

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

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

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*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

INTRODUCTION

A. Background

Petitioner, Commerce Bancshares, Inc., Compass Bank, and First National Bank of Omaha, filed a Petition (Paper 1, “Pet.”) requesting an *inter partes* review of claims 1–33 of U.S. Patent No. 6,715,084 B2 (Ex. 1001, “the ’084 patent”). On December 1, 2014, we instituted a review (Paper 7, “Decision to Institute” or “Dec.”) based upon Petitioner’s assertion that claims 26, 28, and 30–33 are unpatentable, under 35 U.S.C. § 102(b), as anticipated by Aucsmith.¹ Dec. 18. Petitioner provides a Declaration from Dr. George Kesidis (Ex. 1003), and Patent Owner provides a Declaration from Dr. David Goldschlag (Ex. 2011).

This is a Final Written Decision under 35 U.S.C. § 318(a). Based on the record presented, we are persuaded that Petitioner has shown by a preponderance of the evidence that claims 26, 28, and 30–32 are unpatentable. We are not persuaded that Petitioner has shown by a preponderance of the evidence that claim 33 is unpatentable.

B. Related Matters

At the time of filing the Petition in this proceeding, Petitioner filed another petition for *inter partes* review in IPR2014-00793 challenging claims 1–10 and 12–33 of the ’084 patent. We denied institution in that proceeding and denied Petitioner’s subsequent request for rehearing. See IPR2014-00793, Papers 7, 9.

Another petitioner also filed two petitions challenging claims of the ’084 patent in IPR2014-00681 and IPR2014-00682. We denied institution and a subsequent request for rehearing in IPR2014-00681. See IPR2014-

¹ U.S. Patent Publication No. 2003/0110392 A1 (Ex. 1004) (“Aucsmith”).

00681, Papers 11, 14. We instituted *inter partes* review in IPR2014-00682 on October 30, 2015. IPR2014-00682, Paper 11 (final written decision being issued concurrently).

Petitioner indicates that the '084 patent is the subject of concurrent proceedings in various district courts, at least one of which names Petitioner as a defendant. *See* Pet. 1–2.

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 disclosed in 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. 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.

Figure 2 of the '084 patent is reproduced below.

