure an access point in response to approval
of the device by the gatekeeper.

Ex. 1201, 16:19–36.

E. Prior Art

Petitioner relies on the following prior art:

U.S. Patent Application Publication No. 2004/0111520
A1, filed Dec. 6, 2002, published June 10, 2004 (Ex. 1305,
“Krantz”); and

U.S. Patent Application Publication No. 2004/0107360
A1, filed Mar. 13, 2003, published June 3, 2004 (Ex. 1306,
“Herrmann”).

F. The Asserted Grounds

Petitioner challenges claims 1, 2, 5, and 6 of the ’645 patent based on
the following grounds (Pet. 3):

Claims Challenged	35 U.S.C. §	References
1, 2, 5, 6	103(a) ²	Krantz
1, 2, 5, 6	103(a)	Krantz, Herrmann

² 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. Because the ’645 patent claims priority to an application filed before March 16, 2013 (the effective date of the relevant amendments), we assume that the pre-AIA versions of §§ 102 and 103 apply. However, our decision would be the same under the current version of the statutes.

II. ANALYSIS

We now consider Petitioner’s asserted grounds and Patent Owner’s arguments to determine whether Petitioner has met the “reasonable likelihood” standard for institution under 35 U.S.C. § 314(a).

A. *Legal Standards*

A 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 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. *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) where in evidence, so-called secondary considerations. *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966). We also recognize that prior art references must be “considered together with the knowledge of one of ordinary skill in the pertinent art.” *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994) (citing *In re Samour*, 571 F.2d 559, 562 (CCPA 1978)).

B. *Level of Ordinary Skill in the Art*

Citing testimony from Dr. Houh, Petitioner contends that 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 relevant experience in networking and network security, and related fields.” Pet. 4. Petitioner also asserts that “[l]ack of professional experience can be

remedied by additional education, and vice versa.” *Id.* Patent Owner argues that a person of ordinary skill in the art “would have had a bachelor’s degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cybersecurity.” Prelim. Resp. 1. Alternatively, Patent Owner argues that a person of ordinary skill in the art would have had “a master’s degree in one of the foregoing and at least two years of experience in the aforementioned fields.” *Id.* at 2. Patent Owner does not cite any evidence supporting its assessment of the level of ordinary skill. Neither party explains why the outcome of this case would be affected by the adoption of any of the proffered definitions of a person of ordinary skill in the art.

For purposes of this Decision, we adopt Petitioner’s definition of the level of ordinary skill in the art. On the present record, we are satisfied that this definition of the level of skill is consistent with the teachings of the ’645 patent and the asserted prior art.

C. *Claim Interpretation*

In an *inter partes* review, we construe each claim using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim 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). Accordingly, our claim construction standard is the same as that of a district court. *See id.* Under the standard applied by district courts, claim terms are generally given their plain and ordinary meaning, as would have been understood by a person of ordinary skill in the

art at the time of the invention and in the context of the entire patent disclosure. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc). “There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution.” *Thorner v. Sony Comput. Entm’t Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012).

Petitioner argues that “a [person of ordinary skill in the art] would find the challenged claims unpatentable under any interpretation consistent with their plain and ordinary meaning in the context of the [’645 patent],” so we “need not expressly construe the claim terms.” Pet. 8. Patent Owner also argues that we should apply the plain and ordinary meaning of all claim terms. Prelim. Resp. 6. Nonetheless, Patent Owner argues that Petitioner deviates from the plain and ordinary meaning of certain limitations. *Id.* at 6–7. Thus, Patent Owner puts forth its understanding of the plain and ordinary meaning for the following recitations: “configure an access point in response to approval of the device by the gatekeeper” and “device information received from the device in response to the audit request.” *Id.* at 7–13.

