

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
U.S. Patent No. 8,347,350

REQUEST FOR DIRECTOR REVIEW

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. ARGUMENT	2
A. THE PANEL OVERLOOKED THAT USER AUTHENTICATION MAY BE PART OF THE APPLICATION OF A SECURITY POLICY	2
B. PETITIONERS' EVIDENCE THAT KRANTZ DISCLOSES A SECURITY POLICY AUDIT BASED ON USER AUTHENTICATION IS DISPOSITIVE	7
C. THE PETITION INCLUDES EVIDENCE THAT KRANTZ DISCLOSES LIMITATION [1.2] EVEN UNDER THE PANEL'S RESTRICTIVE READING OF THE '350 PATENT.....	8

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Baxalta Inc. v. Genentech, Inc.</i> , 972 F.3d 1341 (Fed. Cir. 2020)	5
<i>Gemtron Corp. v. Saint-Gobain Corp.</i> , 572 F.3d 1371 (Fed. Cir. 2009)	12, 14
<i>Icon Health & Fitness, Inc. v. Strava, Inc.</i> , 849 F.3d 1034 (Fed. Cir. 2017)	12, 14
<i>Littelfuse, Inc. v. Mersen USA EP Corp.</i> , 29 F.4th 1376 (Fed. Cir. Apr. 4, 2022)	1, 4, 5
<i>Mars, Inc. v. H.J. Heinz Co., L.P.</i> , 377 F.3d 1369 (Fed. Cir. 2004)	3
<i>Omega Eng'g, Inc v. Raytek Corp.</i> , 334 F.3d 1314 (Fed. Cir. 2003)	6
<i>Ortho-McNeil Pharm. v. Mylan Lab'ys, Inc.</i> , 520 F.3d 1358 (Fed. Cir. 2008)	6
<i>SanDisk Corp. v. Memorex Products, Inc.</i> , 415 F.3d 1278 (Fed. Cir. 2005)	3
<i>Wright Med. Tech., Inc. v. Osteonics Corp.</i> , 122 F.3d 1440 (Fed. Cir. 1997)	5
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022)	13
Other Authorities	
37 C.F.R. § 42.65(a)	13

I. INTRODUCTION

Petitioners Cisco Systems, Inc. and Fortinet, Inc. (“Petitioners”) respectfully request that the Director vacate the Board’s Preliminary Decision (“Decision” or “ID”) denying institution of *inter partes* review of U.S. Patent No. 8,347,350 (“the ’350 Patent”) and institute review.

Vacatur of the Decision is warranted in light of the Board’s abuse of discretion in two critical findings.

First, the Panel erroneously held that “user authentication and application of a security policy are accomplished in separate processes.” ID at 13. This finding and implicit construction overlooks the ’350 Patent’s express teaching that: “[i]n some embodiments, Authenticate User Step 440 is considered part of the security audit.” *See* Pet. at 27, 35 (citing Ex.1101, 12:2-4). This embodiment—encompassed by dependent claim 5 and others—unequivocally shows that user authentication may be accomplished as part of the security policy recited in claim 1. *Littelfuse, Inc. v. Mersen USA EP Corp.*, 29 F.4th 1376, 1380 (Fed. Cir. Apr. 4, 2022) (“[A]n independent claim is broader than a claim that depends from it, so if a dependent claim reads on a particular embodiment of the claimed invention, the corresponding independent claim must cover that embodiment as well.”)

Second, the Panel’s finding that the Petition’s evidence regarding limitation [1.2] is solely related to user authentication is also incorrect. Not only does this

finding ignore that user authentication may be accomplished as part of the security policy, it also overlooks the compelling evidence that Krantz audits actual **devices** in accordance with a security policy based on audit data beyond mere user authentication. This includes evaluating and authorizing a device based on operating system credentials, machine information, and encryption protocols, each of which is an important element in the application of Krantz's comprehensive security policy.

Given these errors, Petitioners respectfully request that the Director vacate the Decision and institute *inter partes* review of the '350 Patent.

II. ARGUMENT

A. The Panel Overlooked that User Authentication May Be Part of the Application of a Security Policy

In the Decision, the analysis by the Panel rested entirely on its determination and implicit construction that user authentication is a **separate process step** from the application of a security policy as described and claimed in the '350 Patent. ID at 12-13. In particular, the Panel explained:

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.

ID at 12-13 (emphasis added).