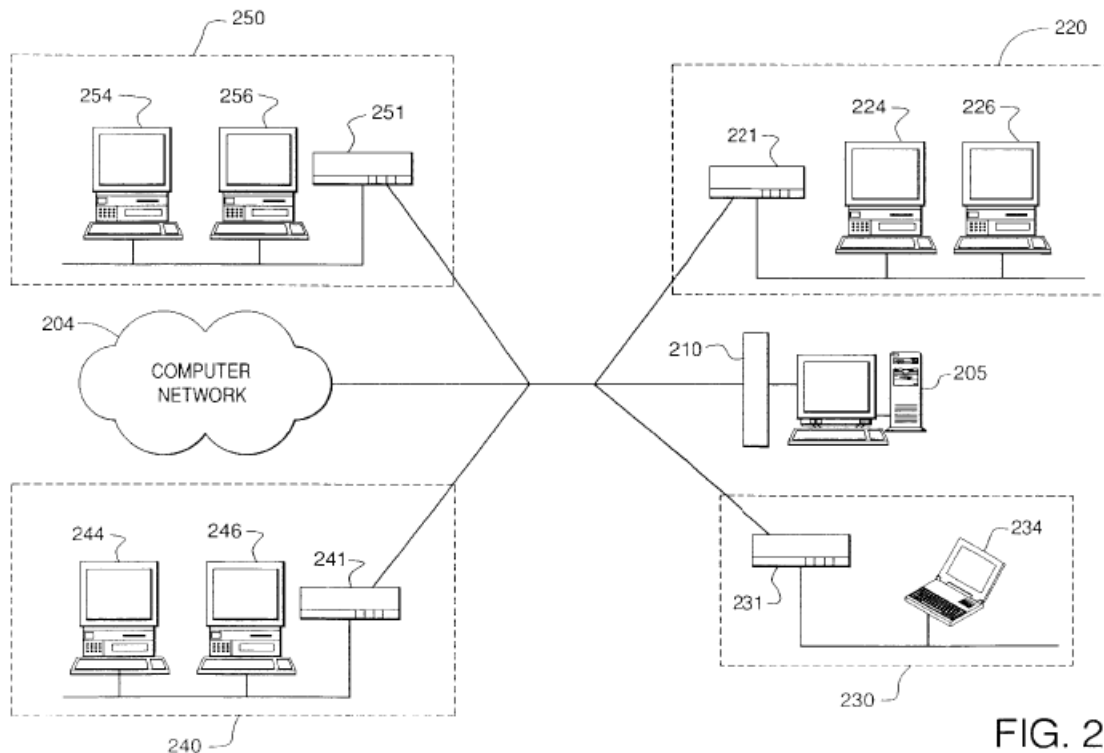


FIG. 2

Figure 2 shows a broad-scope intrusion detection system as described by the '084 patent. *Id.* at 6:50–52. A separately maintained data collection and processing center, comprising computer or server 205 and firewall 210, is coupled to network 204. *Id.* at 7:18–20. The data collection and processing center receives information from the various network devices coupled to network 204. *Id.* at 7:33–36. “For example, all communications sent to each host 220, 230, 240, 250 are forwarded to, or otherwise captured by, the data collection and processing center.” *Id.* at 7:36–39. The '084 patent also discloses that “certain devices can be used as sensors to sense data traffic and pass their findings on to the data collection and processing center.” *Id.* at 7:45–47.

To detect intrusions, the '084 patent describes a “multi-stage 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. Ex. 1001, 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, appropriate alerts or notifications can be transmitted to pertinent devices. *Id.* at 10:62–65.

D. Claims at Issue

Of the claims at issue, claim 26 is independent. Claims 28, 30, 31, and 33 depend from claim 26. Claim 32 depends from claim 31. Claim 26 recites:

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.

ANALYSIS

A. Claim Construction

For purposes of the Decision to Institute we expressly construed the terms “anomaly” and “determining which . . . are anticipated to be affected by the anomaly.” Dec. 7–9. In its response, Patent Owner does not address explicitly the construction of any claim terms, including the two discussed in the Decision to Institute. Paper 13 (“PO Resp.”). Petitioner also does not address explicitly the constructions adopted by the Decision to Institute.

Petitioner, however, characterizes Patent Owner's position as "depend[ing] on applying a very narrow construction of the claim term 'data.'" Paper 16 ("Reply"), 1.

We construe all claim terms using the broadest reasonable construction in light of the '084 patent specification. 37 C.F.R. § 42.100(b). Based on the record, and to properly resolve the issues presented in this proceeding, we address explicitly only the terms below.

1. *"anomaly"*

In the Decision to Institute, we construed the term "anomaly" as "a departure from the usual or expected; an abnormality or irregularity." Dec. 7–8. Specifically, we agreed with Patent Owner's assertion that this is the plain meaning of the term and is consistent with the specification of the '084 patent. *Id.* at 7. 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." *Id.* at 8 (citing Ex. 1001, 3:54–57). Neither party contests this construction. We discern no reason to deviate from this construction of "anomaly."

2. *"data / data communicated to the network / data entering into a plurality of hosts"*

Although Patent Owner never proposes expressly a claim construction for the term "data" in its response, Patent Owner, at least arguably, implies that the term requires construction by emphasizing it throughout much of its brief. In the claims, the term "data," however, never stands on its own. Thus, based on the context, we understand the term being discussed to be two phrases in which data is used in the claims—"data communicated to the

network” and “data entering into a plurality of hosts” (“the data limitations”).

