Trials@uspto.gov
Tel: 571-272-7822

Paper 7
Entered: December 1, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

COMMERCE BANCSHARES, INC., COMPASS BANK, and FIRST NATIONAL BANK OF OMAHA,
Petitioners,

v.

INTELLECTUAL VENTURES II LLC,
Patent Owner.

Case IPR2014-00801
Patent 6,715,084 B2

Before KRISTEN L. DROESCH, JENNIFER S. BISK, and JUSTIN BUSCH, *Administrative Patent Judges.*

BISK, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

INTRODUCTION

A. Background

Commerce Bancshares, Inc., Compass Bank, and First National Bank of Omaha (collectively "Petitioner") filed a Petition (Paper 1, "Pet." or "Petition") requesting an *inter partes* review of claims 1–33 (the "challenged claims") of U.S. Patent No. 6,715,084 B2 (Ex. 1001, "the '084 patent").

Intellectual Ventures II LLC ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

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

After considering the Petition and Preliminary Response, we determine that Petitioner has established a reasonable likelihood of prevailing on claims 26, 28, and 30–33 challenged in the Petition, but not claims 1–25, 27, and 29. Accordingly, we institute an *inter partes* review of claims 26, 28, and 30–33.

B. Related Matters

Prior to filing this Petition, two other petitions challenging the '084 patent were filed by International Business Machines Corporation ("IBM")—IPR2014-00681, Paper 4 and IPR2014-00682, Paper 4. We denied an *inter partes* review in IPR2014-00681 (Paper 11) and instituted an *inter partes* review of claims 26, 28, and 30–33 in IPR2014-00682 (Paper 11). Petitioner also filed another petition challenging the '084 patent—IPR2014-00793, Paper 1.

Petitioner indicates that the '084 patent is the subject of concurrent proceedings in various district courts, several of which name one or more of the named petitioners as a defendant. *See* Pet. 1–2; Paper 5.

C. The ’084 Patent

The ’084 patent relates to network-based intrusion detection systems. Ex. 1001, 1:7–10. Intrusion detection systems are used to determine that a breach of computer security—access to computer resources by an unauthorized outsider—has occurred, is underway, or is beginning. *Id.* at 3:38–49. Conventional intrusion detection products and services are based on specialized equipment located on a customer’s premises and are directed to the analysis of a single customer’s data. *Id.* at 4:51–67. These systems may produce false alarms and are often unable to detect the earliest stages of network attacks. *Id.* In contrast, the broad-scope intrusion detection system of the ’084 patent analyzes the traffic coming into multiple hosts or other customers’ computers or sites, providing additional data for analysis, and consequently, the ability to recognize intrusions that would otherwise be difficult or impossible to diagnose. *Id.* at 5:44–56.

As described, one embodiment of the broad-scope intrusion detection system monitors the communications on a network or on a particular segment of the network by a data collection and processing center coupled to the network. *Id.* at 7:18–24; 7:31–35. Because the data collection and processing center gathers information from multiple network devices, including potentially multiple customers, it has access to a broader scope of network activity. *Id.* at 8:13–21. This additional data allows for the recognition of additional patterns of suspicious activity beyond those detectable with conventional systems. *Id.* at 8:21–22.

To detect intrusions, the ’084 patent describes one technique of collecting suspicious network traffic events, forwarding those events to a central database and analysis engine, and then using pattern correlations to

determine suspected intrusion-oriented activity. *Id.* at 8:23–31. Upon detection of suspected malicious activity, adjustments to devices such as firewalls can be made to focus sensitivity on attacks from suspected sources or against suspected targets. *Id.* at 8:31–35; 10:49–67. In addition, if any intrusions or attempted intrusions have been detected, alerts can be sent both to the system to which the suspicious communication was directed and also to systems that have not yet received the communication. *Id.* at 11:54–12:4.

