

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
U.S. Patent No. 8,117,645

REQUEST FOR DIRECTOR REVIEW

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. ARGUMENT	2
A. THE PETITION INCLUDES SEVERAL EXAMPLES THAT DEMONSTRATES THAT KRANTZ DISCLOSES THE <i>FORMULATE AN AUDIT REQUEST</i> LIMITATION.	2
1. The Panel Overlooked that Krantz’s Disclosure of User Authentication May Be Part of the Application of a Security Policy Audit	4
2. The Panel Overlooked that Krantz’s Disclosure of Configuration Information Including Operating System and Encryption Protocols May Be Part of the Application of a Security Policy Audit	9

TABLE OF AUTHORITIES

Page(s)

Cases

<i>Baxalta Inc. v. Genentech, Inc.</i> , 972 F.3d 1341 (Fed. Cir. 2020).....	8
<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)	7, 8
<i>Lockwood v. Am. Airlines, Inc.</i> , 107 F.3d 1565 (Fed. Cir. 1997).....	11
<i>Omega Eng'g Inc v. Raytek Corp.</i> , 334 F.3d 1314 (Fed. Cir. 2003).....	6
<i>Vivint, Inc. v. SB IP Holdings LLC</i> , IPR2022-01365, Paper 23 (PTAB Apr. 24, 2024).....	11
<i>Wright Med. Tech., Inc. v. Osteonics Corp.</i> , 122 F.3d 1440 (Fed. Cir. 1997).....	8

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. 8,117,645 (“the ’645 Patent”) and institute review.

Vacatur of the Decision is warranted in light of the Board’s abuse of discretion in finding that the Krantz reference did not disclose the “*formulate an audit request*” limitation. Specifically, the Panel was misled by the Patent Owner’s arguments that Krantz only discloses authentication, and thus the Panel overlooked the broad overlap between Krantz’s disclosure that the information that can be used for authentication is the same information that can be used for auditing a security policy in the ’645 Patent. For example, Krantz discloses that a **device** can be authenticated and/or authorized by checking the operating system of the device or checking the required encryption protocol of the device, while the ’645 Patent discloses that auditing a security policy can including checking the operating system of the device or checking the encryption protocol of the device.

Thus, the Panel’s finding that the Petition’s evidence regarding limitation [1.3]—“*to formulate an audit request*”—“related solely to authentication” is incorrect. This finding overlooks the compelling evidence that Krantz audits actual **devices** in accordance with a security policy based on audit data, *e.g.*, operating

system and encryption protocol, separate from and beyond mere user authentication using user identifiers and passwords. The broad disclosure of the '645 Patent includes evaluating and authorizing a device based on, for example, operating system credentials, machine information, encryption protocols, and configuration settings, each of which is an important element in the application of Krantz's comprehensive security policy.

Thus, it was an abuse of discretion for the Panel to hold that Krantz does not disclose the “*formulate an audit request*” limitation. Petitioners respectfully request that the Director vacate the Decision and institute *inter partes* review of the '645 Patent.

II. ARGUMENT

A. The Petition Includes Several Examples that Demonstrates That Krantz Discloses the *formulate an audit request* Limitation.

The Petition describes that the '645 Patent broadly discloses that a “security audit typically includes determining if access device 230 satisfies requirements of the security policy” and that in some embodiments “authenticate user step 440 is considered party of the security policy audit.” Pet. at 38 (citing to EX.1301, 11:67-12.6. Based on this broad disclosure, the Petition identifies several examples in Krantz of the “*formulate an audit request*” limitation based on information requested by server 215 for client device 205, including:

- Server 215 may request that the client 205 provide a password that is associated with a user identifier. Pet. at 38 (citing Ex.1305, [0074]).
- Client 205 and server 215 exchange EAP-messages to pass certificates, keys, and supported cyber suites. Pet. at 38 (citing Ex.1305, [0074]).
- Depending on the EAP type, other credential information may also be exchanged between client 205 and server 215. Pet. at 38 (citing Ex.1305, [0074]).
- Server 215 can send an EAP-Notification which can include conditions a user must satisfy to become authorized to access resources located on VLAN C. Pet. at 39 (citing Ex.1305, [0074]).