For example, in the section entitled “Summary of Response,” Patent Owner states that Petitioner “ignored that the claimed data collection and processing center must detect anomalies by analyzing the *data* entering computers in the network, instead proffering a reference that, at best, discloses a central unit (server 104) that performs a meta-analysis of anomaly reports received from distributed agents residing on clients.” PO Resp. 1 (emphases added by Patent Owner); *see also id.* at 3 (same emphasis added to the word data). Patent Owner, thus, argues that the data limitations are not equivalent to reports about such data being sent by distributed agents. *See also id.* at 1–2 (“As the name suggests, the data collection and processing center of claim 26 is a central unit that collects and processes data to detect anomalies rather than merely receiving reports of detected anomalies.”).

Patent Owner reinforces the understanding that they are arguing for a limited interpretation of the data limitations by emphasizing that Aucsmith’s “server 104 logs anomaly reports it receives from the agents (which are part of the clients), and uses the logged reports to further analyze the detected anomaly.” PO Resp. 8. To support its assertion that “the claims at issue do not read on a system that merely processes anomaly reports received from remote clients,” Patent Owner points to the following language from the ’084 patent:

[For example,] all communications sent to each host 220, 230, 240, 250 are forwarded to, or otherwise captured by, the data collection and processing center. Thus, the data collection and processing center receives all communications (i.e., the data) originating from a user on the computer network 204 and

flowing to host 220 (and vice versa), for example, as well as all communications originating from the computer network 204 and flowing to all other hosts (and vice versa).

PO Resp. 2–3 (quoting Ex. 1001, 7:37–44). Taken together, Patent Owner’s arguments appear to propose a construction of the data limitations that excludes “anomaly reports” or “analysis results” sent to a central collection and processing center.

Petitioner similarly interprets Patent Owner’s arguments to be a proposed construction of the claim term “data.” Reply 1–5. Based on this understanding, Petitioner argues that Patent Owner’s proposed construction is improperly narrow, requiring the data collection and processing center to monitor and analyze “data” “firsthand.” *Id.* at 3. Petitioner points out that the language quoted above, relied upon by Patent Owner for the proposition that the claims do not read on analyzing anomaly reports, is immediately followed by language stating that “[i]t should be noted that certain devices can be used as sensors to sense data traffic and pass their findings on to the data collection and processing center” *Id.* at 4 (quoting Ex. 1004, 7:44–51.)

According to Petitioner, this language shows that the ’084 patent contemplates that the data collection and processing center may not necessarily look at “data communicated to the network” firsthand. Reply 4. Instead, this language indicates that the ’084 patent also considers monitoring and analysis of “findings” based on sensed data traffic to be within the scope of the subject matter at issue. *Id.* (citing Ex. 1003 ¶¶ 19–21). Further, Petitioner points out that the ’084 patent describes an example in which “[d]ata from existing customer’s conventional intrusion detection system is provided to the central database and then analyzed” where “[d]ata

records comprise, for example, a time-stamp, a description of the activity, and the source of the probe.” *Id.* at 4–5 (quoting Ex. 1004, 9:4–8).

Petitioner explains that the construction of the term “data” must be broad enough to encompass all of the listed types of data. *Id.* at 5.

We agree with Petitioner that the data limitations do not necessarily exclude anomaly reports or analysis results sent to a central collection and processing center. Instead, we are persuaded that, as used by the ’084 patent, the plain and ordinary meaning of these terms governs. The plain and ordinary meaning of “data” allows for transfer between entities without losing acquired characteristics, such as where the item came from. In other words, “data communicated to the network” qualifies as such when it is initially intercepted by a computer on the network, after it is placed in a report or other record (whether or not that record contains further analysis or additional data items), and after it has been forwarded to another computer. Thus, without an express description to the contrary, we presume that “data communicated to the network” and “data entering into a plurality of hosts,” as recited in claim 26, retains the plain and ordinary meaning of those phrases before, during, and after initial interception by a computer or computers. Patent Owner does not point to persuasive evidence to the contrary.