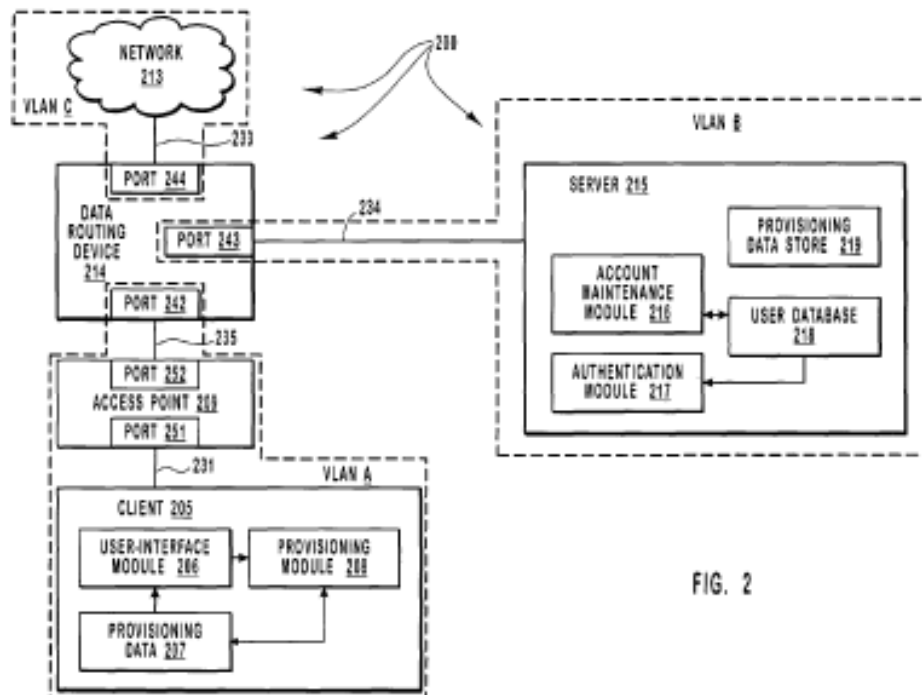
Based on the present record, we need not expressly construe any claim terms in order to render the instant Decision. *See, e.g., Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Obviousness Ground Based on Krantz

Petitioner contends the subject matter of claims 1, 2, 5, and 6 would have been obvious over Krantz. Pet. 21–70. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 19–35, 40–53.

1. *Krantz*

Krantz is a U.S. patent application titled “Increasing the Level of Automation when Provisioning a Computer System to Access a Network.” Ex. 1305, code (54). Krantz “relates to configuring computer systems to appropriately communicate on a network, and more specifically, to automatically providing a computer system with appropriate information such that the computer system can be provisioned to communicate on a network.” *Id.* ¶ 2. Figure 2 of Krantz is reproduced below.



Id. at Fig. 2. Figure 2 “illustrates an example of a network architecture that can facilitate increasing the level of automation when provisioning a client.”

Id. ¶ 28. In Figure 2, “[d]ata can be transferred between access po[in]t 209 and client 205 through port 251. Likewise, data can be transferred between access point 209 and data routing device 214 through port 252.” *Id.* ¶ 63. “Data routing device 214 can be configured to transfer both tagged data frames and untagged data frames between the VLANs depicted in FIG. 2.” *Id.* ¶ 60.

2. *Claim 1*

Our disposition of this ground turns on the limitation “formulate an audit request,” which is part of a larger limitation reciting “a gatekeeper stored in memory and executable to: formulate an audit request.” Ex. 1301, 16:24–25. Petitioner maps the recited “gatekeeper” to Krantz’s server 215. Pet. 35–36 (citing Ex. 1305, Fig. 2). For “formulat[ing] an audit request,” Petitioner cites Krantz’s teaching of requesting that client 205 send a password associated with a user identifier or other credential information. Pet. 38 (citing Ex. 1305 ¶ 74). Petitioner notes that this may be accomplished when “client 205 and server 215 exchange EAP-messages to pass certificates, keys, and supported cipher suites.” *Id.* Petitioner further contends that server 215 formulates such requests for sending within HTTP packets. *Id.* at 38–39 (citing Ex. 1305 ¶¶ 67–68, 78). Petitioner additionally notes that the requests can include various configuration settings related to the specific EAP type of authentication that is desired. *Id.* at 39–40 (citing Ex. 1305 ¶¶ 67–68).

