

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.

IPR2024-00540
Patent 8,347,350 B2

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

KAISER, *Administrative Patent Judge*.

DECISION

Denying 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. and Fortinet, Inc. (collectively, “Petitioner”) filed a Petition (Paper 1, “Pet.”) requesting *inter partes* review of claims 1, 2, 4–10, 13, 16, 18, and 19 (“the challenged claims”) of U.S. Patent No. 8,347,350 B2 (Ex. 1101, “the ’350 patent”). InfoExpress Inc. (“Patent Owner”) filed a Preliminary Response (Paper 7, “Prelim. Resp.”). With our authorization, Petitioner filed a Reply to Patent Owner’s Preliminary Response (Paper 11, “Prelim. Reply”), and Patent Owner filed a Preliminary Sur-Reply (Paper 12, “Prelim. Sur-Reply”).

We have authority, acting on the designation of the Director, to determine whether to institute an *inter partes* review under 35 U.S.C. § 314 and 37 C.F.R. § 42.4(a). *Inter partes* review may not be instituted unless “the information presented in the petition filed under [35 U.S.C.] section 311 and any response filed under [35 U.S.C.] 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) (2018). “When instituting *inter partes* review, the Board will authorize the review to proceed on all of the challenged claims and on all grounds of unpatentability asserted for each claim.” 37 C.F.R. § 42.108(a) (2023).

For the reasons set forth below, upon considering the briefing and the evidence of record, we determine that the information presented in the Petition does not establish a reasonable likelihood that Petitioner will prevail with respect to any of the challenged claims. Accordingly, we do not institute *inter partes* review.

B. 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, 2.

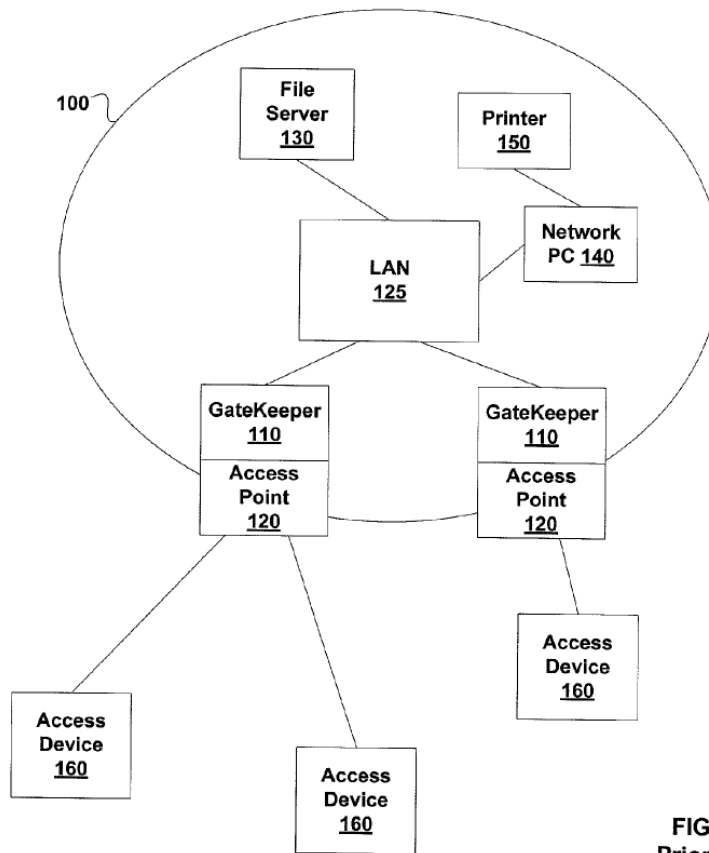
C. Related Matters

The parties identify the following related court proceedings:
InfoExpress Inc. v. Cisco Systems, Inc., Case No. 4:23-cv-02698-YGR (N.D. Cal.), and *InfoExpress Inc. v. Fortinet, Inc.*, Case No. 4:23-cv-04389-YGR (N.D. Cal.). Pet. 1; Paper 5, 2.

D. The '350 Patent

The '350 patent is titled “Systems and Methods of Controlling Network Access” and issued on January 1, 2013. Ex. 1101, codes (45), (54). It is directed to “[a] new approach to network security.” *Id.* at code (57).