B. Anticipation by Aucsmith

Petitioner asserts that claims 26, 28, and 30–33 are anticipated by Aucsmith. Pet. 11–13, 40–43, 45–49. In the Decision to Institute, we determined that Petitioner had shown a reasonable likelihood of prevailing on this proposed ground of unpatentability. Dec. 12–15.

We have reviewed Petitioner’s anticipation arguments and supporting evidence, including Aucsmith’s disclosure, the detailed claim chart appearing on pages 40–49 of the Petition, and the testimony of Dr. Kesidis. Despite the counter-arguments in Patent Owner’s Response, and the evidence cited therein, which we also have considered, Petitioner has shown, by a preponderance of the evidence, that each of claims 26, 28, and 30–32 is unpatentable under 35 U.S.C. § 102(b) as anticipated by Aucsmith.

1. Overview of Aucsmith

Aucsmith discloses an intrusion detection system to help discover illicit attempts to access resources and actual security breaches. Ex. 1004 ¶ 2.

Figure 1 of Aucsmith is reproduced below:

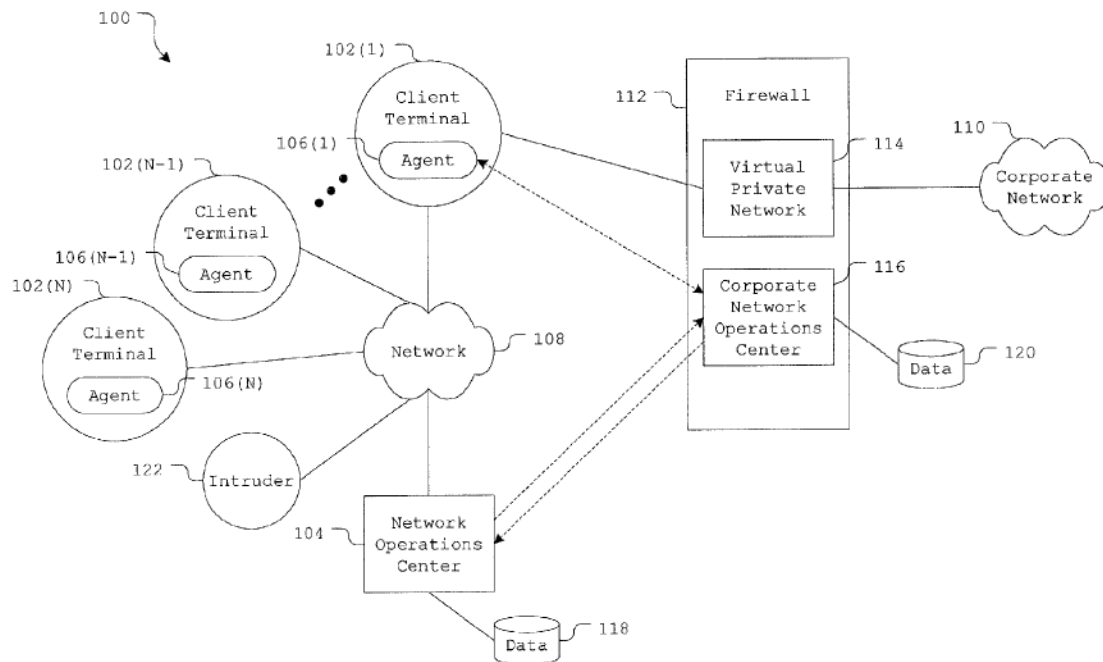


FIG. 1

Figure 1 is a block diagram 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.*