D. Illustrative Claims

Of the challenged claims in the '084 patent, claims 1, 9, 19, and 26 are independent. Claims 1 and 26 are illustrative and recite:

> 1. A method of alerting at least one device in a networked computer system comprising a plurality of devices to an anomaly, at least one of the plurality of devices having a firewall, comprising:
>
> detecting an anomaly in the networked computer system using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system;
>
> determining which of the plurality of devices are anticipated to be affected by the anomaly by using pattern correlations across the plurality of hosts, servers, and computer sites; and
>
> alerting the devices that are anticipated to be affected by the anomaly.
>
> 26. A data collection and processing center comprising a computer with a firewall coupled to a computer network, the data collection and processing center monitoring data communicated to the network, and detecting an anomaly in the network using network-based intrusion detection techniques comprising analyzing data entering into a plurality of hosts, servers, and computer sites in the networked computer system.

E. Asserted Prior Art

Petitioner relies upon the following prior art references as its bases for challenging claims 1–33 of the '084 patent.[1]

Reference	Patents/Printed Publications	Exhibit
Aucsmith	U.S. Patent Publication No. 2003/0110392 A1	Ex. 1004 ("Aucsmith")
Gleichauf	U.S. Patent No. 6,415,321 B1	Ex. 1005 ("Gleichauf")

F. The Asserted Grounds of Unpatentability

Petitioner contends that the challenged claims are unpatentable under 35 U.S.C. §§ 102 and/or 103 based on the following grounds (Pet. 4):

Statutory Ground	Basis	Challenged Claims
§ 102(e)	Aucsmith	1–9 and 11–33
§ 103	Aucsmith and Gleichauf	1–33

ANALYSIS

A. Real Party-In-Interest

Patent Owner asserts that the Petition should be denied for failing to name all real parties-in-interest, as required by 35 U.S.C. § 312(a)(2). Prelim. Resp. 4–8. Specifically, Patent Owner contends that Petitioner failed to name both Banco Bilbao Vizcaya Argentaria, S.A. (BBVA) (*id.* at 4–7) and IBM (*id.* at 7–8) as real parties-in-interest.

Patent Owner asserts that BBVA is a real party-in-interest because it owns and controls BBVA Compass Bancshares, Inc. ("BBVA Compass"), one of the identified real parties-in-interest. *Id.* at 4–5. Patent Owner argues that BBVA Compass has admitted that it is controlled by BBVA, and admitted that BBVA serves as a source of strength and capital to BBVA Compass. *Id.* at 5 (citing Ex. 2001, 28, 30).

[1] Petitioner also proffers the Declaration of Dr. George Kesidis. *See* Ex. 1003.

Patent Owner asserts that IBM is a real party-in-interest because IBM entered (with the parties named as petitioners in this case) a "Common Interest and Confidentiality Agreement" purportedly containing "strategies of attorneys jointly defending cases against" Patent Owner. *Id.* at 7 (citing Ex. 2003, 1). IBM is not a named defendant in the district court cases involving the '084 patent. Thus, according to Patent Owner, the existence of this agreement, between IBM and other named defendants to the district court case, "is compelling circumstantial evidence that an agreement to defend and/or indemnify [Petitioner] likely exists." *Id.* at 8.

Whether a party who is not a named participant constitutes a real party-in-interest to a proceeding is a highly fact-dependent question. *Office Patent Trial Practice Guide*, 77 Fed. Reg. 48,756, 48,759 (Aug. 14, 2012) (citing *Taylor v. Sturgell*, 553 U.S. 880 (2008); 18A Charles Alan Wright, Arthur R. Miller & Edward H. Cooper, Federal Practice & Procedures §§ 4449, 4451 (2d ed. 2011)). The Office Patent Trial Practice Guide provides guidance regarding factors to consider in determining whether a party is a real party-in-interest. *Id.* One important consideration is whether a non-party exercises, or could have exercised, control over a party's participation in the proceeding. *Id.* An example justifying the real party-in-interest label is a party that funds, directs, and controls an IPR petition or proceeding. *Id.* at 48,760.

Patent Owner's evidence does not demonstrate sufficiently that BBVA or IBM exercised, or could have exercised, control over the filing of this Petition. Likewise, Patent Owner's evidence does not demonstrate sufficiently that BBVA or IBM funded, directed, and controlled the filing of this Petition.

Based on the record before us, Patent Owner does not provide a sufficient factual basis to conclude that BBVA or IBM should have been identified as a real party-in-interest. Accordingly, we do not deny the Petition for failure to identify all real parties-in-interest under 35 U.S.C. § 312(a)(2).