Although the Panel was correct that the '350 Patent describes **an embodiment** where “user authentication and application of a security policy . . . are accomplished in separate process steps,” the Panel erred in not acknowledging a separate embodiment where user authentication (among other things) is **part of**—and not separate from—the security policy audit. Indeed, the '350 Patent explains that “[in] some embodiments, Authenticate User Step 440 **is considered part of the security policy audit.**” Ex.1101, 12:2-4; *see also id.* 11:34-42 (“In optional Authenticate User Step 440, **Policy Auditor 325 authenticates the identity of Access Device 230 and/or a user of Access Device 230. This authentication may be required by a member of Security Policies 330A-330B[.]**”); *see* Pet. at 27, 35.

In addition, dependent Claims 5 and 16 confirm that user authentication can be part of the application of a security policy recited in claim 1. Limitation [1.2] recites “*auditing the device in accordance with a security policy based at least in part on the audit data.*” Ex.1101, Claim 1. Dependent claim 5 specifies “*wherein the security policy includes¹ authentication of the user of the device.*” Claim 5

¹ *SanDisk Corp. v. Memorex Products, Inc.*, 415 F.3d 1278, 1284 (Fed. Cir. 2005)

(“As a patent law term of art, ‘includes’ means ‘comprising.’”); *Mars, Inc. v. H.J.*

therefore encompasses the embodiment described in the '350 Patent at 12:2-4—i.e., where “*authentication of the user*” and the application of a “*security policy*” are part of the same process, which means claim 1 **must encompass** that reading as well. *Littelfuse*, 29 F.4th at 1380 (“[A]n independent claim is broader than a claim that depends from it, so if a dependent claim reads on a particular embodiment of the claimed invention, the corresponding independent claim must cover that embodiment as well.”) Likewise, claim 16—which also depends from claim 1—specifies “*wherein the security policy audit is based at least in part on the information concerning an identity of a user of the device.*” Ex.1101, Claim 16. These dependent claims confirm that “*auditing the device in accordance with a security policy*” of claim 1 encompasses user authentication and other techniques that authorize access based on “*audit data*” concerning the user of the device. Pet. at 32, 53-54.

Heinz Co., L.P., 377 F.3d 1369, 1375–76 (Fed. Cir. 2004) (“Comprising is a term of art used in claim language which means that the named elements are essential, but other elements may be added”) (citation omitted). Thus, while “*authentication of the user*” is a necessary element of the “*security policy*” of claim 5, there could be other “*security policy*” techniques.

The Federal Circuit’s ruling in *Littelfuse* is instructive. In that case, independent claims 1 and 10 described a “fuse end cap” with three components: a mounting cuff, a terminal, and a fastening stem. *Littelfuse*, 29 F.4th at 1379-80. Dependent claims 8, 9, 19, and 20 further specified that this “fuse end cap” be made “from a single, contiguous piece of conductive material.” *Id.* at 1380.

The district court initially interpreted claims 1 and 10 to only cover “multi-piece construction[s].” *Id.* However, the Federal Circuit reversed this decision, explaining that the dependent claims’ “recitation of a single-piece apparatus in claims 8, 9, 19, and 20 is persuasive evidence that claims 1 and 10 also cover a single-piece apparatus.” *Id.* The *Littelfuse* court emphasized that “if a dependent claim reads on a particular embodiment of the claimed invention, the corresponding independent claim must cover that embodiment as well.” *Id.* (citing *Baxalta Inc. v. Genentech, Inc.*, 972 F.3d 1341, 1346 (Fed. Cir. 2020) (“The district court’s construction [of the independent claim] which excludes these explicitly claimed embodiments [in the dependent claims] is inconsistent with the plain language of the claims.”); *Wright Med. Tech., Inc. v. Osteonics Corp.*, 122 F.3d 1440, 1445 (Fed. Cir. 1997) (“[W]e must not interpret an independent claim in a way that is inconsistent with a claim which depends from it.”))

In the present case, claim 5 specifies “wherein the security policy includes authentication of the user of the device,” and limitation [1.2] recites “auditing the

*device in accordance with **a security policy** based at least in part on the audit data.”*

Therefore, the “*security policy*” of claim 1 must at least encompass the “*authentication of the user*”—any interpretation holding otherwise would render claim 5 meaningless. *Ortho-McNeil Pharm. v. Mylan Lab’ys, Inc.*, 520 F.3d 1358, 1362 (Fed. Cir. 2008) (“[T]his court strives to reach a claim construction that does not render claim language in dependent claims meaningless.”) Because independent claim 1 is presumed both different from and broader than dependent claim 5, the “*security policy*” of claim 1 may encompass techniques other than, and in addition to, “*authentication of the user*.”