To detect intrusions, agent 106 examines information arriving at client 102 and determines if that information includes or indicates a known anomaly. Ex. 1004 ¶ 37. If agent 106 detects a known anomaly, it can report the anomaly to server 104 in real time. *Id.* ¶ 41. Server 104 receives notice of the anomaly and can examine the anomaly “to determine . . . if the anomaly constitutes an actual anomaly, e.g., a known security problem, a possible security problem serious enough to report to the client terminals.” *Id.* ¶ 43. If server 104 determines that the anomaly is an actual anomaly, then it may document the anomaly and/or perform or instigate corrective procedures. *Id.* ¶ 48. Server 104 may then use the documented information about the anomaly along with other security problem information in performing general intrusion detection actions. *Id.* ¶ 50. “Such actions can include monitoring and analyzing client and system activity (including examination of other anomalies sent to the server 104), performing audits, inspecting all incoming and outgoing information (e.g., packets), assessing integrity, recognizing attack patterns, reporting possible intrusions, and performing other similar tasks.” *Id.* Server 104 can notify client terminals 102(1)–102(N) or the firewall of the anomaly and may follow up on the source of the anomaly. *Id.* at ¶¶ 51, 54, 58.

Figure 5 of Aucsmith is reproduced below.

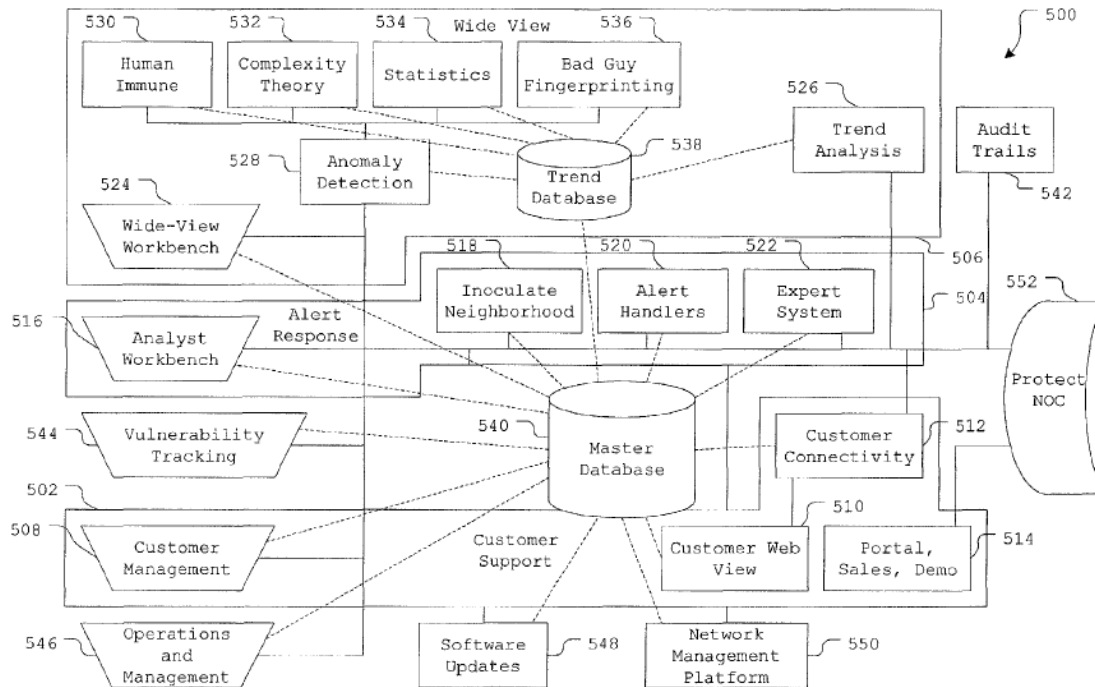


FIG. 5

Figure 5 is a block diagram of an example configuration of server 104. Ex. 1004 ¶ 72. Server setup 500 may include protection mechanism 552, “e.g., a firewall between the server 104 and the network 108.” *Id.* ¶ 78.