The '350 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 1:26–30. “A first level of access control is achieved by requiring authentication of a user.” *Id.* at 1:35–36. “A greater level of access control may be achieved by including a gatekeeper between the secure network and the access device.” *Id.* at 1:57–59. Figure 1 of the '350 patent depicts such a gatekeeper and is reproduced below.

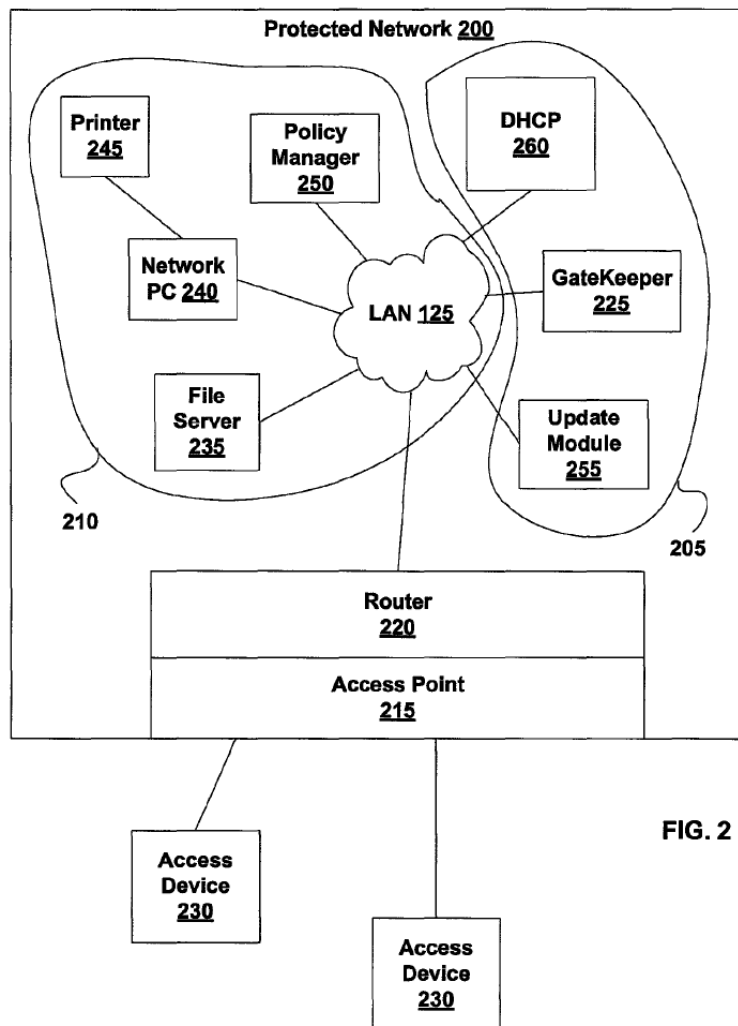


Id. at Fig. 1. In Figure 1, access devices 160 communicate with access points 120, each of which connects with LAN 125 within secure network 100 through gatekeeper 110. *Id.* at 1:61–2:17. “A disadvantage of the use of GateKeeper 110, as practiced in the prior art, is that all communications between Access Device 160 and LAN 125 pass through GateKeeper 110,” which “can be a significant burden.” *Id.* at 2:30–35.

The '350 patent seeks to remove this disadvantage using “a protected network physically and logically divided into a restricted subset and one or more less-restricted subsets.” *Id.* at 2:52–54. “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 2:56–60. “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 3:24–26. “The reconfiguration typically includes reassigning the communication port from the restricted VLAN to the less-restricted VLAN.” *Id.* at 3:26–29.

Figure 2 of the '350 patent depicts “a protected network, according to various embodiments of the invention.” *Id.* at 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.

E. Illustrative Claim

Petitioner challenges claims 1, 2, 4–10, 13, 16, 18, and 19 of the ’350 patent. Claim 1 is independent and illustrative; it is reproduced below.

1. A method for network access control, the method comprising:
 - receiving audit data pertaining to a device that does not have access to a less-restricted subset of a network;
 - auditing the device in accordance with a security policy based at least in part on the audit data;
 - reconfiguring an access point to allow access to the less-restricted subset of the network in response to the security policy audit;
 - receiving updated audit data pertaining to the device subsequent to reconfiguring the access point; and
 - monitoring continued compliance of the device with the security policy using the updated audit data.