B. Claim Construction

Petitioner proposes interpretations for "an anomaly in the network," "network-based intrusion detection techniques," "alerting the device/alerts the devices," and "adjusting the firewall/controlling the device." Pet. 7–9. Patent Owner disputes Petitioner's analysis and provides its own interpretations for "anomaly," "determining which of the plurality of devices are anticipated to be affected by the anomaly," and "alert [-ing/-s] the device." Prelim. Resp. 11–16. Of these terms, we consider it necessary, for purposes of this decision, to construe the terms "anomaly" and "determining which . . . are anticipated to be affected by the anomaly." None of the remaining terms requires an express construction at this time.

1. "anomaly"

Petitioner proposes that "an anomaly in the network" be construed as "an irregularity in the network indicative of misuse of network systems or resources." Pet. 8. Patent Owner disagrees, arguing that the inclusion of "indicative of misuse of network systems or resources" does not comport with the broadest reasonable construction of the term. Prelim. Resp. 11.

We agree that Petitioner's construction of this term is not the broadest reasonable construction. Instead, the Specification supports a construction using the plain and ordinary meaning of anomaly—a departure from the usual or expected; an abnormality or irregularity. *See* Ex. 2004 (defining

anomaly as a "departure from the regular arrangement, general rule, or usual method; abnormality"). For example, the '084 patent states that "[a]nomaly detection systems look for statistically anomalous behavior . . . [s]tatistical scenarios can be implemented for user, dataset, and program usage to detect 'exceptional' use of the system." Ex. 1001, 3:54–57.

2. "determining which of the plurality of devices are anticipated to be affected by the anomaly"

Petitioner does not propose explicitly a construction for "determining which of the plurality of devices are anticipated to be affected by the anomaly" ("the determining limitation").[2] Patent Owner proposes that the broadest reasonable construction is "deciding or ascertaining which devices are expected or foreseen to be affected by the detected anomaly." Prelim. Resp. 13–15. Patent Owner bases this construction on dictionary definitions of "determine" and "anticipate." *Id.* at 13 (citing Exs. 2007, 2008 (defining determine as "to set limits to; bound; define . . . to reach a decision about after thought and investigation; decide upon")), 14 (citing Exs. 2009, 2010 (defining anticipate as "to . . . expect . . . to foresee (a command, wish, etc.) and perform in advance")).

Patent Owner's proposed construction is consistent with the Specification. For example, the Specification states that "[a]n anomaly is detected in the computer system, and then it is determined which device[] or

[2] This language is recited by claim 1. Claim 9 has a similar limitation, "determining a device that is anticipated to be affected by the anomaly," as does Claim 19, "determining which of the devices are anticipated to be affected by the anomaly." Claim 26 does not include the determining limitation, but claim 29, dependent from claim 26, recites, "adjusts a firewall of a plurality of devices . . . that is anticipated to be affected by the anomaly."

devices are anticipated to be affected by the anomaly in the future. These anticipated devices are then alerted to the potential for the future anomaly." Ex. 1001, 5:57–65. Although the Specification also states that "the devices are polled in a predetermined sequential order, and a device anticipated to be affected by the anomaly is a device that has not been polled," the '084 patent does not clearly depart from the plain and ordinary meaning and redefine "anticipated to be affected" to be equivalent to devices that have not been polled. *Id.* at 5:66–6:2; *see also* Fig. 5, 10:65–11:9 (using language—"hosts . . . that have not yet been hit by the intrusion attempt"—consistent with the plain language of the determining limitation).

In keeping with the broadest reasonable interpretation that is consistent with the Specification, we construe the determining limitation to mean deciding or ascertaining which devices are expected or foreseen to be affected by the anomaly.

C. The Asserted Grounds

1. Anticipation by Aucsmith (Ex. 1004)

Petitioner challenges claims 1–9 and 11–33 as anticipated by Aucsmith. Pet. 11–27. Aucsmith discloses an intrusion detection system to help discover illicit attempts to access resources and actual security breaches. Ex. 1004 ¶ 2.