2. Claim 26

Petitioner asserts that Aucsmith discloses each of the limitations of claim 26. Specifically, Petitioner relies on Aucsmith’s server 104 as teaching the claimed data collection and processing center. Pet. 40–41; Paper 22 (Transcript of Oral Hearing, “Tr.”), 4:20–6:2. Petitioner asserts that Aucsmith discloses “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” (“the detecting limitation”) relying on several

portions of Aucsmith, including language stating that server 104: (1) “use[s] possible security problems reported by agents 106 to help detect intrusion patterns” and examines an anomaly sent from agent 106 to determine “if the anomaly constitutes an actual anomaly” (“the indirect detecting method”); and (2) “analyz[es] client and system activity (including examination of other anomalies sent to the server 104), . . . assessing integrity, recognizing attack patterns, reporting possible intrusions, and performing other similar tasks” (“the direct detecting method”). Pet. 42–43 (quoting Ex. 1004 ¶¶ 13, 43, 50).

At the hearing, Petitioner clarified that Aucsmith describes server 104 using two methods of detecting anomalies. Tr. 8:21–10:9, 15:12–17:15, 25:5–26:16. Under the indirect detecting method, server 104 receives reports of possible anomalies from the distributed agents and using these reports, further detects anomalies, essentially doing a second-hand, or indirect, analysis of data entering the network that is passed on by the agents. Petitioner explained that the direct detecting method describes server 104 detecting anomalies by directly analyzing data entering the network. According to Petitioner, both disclosed methods of detecting anomalies satisfy the detecting limitation.

Patent Owner argues that Petitioner has not shown that server 104 discloses the detecting limitation. PO Resp. 3–16. According to Patent Owner, the indirect detecting method does not satisfy the detecting limitation because server 104 does not detect anomalies firsthand, but instead detects anomalies based on reports made by the distributed agents. *Id.* at 6–7, 9–15 (citing Ex. 1004 ¶¶ 10, 13, 43, 45, 46, 48; Ex. 2011 ¶¶ 39, 42). Thus, for example, Aucsmith’s disclosure of “us[ing] possible security

problems reported by agents 106 to help detect intrusion patterns,” refers solely to “perform[ing] post-detection analysis” and does not disclose server 104 *itself* “analyzing the data to detect the anomalies.” *Id.* at 6–7 (citing Ex. 1004 ¶¶ 13; Ex. 2011 ¶ 39). In other words, Patent Owner contends that server 104 does not detect an anomaly because the agents have already detected the anomaly by detecting the “possible security problem,” and the further detecting that server 104 does is merely “classifying,” not “detecting.” Tr. 37:21–38:8. According to Patent Owner, although Aucsmith discloses server 104 “classif[ying] the anomalies as whether they’re a possible attack or an actual attack, something to be worried about, or merely an innocuous statistical fluke,” this is not detecting an anomaly because “[i]t’s already been detected as an anomaly, and an anomaly is a statistical deviation.” Tr. 41:18–42:25.

Further, Patent Owner argues that the direct detecting method of Aucsmith does not satisfy the detecting limitation because it does not actually directly analyze data entering the network. PO Resp. 9. According to Patent Owner, the actual language in Aucsmith relied upon by Petitioner, read in context, discloses “that server 104 may perform a variety of other ‘general intrusion detection actions’ based on a logged anomaly report, but it does not disclose that server 104 itself detected the anomaly.” *Id.* (citing Ex. 1004 ¶¶ 49–50; Ex. 2011 ¶ 41).

As explained above, we do not agree with Patent Owner that the broadest reasonable interpretation of the term “data” or the data limitations excludes “anomaly reports” or “analysis results” sent to a central collection and processing center. Moreover, we are not persuaded that the claimed data collection and processing center must monitor and analyze data