Ex. 1101, 15:57–16:8.

F. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability (Pet. 3, 20–74):

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1, 2, 4, 5, 16	103	Krantz ¹
6–10, 13, 18, 19	103	Krantz, Herrmann ²

In support of its unpatentability arguments, Petitioner relies on the declaration of Henry Houh, Ph.D. (Ex. 1103).

II. ANALYSIS

A. Legal Standards

In *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1 (1966), the Supreme Court set out a framework for assessing obviousness under 35 U.S.C. § 103 that requires consideration of four factors: (1) the “level of ordinary skill in the pertinent art,” (2) the “scope and content of the prior art,” (3) the “differences between the prior art and the claims at issue,” and (4) if in evidence, “secondary considerations” of non-obviousness, such as “commercial success, long-felt but unsolved needs, failure of others, etc.” *Id.* at 17–18. “While the sequence of these questions might be reordered in any particular case,” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 407 (2007), the U.S. Court of Appeals for the Federal Circuit has repeatedly emphasized that “it is error to reach a conclusion of obviousness until all those factors are considered,” *WBIP, LLC v. Kohler Co.*, 829 F.3d 1317, 1328 (Fed. Cir. 2016). Because Patent Owner does not address objective evidence of non-obviousness, we focus solely on the first three *Graham* factors.

¹ US 2004/0111520 A1, published June 10, 2004 (Ex. 1105).

² US 2004/0107360 A1, published June 3, 2004 (Ex. 1106).

B. Level of Ordinary Skill in the Art

The level of ordinary skill in the pertinent art at the time of the invention is a factor in how we construe patent claims. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1312–13 (Fed. Cir. 2005) (en banc). It is also one of the factors we consider when determining whether a patent claim is obvious over the prior art. *See Graham*, 383 U.S. at 17–18.

Factors pertinent to a determination of the level of ordinary skill in the art include “(1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) educational level of active workers in the field.” *Envtl. Designs, Ltd. v. Union Oil Co. of Cal.*, 713 F.2d 693, 696–697 (Fed. Cir. 1983) (citing *Orthopedic Equip. Co. v. All Orthopedic Appliances, Inc.*, 707 F.2d 1376, 1381–82 (Fed. Cir. 1983)). “Not all such factors may be present in every case, and one or more of these or other factors may predominate in a particular case.” *Id.*

Petitioner contends that one 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. 1–2. 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. 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 assessment of the level of ordinary skill in the art, as it appears consistent with the ’350 patent and the asserted prior art. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

C. Claim Construction

We apply the same claim construction standard used in the federal courts—in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. § 282(b), which is articulated in *Phillips*. *See* 37 C.F.R. § 42.100(b). Under the *Phillips* standard, the “words of a claim ‘are generally given their ordinary and customary meaning,’” which “is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application.” *Phillips*, 415 F.3d at 1312–13.

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 [’350 patent],” so we “need not expressly construe the claim terms.” Pet. 7. Patent Owner argues to the contrary that we should construe the phrase “reconfiguring the communication port” as “to change the access point itself [rather than something else] in a way that the checked device is able to access the less-restricted portion of the protected network.” Prelim. Resp. 7–9. Patent

Owner also argues that we should construe the phrases “audit data pertaining to a device” and “auditing the device in accordance with a security policy” as “requir[ing] that the ‘audit data’ and ‘auditing’ . . . be expressly about the device” rather than “the user.” *Id.* at 9–12.

As discussed below, we are able to determine whether to institute review without resolving the construction of any claim terms. Accordingly, we need not and do not construe any terms expressly. *See Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms . . . that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

D. Asserted Obviousness over Krantz

Petitioner argues that claims 1, 2, 4, 5, and 16 would have been obvious over Krantz. Pet. 20–54; Prelim. Reply 1–7. Patent Owner disagrees. Prelim. Resp. 17–31, 33–45; Prelim. Sur-Reply 1–7. Based on the current record, we are not persuaded that Petitioner has established a reasonable likelihood of prevailing on this asserted obviousness ground with respect to any claim.

1. Overview of Krantz

Krantz is a U.S. patent application titled “Increasing the Level of Automation when Provisioning a Computer System to Access a Network.” Ex. 1105, 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.