Figure 1 is reproduced below:

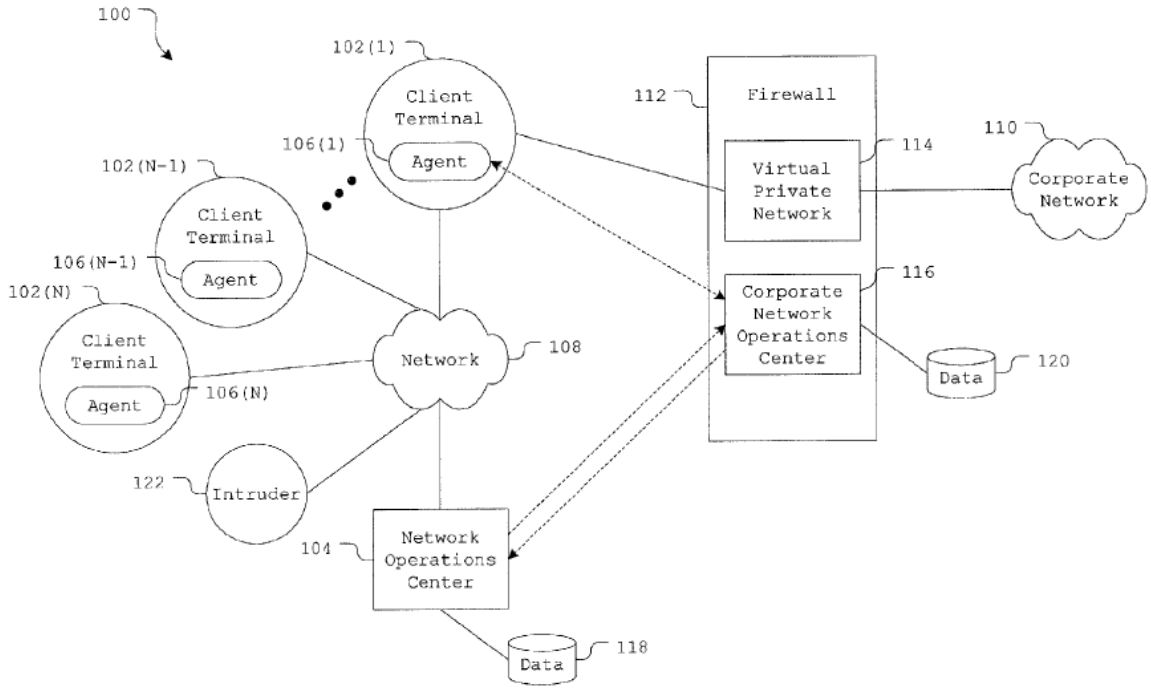

FIG. 1

Figure 1 of Aucsmith is a block diagram of an embodiment of a network configuration. *Id.* ¶ 4. Client terminals 102(1)–102(N) each include an agent 106(1)–106(N) that can monitor information received at the associated client terminal from network 108. *Id.* ¶ 10. The agent can report potential problems it detects to server 104 (labeled "Network Operations Center" on Figure 1) through firewall 112. *Id.* Server 104 may update its collection of security data 118 and corporate server 116's collection of security data 120. *Id.* ¶ 11. Server 104 "can in real time inform all of the client terminals . . . of this possible security problem via each of the agents." *Id.*

a. Claims 1–9, 11–25, 27, and 29

With respect to the determining limitation, required by all these claims,[3] Petitioner points to Aucsmith's disclosure

> with the server 104 able to receive security updates from multiple client terminals and to inform all (or at least a subset) of the client terminals 102(1)-102(N) in real time upon detection and/or correction of a security problem, any potentially negative effects of the security problem can be reduced or eliminated in real time.

Pet. 14 (quoting Ex. 1004 ¶ 12), 17. Petitioner also points to the prosecution history of a continuation application of the '084 patent ("the '585 application"). *Id.* According to Petitioner, the Examiner in the '585 application found that Aucsmith disclosed a more narrow element similar to the determining limitation. *Id.* (citing Ex. 1007, 18).