Finally, claims in patents related to the ’350 Patent (and challenged by Petitioners in related IPRs) also demonstrate beyond a doubt that user authentication is encompassed by the claimed “*security policy*.” Claim 1 of the related ’450 Patent, for example, recites “*a method for **applying a security policy** . . . comprising: **performing an authentication of a device***” and dependent claim 5 further recites “*wherein the **authentication identifies the user of the device**.*” See IPR2024-00676, Ex.1401. *Omega Eng’g Inc v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003) (“[W]e presume, unless otherwise compelled, that the same claim term in the same patent or related patents carries the same construed meaning”)

Accordingly, the Panel’s finding and implicit construction that user authentication is “outside the scope of applying a security policy” as required in claim 1 is erroneous and Petitioners respectfully request it be vacated. ID at 12-13.

B. Petitioners’ Evidence that Krantz Discloses a Security Policy Audit Based on User Authentication Is Dispositive

In the analysis regarding limitation [1.1]—which recites “*receiving audit data pertaining to a device that does not have access to a restricted subset of a network*”—Petitioners explain that Krantz discloses several examples of “*audit data*,” including user-specific credentials (*e.g.*, user-identifier and password), which are audited by comparing entries in a “user database” so that the user of “client 205” in Krantz may become authorized. Pet. at 27 (citing Ex.1105, [0076] & Ex.1103, ¶79). Petitioners then explained that:

Krantz’s disclosure is consistent with the ’350 Patent’s description that audit data can be used to authenticate a user.” Ex.1101, 12:2-4 (“In some embodiments, **Authenticate User Step 440 is considered part of the security audit**”); *see also* Ex 1101, 11:34-42 (“In optional **Authenticate User Step 440**” the “**Policy Auditor 325 authenticates** the identity of Access Device 230 and/or a user of Access Device 230 . . . **the authentication may include receipt of a user name and a password** . . . or the like.”).

Pet. at 27. Petitioners therefore identified in Krantz the same kind of “*audit data*” described and claimed in the ’350 Patent.

For the analysis regarding limitation [1.2]—which recites “*auditing the device in accordance with a security policy based at least in part on the audit data*” and which the Panel found dispositive—Petitioners expressly referenced their analysis of Krantz auditing user credentials, Pet. at 31-32 and 35,² and further noted that the ’350 Patent’s disclosure provides 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. at 32 (citing Ex. 1101, 6:40-45 & Ex.1103, ¶¶83, 88). Petitioners also explained that protocols like EAP-TLS and EAP-MSChapV2 include techniques to authenticate and authorize users (and devices) seeking access. Pet. at 33-35.

Accordingly, because Krantz’s disclosure related to user authentication is within the scope of applying a “*security policy*,” this further demonstrates that the Panel erred in denying institution. ID at 12-13.

C. The Petition Includes Evidence that Krantz Discloses Limitation [1.2] Even Under the Panel’s Restrictive Reading of the ’350 Patent.

² Petitioners identified the same Krantz disclosure of comparing the user-identifier and password credentials to entries in a user database to satisfy dependent claims 5 and 16. Pet. at 53-54 (citing Ex.1105, [0076]).

Even under the Panel’s restrictive reading of claim 1 of the ’350 Patent—i.e., the finding and implicit construction that user authentication and application of a security policy must be accomplished in separate processes—the Petition included evidence that Krantz “*audit[s] the device in accordance with a security policy*” based on audit data other than user authentication, including evaluating and authorizing a device based on operating system credentials, machine information, authentication protocols, and encryption protocols.

Apart from describing user authentication and the exchange of user names and passwords as part of the application of a security policy (*see* Ex.1101, 6:38-47, 6:54-64, 12:2-4, claims 5, 16), the ’350 Patent broadly describes a security policy audit as requiring “configuration requirements related to the configuration of Access Device 230” or “application requirements relating to applications running on Access Device 230.” Ex.1101, 6:42-45. Other examples of a security policy audit described in the ’350 Patent include the audit of, among other things, “operating system status (version, updates, etc.), antivirus software status, information concerning devices connected to Access Device 230, Windows registry information, MAC address, IP addresses, cookies, status of applications executing on Access Device 230, or the like.” Ex.1101, 11:43-53. Critically, Petitioners explained that Krantz discloses some of these exact same examples of a security policy audit that addresses “*audit data*” other than those focused on user authentication, including operating-system

credentials (Pet. at 34 (citing Ex.1105, [0099] & Ex.1103, ¶90)) and **configuration settings** including supported types of encryption and supported types of authentication (Pet. at 32-34 (citing Ex.1105, [0066]-[0067], [0074], [0100], Ex.1116 [RFC2716] & Ex.1103, ¶89).