Patent Owner argues that Krantz’s server 215 (i.e., the “gatekeeper”) is “only for authentication.” Prelim. Resp. 27 (citing Pet. 36–37; Ex. 1320, 3). Patent Owner cites Petitioner’s statements from the Petition that

“server 215 logically represents a Remote Authentication Dial-In User Service (‘RADIUS’) server” and that “RADIUS was ***a well-known authentication software*** system.” *Id.* (emphasis by Patent Owner) (quoting Pet. 36–37). Patent Owner further notes that the ’645 patent recites authentication and auditing as “separate and distinct elements.” *Id.* Thus, Patent Owner argues that Krantz does not teach a “gatekeeper” that “formulate[s] an audit request.”

We are persuaded by Patent Owner’s arguments. As noted by Patent Owner (Prelim. Resp. 27), claim 1 separately recites (1) “an authentication module” that seeks access based on “authentication information” and (2) a “gatekeeper” that “formulate[s] an audit request” and evaluates whether to approve access based on a response to the audit request. The fact that authentication can be a part of a security policy audit (*see* Pet. 38 (citing Ex. 1301, 11:67–12:6)) does not change the fact that claim 1 recites separate sets of limitations for authentication and auditing that Petitioner must account for in its unpatentability contentions.

Furthermore, the specification of the ’645 patent distinguishes between authenticating a user with a username and password and ensuring that a device complies with a security policy. Ex. 1301, 1:33–37 (“A first level of access control is achieved by requiring authentication of a user. This may be accomplished by requiring the user to enter a username and a password.”), 1:43–46 (“Reliance on mere user authentication includes several disadvantages. For example, there are no provisions to assure that an access device used by the authenticated user meets network security policies.”), 1:55–58 (“A greater level of access control may be achieved by including a gatekeeper between the secure network and the access device.

The gatekeeper is configured to ensure that the access device conforms to a predetermined security policy.”). Although the specification describes both user authentication and security auditing as being carried out by a gatekeeper, this is accomplished in separate process steps. *Id.* at 10:38–41 (“GateKeeper 225 authenticates a user, obtains audit data, and applies a security policy in an Authenticate User Step 440, an Obtain Audit Data Step 450 and an Apply Security Policy Step 460, respectively.”). Thus, we are not persuaded that, as Petitioner argues, data exchanges related to user authentication in the ’645 patent constitute the formulation of an audit request.

Yet Petitioner’s contentions for “formulat[ing] an audit request” relate solely to authentication. Petitioner cites Krantz’s teachings on providing passwords associated with a user identifier, exchanging EAP messages with “certificates, keys, and supported cipher suites,” and exchanging “other credential information.” Pet. 38 (citing Ex. 1305 ¶ 74). Krantz teaches that the exchange of EAP messages relates to the authentication of a user through “a User-Identifier” to determine whether “a user of client 205 has an account with server 215.” Ex. 1305 ¶ 71. Moreover, Krantz states that its “credentials” include a “user-identifier and password” that are “compare[d] . . . to entries in [a] user database.” *Id.* ¶ 76. Regarding “certificates, keys, and supported cipher suites,” Petitioner does not explain why any of these items would relate to an audit rather than authentication. And Petitioner and Dr. Houh call these items “authentication information” in other parts of the record. Pet. 52; Ex. 1303 ¶ 136. We additionally note that Petitioner associates Krantz’s server 215, the alleged “gatekeeper,” with a RADIUS server, which Petitioner acknowledges to be “a well-known authentication

software system.” Pet. 36–37 (citing Ex. 1303 ¶ 92; Ex. 1305 ¶ 58; Ex. 1320, 3). Based on the present record, Petitioner has not shown sufficiently that any of these disclosures from Krantz teach or suggest “formulat[ing] an audit request.”

In addition, Petitioner cites the same or similar teachings from Krantz for teaching limitations directed to authentication. *See, e.g.*, Pet. 30 (mapping “authentication information” to Krantz’s credentials sent from client 205 to server 215), 31 (mapping “authentication information” to Krantz’s EAP Response/Identity message from the client to the server). As such, Petitioner relies on essentially the same analysis based on Krantz for teaching two processes that are expressly distinguished in the specification of the ’645 patent. Because Petitioner fails to develop a coherent unpatentability theory with respect to both the “audit” and “authentication” limitations, we find that Petitioner has not shown sufficiently that Krantz teaches or suggests “a gatekeeper . . . to: formulate an audit request.”