Patent Owner asserts that Petitioner does not show that Aucsmith discloses the determining limitation. Prelim. Resp. 19–25. We agree with Patent Owner that the language of Aucsmith relied upon by Petitioner states that once a security problem is detected by the server, either all or a subset of the clients may be informed. *See* Pet. 17–18 (citing Ex. 1004 ¶¶ 12 (stating that server 104 is able to "inform *all (or at least a subset)* of the client terminals . . . in real time") (emphasis added), 13 ("The server . . . *can inform all of the client terminals* . . . in real time") (emphasis added), 51 ("The server . . . *may only notify the client 102, but typically notifies all of the client terminals*. . .") (emphasis added)). However, nothing in the cited language discloses determining which of the subset of client terminals *is*

[3] Claim 29 recites "wherein the data collection and processing center further adjusts a firewall of each of a plurality of devices that is connected to the *network that is anticipated to be affected by the anomaly* responsive to the detection of the anomaly" (emphasis added).

anticipated to be affected. Instead, Aucsmith explicitly discusses only that "[i]nformation logged about an anomaly can include which of the client terminals 102(1)-102(N) *reported the anomaly to the server 104*, the time that the anomaly was sent to and/or received by the server 104, the nature of the anomaly, and/or other similar types of information." Ex. 1004 ¶ 49 (emphasis added). Although Petitioner proffers testimony contending that a skilled artisan would have understood Aucsmith to teach the determining limitation, Petitioner and Dr. Kesidis provide no persuasive explanation or objective evidence to support this conclusion. *See* Ex. 1003 ¶ 64. We are not persuaded, therefore, that Petitioner has made a sufficient threshold showing that Aucsmith discloses determining which of the devices are *expected to be affected* by the attack.

We have reviewed the rest of the portions of Aucsmith relied upon by Petitioner (Pet. 17–19), and we are not persuaded that any of the remaining portions disclose the determining limitation. Nor does Petitioner point to persuasive evidence that the determining limitation is inherently disclosed by Aucsmith. Thus, we deny Petitioner's challenge that Aucsmith anticipates claims 1–9, 11–25, 27, and 29.

b. Claim 26

Independent claim 26 does not recite the determining limitation. Claim 26 recites "[a] data collection and processing center comprising a computer with a firewall" that "monitor[s] data communicated to the network" and "detect[s] an anomaly in the network." Ex. 1001, 14:18–25.[4] Petitioner equates server 104 or server setup 500 of Aucsmith with the recited "data collection and processing center." Pet. 40–41; Ex. 1003 ¶ 148.

[4] Independent claim 19 recites a similar element. Ex. 1001, 13:41–52.

Petitioner asserts that Aucsmith describes server 104 "monitoring data communicated to the network" ("the monitoring limitation") and "detecting an anomaly in the network using network-based intrusion detection techniques comprising analyzing data" ("the detecting limitation") as required by claim 26. Pet. 41–43; Ex. 1003 ¶¶ 149–153.

Patent Owner argues that Petitioner has not shown that Aucsmith discloses the "data collection and processing center" as required by these claims. Prelim. Resp. 26–28. Specifically, Patent Owner argues that the disclosure Petitioner relies on to show the monitoring and detecting limitations are directed to the activities of the *client terminals* and not server 104. *Id.* at 27 (emphasis added). Patent Owner argues that because Figure 1 of Aucsmith shows server 104 as a separate entity from client terminal 102 and agent 106, Petitioner has not shown how Aucsmith shows the claim elements as arranged in the claims. *Id.*

We are persuaded that Petitioner has made a sufficient threshold showing that Aucsmith discloses all the elements of claim 26, arranged or combined in the same way as recited in the claims. In its discussion of "the data collection and processing center," Petitioner cites to language in Aucsmith describing server 104. Pet. 40–41 (citing Ex. 1004 ¶¶ 27, 78); *see also* Ex. 1003 ¶¶ 148–153 (referencing the same paragraphs of Aucsmith). We are persuaded that Petitioner has shown a reasonable likelihood that Aucsmith discloses server 104 performing both the monitoring and detecting limitations.