“firsthand” as Patent Owner contends. PO Resp. 1–3. In its Response, Patent Owner bases its narrow reading of the scope of claim 26 on the description in the ’084 patent that “all communications sent to each host 220, 230, 240, 250 are forwarded to, or otherwise captured by, the data collection and processing center” and “[t]hus, the data collection and processing center receives all communications (i.e. data) originating from a user on the computer network 204 and flowing to . . . all . . . hosts (and vice versa).” *Id.* at 2–3 (quoting Ex. 1004, 7:37–44). Nothing in this language, however, limits the data collection and processing center to receiving communications that *directly* originate from a user. In other words, nothing in this language prevents a device from intercepting the communications, doing some data manipulation or analysis, and then forwarding the resulting product on to the data collection and processing center. In fact, the language itself seems to contemplate that scenario—“all communications . . . are *forwarded to*, or otherwise captured by, the data collection and processing center.” Ex. 1004, 7:36–37 (emphasis added). We are not persuaded to the contrary by Dr. Goldschlag’s testimony, which simply recites the claim language and concludes that “[m]onitoring and analyzing reports based on such data does not satisfy the claim language.” Ex. 2011 ¶ 20.

Moreover, Patent Owner does not address, in its brief, the very next sentence of the ’084 patent, which describes a situation similar to that described by Aucsmith, where the data collection and processing center does *not* monitor the data “firsthand.” Ex. 1004, 7:45–47 (“It should be noted that certain devices can be used as sensors to sense data traffic and pass their *findings* on to the data collection and processing center.”) (emphasis added). We are persuaded that the correct reading of this language, in context, is that

the '084 patent contemplates network devices that may implement various amounts of processing of incoming data prior to forwarding that data on to the central data collection and processing center. At the very least, the '084 patent does not clearly restrict that amount of data manipulation and processing.

We are persuaded that Petitioner has shown by a preponderance of the evidence that Aucsmith discloses the detecting limitation as required. First, we are persuaded that the indirect detecting method of Aucsmith satisfies the detecting limitation. Aucsmith discloses that “server 104 can also use the possible security problems reported by all of the agents 106(1)–106(N) to help detect intrusion patterns, new intrusion techniques, and other security problems.” Ex. 1004 ¶ 13. As discussed, although we agree that server 104, using this method, is analyzing reports of “possible security problems” created by distributed agents, we are persuaded that this is within the scope of the claim because the reports include data entering the network. For example, Aucsmith discloses that “server 104 receives notice of the anomaly and can examine the anomaly,” and “[i]n individually examining the anomaly [reported by agent 106], the server 104, may, for example, search for particular information in the anomaly such as a network address previously noted as a security problem” Ex. 1004 ¶¶ 43, 45; *see also id.* ¶ 44 (“[S]erver 104 may examine the anomaly in conjunction with other information accessible by the server 104, e.g., information included in the collection of security data 118, information sent to the server 104 from other sources, information accessible to the server 104 through the network 108 and/or the corporate server 116, and other similar types of information.”). We are persuaded that Aucsmith discloses server 104 analyzing data

entering the network, although this data may also have been analyzed previously by the distributed agents.

Second, we are persuaded that the direct detecting method of Aucsmith satisfies the detecting limitation. We agree with Petitioner that the relevant portion of Aucsmith discloses directly analyzing data entering the network. The entire passage in context reads as follows:

In documenting the anomaly, the server 104 can log 220 the anomaly. Generally, logging the anomaly includes storing a record of the anomaly in the collection of security data 118. Information 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.

Once logged, the server 104 may use the information about the anomaly along with other security problem information in performing general intrusion detection actions. Such actions can include monitoring and analyzing client and system activity (including examination of other anomalies sent to the server 104), performing audits, inspecting all incoming and outgoing information (e.g., packets), assessing integrity, recognizing attack patterns, reporting possible intrusions, and performing other similar tasks.

Ex. 1004 ¶¶ 49–50. Contrary to Patent Owner’s arguments, we are not persuaded that server 104 performs all “general intrusion detection actions” based on the logged anomaly report. Instead, the language indicates that *along with* the logged information, server 104 *may also* analyze “system activity” by specifically “inspecting all incoming and outgoing information” and “recognizing attack patterns.” We are persuaded that this discloses server 104 directly analyzing data entering the network to detect an

anomaly—a departure from the usual or expected; an abnormality or irregularity.

Thus, we are persuaded that Petitioner has shown by a preponderance of the evidence that claim 26 is anticipated by Aucsmith.