For these reasons, and based on the present record, we determine that Petitioner has not established a reasonable likelihood that it would prevail in showing that the subject matter of claim 1 would have been obvious over Krantz.

3. *Claims 2, 5, and 6*

Claims 2, 5, and 6 all depend from claim 1. Ex. 1301, 16:37–39, 13:45–49. Petitioner’s analysis for these claims relies on the same deficient analysis that is discussed above with respect to claim 1. *See* Pet. 64–70. Further, Petitioner’s analysis for these claims does not cure the deficiencies discussed above with respect to claim 1. Thus, we determine that Petitioner

has not established a reasonable likelihood that it would prevail in showing that the subject matter of claims 2, 5, and 6 would have been obvious over Krantz.

E. Obviousness Ground Based on Krantz and Herrmann

Petitioner contends that claims 1, 2, 5, and 6 would have been obvious over the combination of Krantz and Herrmann. Pet. 70–73. Patent Owner disputes Petitioner’s contentions. Prelim. Resp. 36–53.

1. Herrmann

Herrmann is a U.S. patent application titled “System and Methodology for Policy Enforcement.” Ex. 1306, code (54). Herrmann “relates generally to information processing and, more particularly, to systems and methods for policy enforcement on computer systems connected to one or more networks.” *Id.* ¶ 3. According to Herrmann, “if a client device connected to a network . . . is infected with a virus or worm, it may infect other machines on the same network,” making it important to “ensur[e] that devices connected to the network are running current anti-virus programs.” *Id.* ¶ 12. To do so, Herrmann teaches a system in which a client device attempts to access a network and information is collected “from the client device” so that the system can “determin[e] whether to authenticate the client device for access to the network based, at least in part, upon the collected information.” *Id.*, code (57).

2. *Claim 1*

Claim 1 recites that the gatekeeper is executable to “formulate an audit request.” Ex. 1301, 16:25. Building on its analysis for the Krantz obviousness ground, Petitioner further contends that, “[t]o the extent one may assert that Krantz does not teach or suggest ‘*formulate*’ with respect to the gatekeeper’s ‘*audit request*,’ it would have been obvious that the gatekeeper of Krantz formulates (i.e., generates) such a request in view of Herrmann. Pet. 70. Specifically, Petitioner cites Herrmann’s teaching of access implementation module 553 formulating “a RADIUS Access-Accept” package for transmission by proxy server 440. *Id.* at 71 (citing Ex. 1306 ¶ 79). Petitioner further contends that an ordinarily skilled artisan would have been motivated to combine Herrmann with Krantz.³ *Id.*

Patent Owner disputes that Herrmann teaches the recitation “formulate an audit request.” Prelim. Resp. 37–38. Patent Owner argues that Petitioner’s cited teaching about Herrmann’s “RADIUS Access-Accept package” is “directed to authentication and is not an audit request.” *Id.* at 37 (citing Ex. 1306 ¶¶ 56, 73).

We agree with Patent Owner. As discussed above, Petitioner acknowledges that a RADIUS server pertains to authentication. *See* Pet. 36–37. Petitioner puts forth no reasoning or evidence to support that Herrmann teaches or suggests “generat[ing] an audit request”—rather than an authentication request—with its disclosed RADIUS server. As such,

³ Petitioner mistakenly references “§VIII.C” of the Petition for its arguments about the combination of Krantz and Herrmann, but the context makes clear that Petitioner intended to reference § VII.C, which is found at pages 15–21 of the Petition.

Petitioner's added analysis based on Herrmann for this limitation suffers from the same deficiencies discussed above with respect to the Krantz obviousness ground. Further, Petitioner's references to other parts of the Petition for its arguments about the combination of Krantz and Herrmann do not salvage its analysis for "formulat[ing] an audit request." We have considered these arguments (*see* Pet. 15–21), and find that they do not show with particularity how the combination of Krantz and Herrmann teaches a particular "request" or how any such request is "formulate[d]." *See* 35 U.S.C. § 312(a)(3) (stating that a petition must "identif[y], in writing and with particularity, each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim"); *see also* 37 C.F.R. § 42.104(b) (stating that a petition must "specify where each element of the claim is found in the prior art patents or printed publications relied upon").