Specifically, in the discussion of the monitoring limitation, Petitioner quotes language of Aucsmith stating that "server 104 may use the information about the anomaly . . . in performing general intrusion detection

actions" and that such actions include "monitoring and analyzing client and system activity . . . inspecting all incoming and outgoing information . . . and performing other similar tasks." Pet. 41 (quoting Ex. 1004 ¶ 50). We are persuaded that this language shows a reasonable likelihood that Aucsmith discloses server 104 performing the monitoring limitation.

Similarly, in discussing the detecting limitation, Petitioner quotes language of Aucsmith stating that "server 104 can also use the possible security problems reported by all of the agents . . . to help detect intrusion patterns, new intrusion techniques . . ." and "the server 104 may use the information . . . in performing general intrusion detection actions." Pet. 42 (quoting Ex. 1004 ¶ 13); *see also* Ex. 1003 ¶¶ 150–151. We are persuaded that this language shows a reasonable likelihood that Aucsmith discloses server 104 performing the detecting limitation.

We are, therefore, persuaded that Petitioner has established that there is a reasonable likelihood that claim 26 is unpatentable as anticipated by Aucsmith.

c. Claim 28

Claim 28 depends from claim 26 and recites "wherein the data collection and processing center further determines which of a plurality of devices that are connected to the network have been affected by the anomaly and alerts the devices." Ex. 1001, 14:33–36. Patent Owner argues that Petitioner does not show that Aucsmith discloses "determining which devices *have been* affected." Prelim. Resp. 29. This limitation is similar to the determining limitation of claim 1 discussed above. However, instead of requiring determination of devices that are *anticipated to be affected*, claim 28 requires determination of devices that *have been affected*.

We are persuaded that Petitioner has made a sufficient threshold showing that Aucsmith discloses this limitation. *See* Pet. 45–46 (citing Ex. 1004 ¶ 57 (stating that server 104 may "follow up . . . on the source of the [problem]" and "[s]uch follow up may include sending notice to the source that a security problem originated at the source's location")). We are persuaded that this language shows a reasonable likelihood that Aucsmith discloses determining which devices "have been affected." We are also persuaded that this language shows a reasonable likelihood that Aucsmith discloses alerting that device.

We are, therefore, persuaded that Petitioner has established that there is a reasonable likelihood that claim 28 is unpatentable as anticipated by Aucsmith.

d. Claims 30–33

Claims 30–33 depend from claim 26. Patent Owner argues that Petitioner has not shown that Aucsmith discloses the additional elements added by these claims because they provide only quotes from Aucsmith without further analysis or explanation. Prelim. Resp. 30–33. On this record, we are not persuaded by Patent Owner's arguments. *See* Pet. 47–49. We are persuaded that Petitioner has established that there is a reasonable likelihood that claims 30–33 are unpatentable as anticipated by Aucsmith.

2. Obviousness Over Aucsmith and Gleichauf (Ex. 1005)

Petitioner challenges claims 1–33 as obvious over Aucsmith and Gleichauf. Pet. 49–59. Gleichauf discloses "[a] method and system for mapping a network domain that provides a centralized repository . . . including an intrusion detection system." Ex. 1005 Abstract.

Petitioner maintains that Aucsmith discloses all the limitations of the challenged claims, but concedes that Gleichauf "explains, in greater detail, the type of vulnerability analysis that was known to one skilled in the art to determine which device 'is anticipated to be affected by the anomaly.'" Pet. 53. Petitioner asserts that a person of ordinary skill would have combined Aucsmith and Gleichauf based on language in the references themselves. *Id.* at 51.

Patent Owner argues that Petitioner did not provide sufficient articulated reasoning with some rational underpinning to support the legal conclusion of obviousness because Petitioner never identifies which aspects of Gleichauf should be incorporated when implementing Aucsmith, or which particular teaching of Aucsmith should be implemented. Prelim. Resp. 36–40 (citing *KSR Int'l v. Teleflex Inc.*, 550 U.S. 398, 418 (2007)). Specifically, Patent Owner points to Petitioner's statement that "it would have been obvious to one having ordinary skill in the art at the time of the alleged invention to include *any aspect* of one identified prior [art] reference in any other identified prior art reference." Prelim. Resp. 36 (quoting Pet. 51) (emphasis added).