Any one of the examples identified above satisfies the “*formulate an audit request*” limitation.

Further, with regard to limitation [1.5]—“*evaluate device information received from the device in response to the audit request*”—the Petition identified the type of information that could be provided in response to the audit request:

- Certificates, keys, and supported cyber suites. Pet. at 42 (citing Ex.1305, [0074]).
- Password and user identifier. Pet. at 42 (citing Ex.1305, [0074]).
- Configuration settings which can include supported types of encryption and supported types of authentication and use of the EAP protocol and operating systems credentials. Pet. at 43-44 (citing EX.1305, [0066]-[0067], [0099]-[100]).

The various types of information above demonstrate that the information received in response to the audit request disclosed in Krantz is not used solely for

user authentication. However, the Patent Owner argued that server 215 in Krantz is “only for authentication,” and the Panel agreed. In doing so, the Panel failed to appreciate that not all information identified above related to user authentication, but instead some related to device authentication and authorization. ID at 14 (“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.) This finding by the Board is factually unsupported, because each of the examples are the same types of information that is included in a security policy that is audited in the ’645 Patent.

1. The Panel Overlooked that Krantz’s Disclosure of User Authentication May Be Part of the Application of a Security Policy Audit

The Petition explains that the ’645 Patent describes that the security policy may proscribe up-to-date virus software and encryption protocols, (Ex.1301, 2:16-27), include requirements related to user identification and passwords or configuration requirements related to the access device (such as aspects of the operating system), (Ex.1301, 6:38-52), or authenticate an access device (or user) of the device. Ex.1301, 10:36-41, 12:2-6; Pet. at 6. Thus, auditing the security policy would include reviewing any of the above information, including user identification and a password.

In the Decision, the analysis by the Panel focused on “user authentication” and is colored by its determination and implicit construction that user authentication is a **separate process step** from the security policy audit claimed and described in the ’645 Patent. ID at 13-14. The Panel explained:

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.**

ID at 14 (emphasis added).

Initially, this determination is inconsistent with its own finding one-page earlier “that authentication can be part of a security policy audit.” ID at 13 (citing Pet. 38, Ex.1301, 11:67-12:6). And although the Panel was correct that the ’645 Patent describes **an embodiment** where “both user authentication and security auditing. . . is accomplished in separate process steps,” the Panel erred in not acknowledging that the ’645 Patent’s disclosure of “auditing a security policy” includes a separate embodiment where user authentication (among other things) **is**

part of—and not separate from—the security policy audit. ID at 14 (citing Ex.1301 at 10:38-41. Indeed, the ’645 Patent explains that “[in] some embodiments, Authenticate User Step 440 **is considered part of the security policy audit.**” Ex.1301, 12:4-6; *see also id.* 11:35-42 (“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 38, 52-53.

This understanding of the ’645 Patent—*i.e.*, that an “*audit request*” in the patented system can encompass both a request for user authentication and device information—is confirmed by Patents related to the ’645 Patent, as explained in the related ’350 Patent Request for Director Review in IPR2024-00540. For example, dependent Claims 5 and 16 of the related ’350 Patent¹, a continuation of the ’645 Patent, confirm that user authentication can be part of the application of a security policy audit. Limitation [1.2] of the ’350 Patent 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 includes*

¹ *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”)

authentication of the user of the device.” Claim 5 of the ’350 Patent therefore encompasses the embodiment described in the ’645 Patent at 12:4-6—i.e., where “*authentication of the user*” and a “*security policy*” audit 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 of the ’350 Patent—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.*” See IPR2024-00540, Ex.1101, Claim 16. These dependent claims in the related ’350 Patent confirm that “*auditing the device in accordance with a security policy*” as claimed in that patent at least encompasses user authentication and other techniques that authorize access based on “*audit data*” concerning the user of the device. See IPR2024-00540, Petition at 38, 53-54.

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, Inc. v. Mersen USA EP Corp.*, 29 F.4th 1376, 1379-80 (Fed. Cir. Apr. 4, 2022). 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.”)).