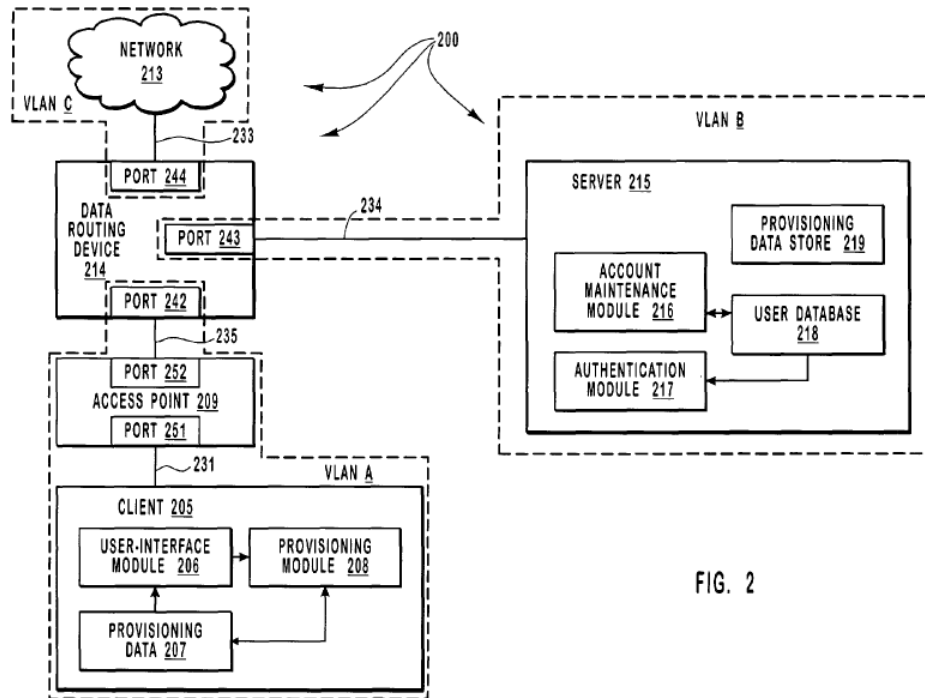


FIG. 2

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. Analysis of Claim 1

a) Disputed Limitation: “Auditing the Device in Accordance with a Security Policy Based at Least in Part on the Audit Data”

Claim 1 recites “auditing the device in accordance with a security policy based at least in part on the audit data.” Ex. 1101, 16:1–2. Petitioner contends that Krantz teaches or suggests this limitation. Pet. 31–35. Patent Owner disagrees. Prelim. Resp. 27–30.

Petitioner argues that the '350 patent “explains that ‘the security policies may include requirements for user identification[] such as usernames and passwords, configuration requirements relating to the configuration of Access Device 230[,] application requirements relating to applications running on Access Device 230, or the like.’” Pet. 32 (quoting Ex. 1101, 6:40–45). According to Petitioner, Krantz teaches the use of a security policy because it discloses authorizing a client for access to a network using EAP messages, such as EAP-TLS and EAP-MSCHAP V2. *Id.* at 32–34. Patent Owner argues that Krantz’s teaching of authorizing clients using EAP messages relates only to user authentication, which the '350 patent describes as outside the scope of applying a security policy. Prelim. Resp. 27–30.

We agree with Patent Owner. The '350 patent distinguishes between user authentication using a username and password and application of a security policy. Ex. 1101, 1:35–39 (“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.”), 1:45–48 (“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.”). Although the '350 patent describes both user authentication and application of a security policy 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, user

authentication in the '350 patent constitutes the application of a security policy.

Petitioner relies on Krantz's disclosure of user authentication as a teaching or suggestion to audit a device in accordance with a security policy. Petitioner first argues that Krantz teaches applying a security policy because Krantz discloses "that access to the network may be controlled by 'configuration settings,' which can include 'supported types of encryption' or 'supported types of authentication,' which can include an indication for EAP, which is short for 'Extensible Authentication Protocol.'" Pet. 32–33 (quoting Ex. 1103 ¶ 89; Ex. 1105 ¶¶ 66–67). But Krantz teaches that EAP 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. 1105 ¶ 71. As noted above, however, according to the '350 patent, user authentication and application of a security policy are separate processes.