We agree with Patent Owner that Petitioner's stated rationale is not sufficiently specific. *See* Prelim. Resp. 36 (quoting Pet. 51). We recognize that Petitioner supplements the very generic language pointed to by Patent Owner by pointing to portions of Aucsmith and Gleichauf and asserting that the references themselves provide a rationale to combine the two references. Pet. 51–52. Specifically, Petitioner quotes the following from Aucsmith:

> server 104 can also use the possible security problems reported by all of the agents . . . to help detect intrusion patterns, new intrusion

> techniques, and other security problems that may not be apparent to an individual client terminal or to a small number of client terminals

(Pet. 51 (quoting Ex. 1004 ¶ 13)), and the following from Gleichauf:

> conventional security products have insufficient information to[] self-configure for reliable detection of policy violations and patterns of misuse.

Pet. 51–52 (quoting Ex. 1005, 1:46–54).

According to Petitioner, Aucsmith thus provides a reason for performing additional analysis at a central entity, a remedy Gleichauf was attempting to provide. *Id.* We, however, are not persuaded that Petitioner has provided sufficient explanation or evidence to support this conclusion. The language quoted by Petitioner does not, by itself, persuade us that a person of ordinary skill would have found it obvious to combine the teachings of the two references for the reasons articulated by Petitioner. Furthermore, Petitioner does not supplement the quoted language with persuasive explanation.

In addition, Petitioner asserts that because Aucsmith teaches a method and system of intrusion detection, although Gleichauf primarily teaches methods of mapping network devices, "[i]t would be a natural extension for one having ordinary skill in the art to incorporate the teachings of Gleichauf when attempting to implement the teachings found in Aucsmith." *Id.* at 52 (citing Ex. 1003 ¶¶ 185–186). Again, however, we are not persuaded that Petitioner has provided sufficient explanation or evidence to support this conclusion.

Instead, we agree with Patent Owner that the portions of Dr. Kesidis's Declaration relied upon by Petitioner (Ex. 1003 ¶¶ 182–187) to support the above conclusions do not shed any light on either assertion. Dr. Kesidis

testifies that Aucsmith and Gleichauf address the same problem and, based on this assertion alone, concludes that a skilled artisan would have found combining the elements to be obvious. Ex. 1003 ¶¶ 182–185. Dr. Kesidis also asserts that "there was a design need or market pressure to solve a problem and a finite number of identified, predictable solutions" such that the combination of Aucsmith and Gleichauf "would have yielded the methods and systems claimed in the '084 patent." *Id.* ¶ 186. Dr. Kesidis, however, does not provide support for his conclusions with persuasive explanation or citation to objective evidence.

Because we are not persuaded that Petitioner's proffered rationale to combine Aucsmith and Gleichauf is based on anything other than hindsight bias, we are not persuaded that Petitioner has established that there is a reasonable likelihood that claims 1–33 are unpatentable as obvious over Aucsmith and Gleichauf.

CONCLUSION

Accordingly, we determine that Petitioner has shown a reasonable likelihood that it would prevail in demonstrating that claims 26, 28, and 30–33 of the '084 patent are unpatentable on at least one challenged ground. The Board has not made a final determination on the patentability of any challenged claim.

ORDER

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review is hereby instituted for claims 26, 28, and 30–33 of the '084 patent as unpatentable, under 35 U.S.C. § 102(e), as anticipated by Aucsmith;

FURTHER ORDERED that no other grounds of unpatentability alleged in the Petition for any claim is authorized; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, the trial commences on the entry date of this Decision, and notice is hereby given of the institution of a trial.

PETITIONERS:

Robert M. Evans, Jr.
Marc Vander Tuig
SENNIGER POWERS LLP
revans@senniger.com
mvandertuig@senniger.com

Geoffrey K. Gavin
JONES DAY
ggavin@jonesday.com

Jason S. Jackson
KUTAK ROCK
jason.jackson@kutarock.com

PATENT OWNER:

Jonathan M. Strang
Lori A. Gordon
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
jstrang-PTAB@skgf.com
lgordon-PTAB@skgf.com

Donald J. Coulman
INTELLECTUAL VENTURES MANAGEMENT
dcoulman@intven.com