Because the ’645 Patent broadly discloses that a security policy includes authentication of the user of the device, the Panel’s statement that authenticating and auditing are “two processes that are expressly distinguished in the specification of the ’645 Patent” is simply not accurate. Similarly, the Panel faulted Petitioners for identifying the same or similar disclosures in Krantz for “*authentication*

information” recited in limitation [1.1] and “*device information*” recited in limitation [1.5] because it failed to appreciate the overlap in this information that is described in the ’645 Patent. ID at 15. Thus, although claim 1 of the 645 Patent may require separate “*evaluation of the device*” and “*authentication*” steps, the specification and the claims of the ’645 Patent (and related Patents) demonstrate that the “*audit*” data sought by the claimed “*gatekeeper*” specifically encompasses both “*authentication information*” and “*device information*.”

2. The Panel Overlooked that Krantz’s Disclosure of Configuration Information Including Operating System and Encryption Protocols May Be Part of the Application of a Security Policy Audit

The Petition included evidence that Krantz “*formulates an audit request*” based on a request for audit data other than user authentication, including evaluating and authorizing a device, e.g., a client, based on operating system credentials, machine information, and configuration settings such as authentication protocols and encryption protocols.

For example, the Petition explained that “[i]t may also be that client 205 and server 215 **exchange EAP-messages to pass certificates, keys, and supported cipher suites**. Depending on the EAP type, **other credential information may also be exchanged between client 205 and server 215.**” Pet. at 38. The Petition further explained that:

[S]erver 215 can send an EAP-Notification ... [which] can [] **include conditions a user must satisfy** [*audit request*] to become authorized to access resources located on VLAN C (e.g., signup, renewal, etc.). If client 205 is to perform downloads by accessing a provided URI, access point 209 can enable the transfer of HTTP packets for port 251. Server 215 may send commands to access point 209 to cause access point 209 to enable the transfer of HTTP packets.”

Pet. at 39 (citing Ex.1305, [0078]; Ex.1303, ¶98) (emphasis added). The Petition further explained that as part of the back-and-forth negotiations (via packets) with the client related to the client’s configuration settings, that “when the configuration of EAP is indicated, further numeric values . . . **can be included in a LCP packet to indicate the specific EAP type of authentication that is desired** [i.e., “*formulate*” the audit request].” Pet. at 39-40.

Apart from describing user authentication and the exchange of user names and passwords as **part of** the application of a security policy (*see* Ex.1301, 6:40-45, 6:53-59, 11:35-42), the ’645 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.1301, 6:38-45. Other examples of a security policy audit described in the ’645 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.1301, 11:35-42. Accordingly, Petitioners explained that Krantz discloses some of these exact same examples of “*device information*” in response to the “*audit request*” other than those focused on authentication, including operating-system credentials (Pet. at 44 (citing Ex.1305, [0099] & Ex.1303, ¶111)) and **configuration settings** including supported types of encryption. Pet. at 43-44 (citing Ex.1305, [0066]-[0067], [0074], [0099]-[0100]; Ex.1316, 2 [RFC2716]; Ex.1303, ¶110).

Critically, the Panel never addresses Krantz’s disclosure regarding assessing “configuration settings,” which is precisely the same kind of “*audit*” described in the ’645 Patent. Ex.1301, 6:38-45 (“The security policies may include requirements for . . . configuration requirements related to the configuration of Access Device 230.”) To the extent the Panel would assert that Krantz was required to describe in more detail what those “configuration settings” require, such an assertion “would require greater particularity of the prior art than is provided in the patent, which is an incorrect approach to obviousness.” *Vivint, Inc. v. SB IP Holdings LLC*, IPR2022-01365, Paper 23 at 36-37 (PTAB Apr. 24, 2024) (citing *Lockwood v. Am. Airlines, Inc.*, 107 F.3d 1565, 1570 (Fed. Cir. 1997)).