Nevertheless, in the Decision, the Panel adopted Patent Owner's erroneous **attorney argument** that Krantz use of EAP messages related only to user authentication:

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**. *Id.* at 12 (emphases added).

That finding, however, misapprehends or overlooks the **only evidence** of record. As demonstrated in detail below, Petitioners explained that both EAP-TLS and EAP-MSCHAPv2 are techniques disclosed in Krantz, *e.g.*, Pet. at 32-34, and further demonstrated how both EAP-TLS and EAP-MSCHAP V2 are used as techniques to authorize a **device**, not merely a user. *Id.*

For example, Petitioners explained that “[a]fter an EAP type is selected . . . **computer systems can attempt to authenticate with one another** through the

transfer of EAP messages . . . in accordance with the selected EAP type. For example, when EAP-TLS is selected, **client 205 may communicate with server 215** through a series of EAP messages in accordance with EAP-TLS **so as to be authenticated and possibly authorized to access resources located on VLAN C.**” Pet. at 33 (citing Ex.1105, [0068]) (emphases added). Petitioners then explained that “use of EAP-TLS (*e.g.*, Ex.1105, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate client devices,” Pet. at 33-34 (emphasis added), which was supported by testimony from Dr. Henry Houh, *see* Ex.1103, ¶ 89 (citing Krantz and Ex.1116, [RFC2716]). Accordingly, the arguments in the Petition were confirmed by Krantz’s own disclosure (i.e., “**computer systems** can attempt to authenticate with one another”; “**client 205** [a “*device*”] may communicate . . . **so as to be authenticated and possibly authorized**,” *see* Pet. at 33), its expert, Dr. Houh, and Exhibit 1116, all of which establish that EAP-TLS includes client “*device*” authentication and authorization techniques. Ex. 1103, ¶89 (citing Krantz and Ex.1116 [RFC2716]); *see* Pet. at 33-35.

Importantly, none of the evidence demonstrating EAP-TLS discloses “*device*” authentication and authorization techniques is addressed by Patent Owner’s own expert but is instead challenged only by Patent Owner’s attorney which cannot rebut Petitioners’ **evidence**. *Gemtron Corp. v. Saint-Gobain Corp.*, 572 F.3d 1371, 1380 (Fed. Cir. 2009) (“[U]nsworn attorney argument . . . is not evidence and cannot rebut

... admitted evidence[.]”); *Icon Health & Fitness, Inc. v. Strava, Inc.*, 849 F.3d 1034, 1043 (Fed. Cir. 2017) (“Attorney argument is not evidence.”).

Petitioners also demonstrated that EAP-MSCHAP V2 discloses client “*device*” authorization techniques. For example, the Petition explains that Krantz discloses that “[w]hen EAP-MSChap V2 is indicated, the MS Chap V2 Parameters element at line 67 can be included in a configuration sub-file to indicate **whether or not operating system credentials should be used for authentication.**” Pet. at 34 (citing Ex.1105, [0099] and Ex.1103 ¶90) (emphasis added). Despite this evidence, the Panel found that “[t]he 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.’” The Panel cited InfoExpress’s expert at paragraph 58 for this assertion, but this is classic *ipse dixit* testimony—testimony without any evidentiary underpinning—and should have been given little to no weight:

[A] POSITA would understand the authentication described in Krantz to be referring to usernames and passwords because Krantz uses the phrase “Operating System Credential”—a term used in the industry to refer to username and password credentials that are used to gain authorization to act on a system. This type of credentials would not be understood by a POSITA to refer to auditing a device, like the ’350 Patent recites.

Ex. 2105, ¶58. It is well-established that “[e]xpert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.” 37 C.F.R. § 42.65(a); *see also Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9, at 15-16 (PTAB Aug. 24, 2022) (precedential) (expert testimony entirely unsupported by underlying facts or data should be given little or no weight).

In contrast, Petitioners’ expert Dr. Houh relied not only on Krantz’s disclosure but also on Exhibit 1117 to support his opinion that Krantz’s credentials (“*audit data*”) encompass at least machine (“*device*”) credentials distinguishable from and in addition to user credentials. *See* Ex. 1103, ¶78 (explaining that such **credentials** “can include sending an **Extensible Authentication Protocol (“EAP”) Response/Identity message from the client to the server.** If the client is attempting to connect to a network via an access point, the EAP Response/Identity message may be encapsulated within some other type of message that can be transferred through the access point.” Ex.1105, [0018]. **Other audit data** provided by Krantz’s “*device*” may include, for example, “user-identifier[s] and password[s].” *Id.* [0076]).