For these reasons, and based on the present record, we determine that Petitioner has not established a reasonable likelihood that it would prevail in showing that the subject matter of claim 1 would have been obvious over the combination of Krantz and Herrmann.

3. *Claims 2, 5, and 6*

Claims 2, 5, and 6 all depend from claim 1. Ex. 1301, 16:37–39, 13:45–49. Petitioner's analysis for these claims relies on the same deficient analysis that is discussed above with respect to claim 1. *See* Pet. 64–70. Further, Petitioner's analysis for these claims does not cure the deficiencies discussed above with respect to claim 1. Thus, we determine that Petitioner has not established a reasonable likelihood that it would prevail in showing

that the subject matter of claims 2, 5, and 6 would have been obvious over the combination of Krantz and Herrmann.

III. CONCLUSION

After considering the evidence and arguments presented in the current record, we determine that Petitioner has not demonstrated a reasonable likelihood that it would prevail with respect to at least one of the claims challenged in the Petition. Therefore, we do not institute an *inter partes* review on the asserted grounds as to any of the challenged claims.

IV. ORDER

Accordingly, it is

ORDERED that the Petition is denied as to all challenged claims, and no *inter partes* review is instituted.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC. and FORTINET, INC.,
Petitioner

v.

INFOEXPRESS INC.,
Patent Owner.

IPR2024-00678
Patent 8,117,645 B2

Before CHRISTOPHER M. KAISER, JOHN A. HUDALLA, and
AARON W. MOORE, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*, dissenting.

I respectfully dissent from the denial of institution in this case because, in my view, Petitioner has established a reasonable likelihood that the challenged claims are not patentable over the combination of Kranz and Hermann presented in the Petition.

Background

Challenged claim 1 is directed to a network access control system with an “authentication module” that “authenticate[s] a device seeking network access based at least on authentication information received from

the device.” There is a “gatekeeper” that “formulate[s] an audit request,” “send[s] the audit request to the device,” “evaluate[s] device information received from the device” and “approve[s] the device based on evaluation of the device information.” There is also “an extensible authentication protocol (EAP⁴) server layer” that “receive[s] the authentication information from the device using an EAP encryption protocol” and “configure[s] an access point in response to approval of the device by the gatekeeper.”

Grounds 1 and 2

For Ground 1, Petitioner relies on Krantz alone. I agree with the majority that Krantz by itself is insufficient to prove these claims unpatentable because, although Krantz discloses authentication, it does not teach or suggest enforcement of security policies.

In Ground 2, Petitioner adds Hermann, which describes “systems and methods for policy enforcement on computer systems connected to one or more networks.” Ex. 1306 ¶ 3. Hermann thus includes the policy enforcement missing from Krantz.

The majority focuses on the claim limitation “formulate an audit request,” finding that Petitioner relied on the RADIUS server for the request formulation but failed to show how the art teaches or suggests generation of an audit request with the RADIUS server. See Majority Decision 17–18. The majority additionally finds that other parts of the Petition describing the

⁴ “The Extensible Authentication Protocol (EAP) is a general protocol for authentication” in which “[t]he clients and an authentication server (e.g., RADIUS server) typically exchange EAP messages by embedding them as attributes of a RADIUS packet.” Ex. 1306 ¶ 27. “Server layer” means that the layer is on the server, as opposed to being a layer on the client. See Ex. 1301, 14:22–15:16.

combination do not sufficiently show how the combination teaches a particular “request” or how any such request is “formulate[d].” *Id.* (referencing pages 15–21 of the Petition).

I agree that the passage quoted on page 71 of the Petition is insufficient to show formulation of an audit request. That paragraph of Hermann describes how the “access implementation module” receives what amounts to a decision from the policy server regarding a given client and creates a “RADIUS Access-Accept package” that is sent to the proxy server to control the client’s access to the network depending on the decision. It is a step that occurs *after* the audit request has been formulated and sent, the audit information has been received, and the decision based on the information has been made.