Nevertheless, in the Decision, the Panel found that “Petitioner’s contentions for ‘formulat[ing] an audit request’ related solely to authentication.” ID. at 14. That finding, however, misapprehends or overlooks the **only evidence** of record. As

demonstrated in detail above and below, Petitioners identified several “configuration settings” or device-specific credentials that were requested of the device. Pet. at 39-40. Petitioners further explained that both EAP-TLS and EAP-MSCHAPv2 are techniques disclosed in Krantz, (*e.g.*, Pet. at 44-45), and further demonstrated how both EAP-TLS and EAP-MSCHAP V2 are used as techniques to authorize a **device**, not merely a user. Pet. at 44-45 (citing Ex.1317, 2; Ex.1303, ¶112).

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 43 (citing Ex.1305, [0068]) (emphases added). Petitioners then explained that “use of EAP-TLS (*e.g.*, Ex.1305, [0067]-[0074], [0100]) was a known authentication protocol that would be used to authenticate **client devices**,” Pet. at 43-44 (emphasis added), which was supported by testimony from Dr. Henry Houh, *see* Ex.1303, ¶110 (citing Krantz and Ex.1316, [RFC2716]).

Importantly, none of the evidence demonstrating that EAP-TLS discloses “*device*” 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 also 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** [*“device information”*] **should be used for authentication.**” Pet. at 44 (citing Ex.1305, [0099] and Ex.1303 ¶111) (emphasis added). Importantly, neither Patent Owner nor its expert addressed this disclosure in Krantz, so Dr. Houh’s testimony on this issue is un rebutted.

Indeed, Petitioners’ expert Dr. Houh relied not only on Krantz’s disclosure but also on Exhibit 1317 to support his opinion that Krantz’s credentials (“*requested audit*” data and “*device information*”) encompass at least machine credentials (“*device information*”) distinguishable from and in addition to user credentials. Pet. at 44. In particular, Petitioners explained:

Krantz also explains that EAP-TLS and EAP-MSCHAP V2 can both be required from a client seeking access and authorization using encryption techniques. Ex.1305, [0099]; Accordingly, a POSITA would understand that each of the above techniques in Krantz would be used

to both audit the device (and authenticate) the client 205 (“*evaluat[ing] device information received from the device.*”) which can be in response to an audit request. Ex.1317, 2 (“EAP-TLS. TLS (SSL) is the encryption method used to protect the EAP exchange. In Windows, TLS uses certificates for machine logon and user logon. The computer first authenticates to the network using a machine certificate; this allows for computer policies in the Active Directory and SMS packages to be applied before a user logs on. ... In Windows, PEAP supports MS-CHAPv2 in addition to TLS. PEAP-MSCHAPv2 uses machine and user credentials for authentication. MSCHAPv2 uses rotating keys **to encrypt** both machine and user password hashes. Certificates are still required for the authentication sever (IAS) and are used for server-to-client authentication; credentials, carried inside MSCHAPv2, are used for client-to-server authentication.”)

Pet. at 44 (citing Ex.1303, ¶112; Ex.1305, [0099], [0111]; Ex.1317, 2). Petitioner explained that “[t]his information was ‘*device information*’ because it includes information unique, specific to, or related to the ‘*device.*’” Pet. at 44 n3. 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 ’645 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 authentication.” Pet. at 43-44 (citing Ex.1305, [0066]-[0067]; Ex.1303, ¶110). 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 ’645 Patent’s disclosure of “configuration requirements relating to the configuration of Access Device 230.” Ex. 1301, 6:38-45. Petitioners’ evidence on this issue—Krantz’s disclosure and Dr. Houh’s testimony—is unrebutted, 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,” POPR at 34—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 ’645 Patent, the Petition includes evidence that demonstrates that Krantz “*formulates an audit request*” that includes “*audit*” data other than user authentication, including “*audit data*” related to the device, such as operating system credentials, machine information, authentication protocols, configurations settings, and encryption protocols.

Dated: November 12, 2024

Respectfully Submitted,

/Scott M. Border/

Scott M. Border

Reg. No. 77,744

Winston & Strawn LLC

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 12th day of November, 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@saul.com

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

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

Dated: November 12, 2024

Respectfully Submitted,

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