Petitioners offered additional evidence demonstrating that EAP-TLS and EAP-MSCHAP V2 may be used in Krantz’s disclosed system to perform “*security policy*” audits specific to the “*device*.” Citing Dr. Houh’s testimony at paragraph 91 and Exhibit 1117 at 2, Petitioners explained that a POSITA would understand that

the techniques in Krantz (and described in the Petition) would be used to authenticate and authorize the **client 205**³ “*device*”—i.e., “*applying a security policy to the access device in response to the request.*” Pet. at 34-35 (citing, e.g., Ex.1117 at 2 and Ex.1103, ¶91). Analyzing Exhibit 1117, Dr. Houh testified that “EAP-TLS . . . **uses certificates for machine logon** and user logon. The computer first authenticates to the network **using a machine certificate.**” Ex.1103, ¶91 (citing Ex. 1117, at 2) (emphases added). With respect to MSChap V2, Dr. Houh credited statements in Exhibit 1117 explaining that “**PEAP-MSCHAPv2 uses machine** and user **credentials for authentication.**” Moreover, none of this evidence demonstrating that EAP-TLS and EAP-MSCHAPv2 disclose “*device*” authentication and authorization techniques was rebutted or even addressed by Patent Owner’s own expert but was instead challenged only by Patent Owner’s attorney—again, this cannot rebut Petitioners’ evidence. *Gemtron*, 572 F.3d at 1380; *see also Icon Health & Fitness*, 849 F.3d at 1043.

Finally, in the Petition, relying on the ’350 Patent disclosure that “security policies may include . . . **configuration requirements relating to the configuration of Access Device 230,**” Petitioners explained that Krantz likewise includes a disclosure that access to the network may be controlled by “configuration settings,” which can include “supported types of encryption” or “supported types of

³ Client 205 is a “device,” not a user. *See, e.g.,* Ex.1105, Fig. 2.

authentication.” Pet. at 32-33 (citing Ex.1105, [0066]-[0067]; Ex.1103, ¶89). Put another way, “configuration settings” including “supported types of encryption”—which pertain to the “device” in Krantz—are precisely the kind of implementation encompassed by the ’350 Patent’s disclosure of “configuration requirements relating to the configuration of Access Device 230.” Ex. 1101, 6:40-45. Petitioners’ evidence on this issue—Krantz’s disclosure and Dr. Houh’s testimony—is un rebutted, as Dr. Cole does not address this argument, and Patent Owner’s attorneys’ argument—i.e., that “Petitioners’ configurations settings argument is again based on user authentication”—is unsupported attorney argument and the sole rebuttal to Dr. Houh’s testimony. The Panel, however, overlooked or misapprehended Krantz’s disclosure and Dr. Houh’s testimony in favor of Patent Owner’s conclusory and unsupported attorney argument.

Thus, even using the Panel’s restrictive reading of the ’350 Patent that “user authentication and application of a security policy are accomplished in separate processes,” the Petition includes evidence that demonstrates that Krantz audits a device in accordance with a security policy based on “*audit data*” other than user authentication, including based on “*audit data*” related to the device, such as operating system credentials, machine information, authentication protocols, and encryption protocols.

Dated: October 18, 2024

Respectfully Submitted,

/Scott M. Border/

Scott M. Border

Reg. No. 77,744

Winston & Strawn LLP

1901 L Street, N.W.

Washington, D.C. 20036

T: 202-282-5054

sborder@winston.com

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I hereby certify that on this 18th day of October, 2024, I caused to be served a true and correct copy of the foregoing on the following:

Brian R. Michalek (Reg. No. 65,816)
Saul Ewing LLP
brian.michalek@saulewing.com

Joseph M. Kuo (Reg. No. 38,943)
Saul Ewing LLP
joseph.kuo@saulewing.com

Brian Landry (Reg. No. 62,074)
Saul Ewing LLP
Brian.Landry@saulewing.com

Dated: October 18, 2024

Respectfully Submitted,

/Scott M. Border/
Scott M. Border
Reg. No. 77,744
Winston & Strawn LLP
1901 L Street, N.W.
Washington, D.C. 20036
T: 202-282-5054
sborder@winston.com