However, the section of the Petition addressing “formulate an audit request” also expressly refers to the Petition’s description of the combination in Section VII.C. There, Petitioner asserts that “Herrmann discloses a ‘policy server 460 [which] may enforce a variety of different types of security policies or rules’” and that “[o]ne such rule . . . would be ‘a policy requiring that a specific virus protection program is operational on each client device that is connected to a network.’” Pet. 15–16 (citing Ex. 1306, 12, 68).

Cited paragraph 68 of Hermann begins a description of how “the policy server 460 may enforce a variety of different types of security policies or rules.” The patent then describes what types of policies could be applied (§ 68), where the policy server may be located (§ 69), and identifies the “TrueVector engine” for policy definition and enforcement (§ 71). Starting at paragraph 72, Hermann details the operation of the policy server.

The process begins “when the proxy server 440 receives an EAP Access-Accept packet from the RADIUS server 330 for a given client” and then “*issues a policy challenge to the client.*” Ex. 1306 ¶ 77 (emphasis added); *see also id.* ¶¶ 93–96 (further describing the policy challenge).

In my view, the Petition’s explicit reference to Hermann’s policy server is sufficient to incorporate the operational aspects of that server, including the description of issuing a policy challenge. I would find that “issu[ing] a policy challenge to the client” would be sufficient to teach or suggest “formulate an audit request.” An audit request is a type of challenge and it would have to be “formulated” to be issued. I note that Hermann operates by querying a policy agent running on the client, which is essentially the same as the mechanism used in the ’645 patent. *Compare* Ex. 1306 ¶ 64 (describing the client-side policy (integrity) agent 413), *with* Ex. 1301, 7:21–30 (describing the client-side software or hardware agent).

For Ground 2, Patent Owner also argues “that Herrmann fails to disclose at least the ‘configur[ing] an access point in response to approval of the device by the gatekeeper’ limitation.” Prelim. Resp. 36. This is not persuasive to me because Petitioner relies on Krantz for the access point configuration, and the *combination* of the references for the configuration being based on gatekeeper approval. The combination contemplates that access would be controlled using Krantz’s configuration technique depending on (a) valid authentication, and (b) satisfaction of the security policy. *See* Pet. 15 (“It would have been obvious to include Herrmann’s techniques related to enforcing security policies (including checking for anti-virus protection at the client) and obtaining system data from an access device in the system of Krantz.”), 16 (arguing that one would have been

“motivated to modify the teachings of Krantz to include in security policy requirements that a specific virus protection program be utilized, and to make a determination if the client device satisfies the applicable security policies before allowing the client device to access protected networks in order to prevent viruses from infecting the protected network and to ensure network compatibility”).

This leaves Patent Owner’s effort to antedate this prior art. As we have already concluded (*see* IPR2024-00539, Paper 13, 14), I think that is an issue best decided on a complete record and therefore would not deny the Petition on the grounds that Krantz and Hermann are not prior art to the challenged claims.

For these reasons, I would find Ground 2 of the Petition sufficient to show a reasonable likelihood that Petitioner would establish that at least challenged claim 1 is unpatentable.⁵

⁵ Patent Owner does not argue that the Kranz/Hermann combination does not meet the “extensible authentication protocol (EAP) server layer (SL)” limitation or that the server layer is not executable to receive the authentication information or configure the access point in response to approval by the gatekeeper.

IPR2024-00678
Patent 8,117,645 B2

PETITIONER:

Scott Border
Winston & Strawn LLC
sborder@winston.com

Patrick McPherson
Patrick Muldoon
David Dotson
DUANE MORRIS LLP,
pdmcperson@duanemorris.com
pcmuldoon@duanemorris.com
dcdotson@duanemorris.com

PATENT OWNER:

Brian R. Michalek
Joseph M. Kuo
Brian R. Landry
Saul Ewing LLP
Brian.Michalek@saul.com
Joseph.Kuo@saul.com
Brian.Landry@saul.com