Petitioner also argues that Krantz teaches auditing a device in accordance with a security policy because it discloses "that 'the server may authorize the client for at least partial access to the second network . . . and/or may deny access to the second network and authorize the client for at least partial . . . access to the first network.'" Pet. 33 (quoting Ex. 1105 ¶ 16). Petitioner does not explain within this argument why the mere act of authorizing or denying access to a network constitutes auditing the device in accordance with a security policy. *Id.* Moreover, Krantz teaches that the decision of whether to authorize or deny access is "[b]ased on the credentials" that the client sends to the server. Ex. 1105 ¶ 16. The record contains unopposed testimony that the term "credentials" would be understood by a person of ordinary skill in the art as "refer[ring] to username

and password credentials.” Ex. 2001 ¶ 58. Moreover, Krantz states that its “credentials” include a “user-identifier and password” that are “compare[d] . . . to entries in [a] user database.” Ex. 1105 ¶ 76.

Thus, Petitioner has not shown sufficiently that Krantz teaches the step of auditing the device in accordance with a security policy.

b) Conclusion Regarding Claim 1

Based on the current record, we determine that Petitioner has not shown that there is a reasonable likelihood that Petitioner will prevail in demonstrating that claim 1 is unpatentable as obvious in view of Krantz.

3. Claims 2, 4, 5, and 16

Petitioner argues that claims 2, 4, 5, and 16 would have been obvious over Krantz. Pet. 48–54. Each of these claims “incorporate[s] by reference all the limitations of” claim 1, because each depends from claim 1.

35 U.S.C. § 112 ¶ 4 (2010); Ex. 1101, 16:9–11, 16:15–20, 16:48–50. As discussed above, however, Petitioner has not shown sufficiently that Krantz teaches or suggests every limitation of claim 1. Accordingly, Petitioner has not shown that there is a reasonable likelihood that Petitioner will prevail in demonstrating that any of claims 2, 4, 5, and 16 is unpatentable as obvious in view of Krantz.

E. Asserted Obviousness over Krantz and Herrmann

Petitioner argues that claims 6–10, 13, 18, and 19 would have been obvious over the combination of Krantz and Herrmann. Pet. 55–74; Prelim. Reply 1–7. Patent Owner disagrees. Prelim. Resp. 31–45; Prelim. Sur-Reply 1–7.

1. Overview of Herrmann

Herrmann is a U.S. patent application titled “System and Methodology for Policy Enforcement.” Ex. 1106, 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. Analysis

Each of claims 6–10, 13, 18, and 19 depends indirectly from claim 1. Ex. 1101, 16:20–33, 16:39–41, 16:53–59. Accordingly, each incorporates all the limitations of claim 1. 35 U.S.C. § 112 ¶ 4 (2010). As discussed above, Petitioner has not shown sufficiently that Krantz teaches or suggests all the limitations of claim 1. In addition, in arguing for the obviousness of claims 6–10, 13, 18, and 19 over the combination of Krantz and Herrmann, Petitioner does not argue that Herrmann teaches or suggests any of the limitations of claim 1. Pet. 55–74. Accordingly, Petitioner has not shown sufficiently that either Krantz or Herrmann teaches or suggests the limitations of any of claims 6–10, 13, 18, and 19.

III. CONCLUSION

For the reasons set forth above, we determine that Petitioner has not demonstrated a reasonable likelihood of prevailing with respect to any challenged claim of the '350 patent. Accordingly, we do not institute *inter partes* review.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that, pursuant to 35 U.S.C. § 314, the Petition is denied, and no *inter partes* review is instituted.

IPR2024-00540
Patent 8,347,350 B2

FOR PETITIONER:

Scott M. Border
Joseph C. Masullo
WINSTON & STRAWN LLP
sborder@winston.com
jmasullo@winston.com

Patrick D. McPherson
Patrick Muldoon
David C. Dotson
DUANE MORRIS LLP
PDMcPherson@duanemorris.com
PCMuldoon@duanemorris.com
DCDotson@duanemorris.com

FOR PATENT OWNER:

Brian R. Michalek
Joseph M. Kuo
SAUL EWING LLP
brian.michalek@saul.com
joseph.kuo@saul.com