3. *Claim 28*

Claim 28 depends from claim 26, adding that “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.” Petitioner asserts that Aucsmith discloses this additional limitation because it discusses “inform[ing] 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,” and “server 104 can notify 222 the client terminals 102(1)–102(N) of the anomaly” where “[s]uch follow up may include sending notice to the source that a security problem originated at the source’s location.” Pet. 45–46 (citing Ex. 1004 ¶¶ 12, 51, 57–58; Ex. 1003 ¶¶ 158–61).

Patent Owner argues that Petitioner does not show either determining which devices have been affected by an anomaly or alerting those devices.² PO Resp. 17 (citing Ex. 2011 ¶ 49). In the Decision to Institute, we were persuaded that Petitioner had shown a reasonable likelihood that Aucsmith discloses this limitation based on Aucsmith’s disclosure that it “send[s]

² Both parties agree that “and alerts *the devices*” recited in claim 28 refers to “devices that . . . have been affected by the anomaly,” as opposed to referring to all of the “plurality of devices.” PO Resp. 17; Tr. 27, 63. Although we note the claim may be unclear in this respect, applying the prior art in this case would result in the same conclusion under either reading.

notice to the source that a security problem originated at the source's location.” Dec. 14–15. Our understanding was that by determining the source of the security problem, Aucsmith discloses determining devices that have been affected by such problem. Patent Owner argues, however, that in the cited Aucsmith passage, the anomaly is not detected by server 104, as required, but is detected by one of the client terminals, and simply reported to server 104. PO Resp. 19–20. Patent Owner's argument relies on the premise we rejected above—that Aucsmith does not disclose server 104 itself detecting anomalies.

Further, Aucsmith explicitly discloses notifying those devices. Ex. 1004 ¶ 58 (“[s]uch follow up may include sending notice to the source that a security problem originated at the source's location.”). Indeed, Aucsmith discloses that it “typically notifies all of the client terminals 102(1)–102(N)” of an anomaly. Ex. 1004 ¶ 51. Because alerting *all devices* necessarily includes alerting those devices determined to have been affected by an anomaly (*see* Tr. 63:1–19), a subset of all devices on the network, we are persuaded that Aucsmith discloses this limitation.

Thus, we are persuaded that Petitioner has shown by a preponderance of the evidence that claim 28 is anticipated by Aucsmith.

4. Claim 30

Claim 30 depends from claim 26, adding that “the anomaly comprises one of an intrusion, an intrusion attempt, and reconnaissance activity.” Petitioner asserts that Aucsmith discloses this additional limitation because it discusses “[t]he entity may set up an intrusion detection system,” and “[r]esponsibilities of the server 104 may include . . . detecting intrusion

patterns or new intrusion techniques.” Pet. 47 (citing Ex. 1004 ¶¶ 2, 27; Ex. 1003 ¶¶ 166–69).

Patent Owner does not separately argue that Aucsmith does not teach the additional limitation of claim 30. We are persuaded that Petitioner has shown by a preponderance of the evidence that claim 30 is anticipated by Aucsmith.

5. Claims 31 and 32

Claim 31 depends from claim 26, adding that “the data collection and processing center detects the anomaly by analyzing a plurality of data packets with respect to predetermined patterns.” Claim 32 depends from claim 31, adding that “the data collection and processing center analyzes data packets that have been received by at least two devices that are connected to the network.”

Petitioner asserts that Aucsmith discloses the additional limitation of claim 31 because it discusses that information communicated within the network may be in packets and server 104 may perform actions including “inspecting all incoming and outgoing information (e.g., packets).” Pet. 47–48 (citing Ex. 1004 ¶¶ 22, 39, 50; Ex. 1003 ¶¶ 170–73). For claim 32, Petitioner relies on several passages of Aucsmith, including the statement that “server 104 can also use the possible security problems reported by all of the agents 106(1)–106(N) to help detect intrusion patterns.” *Id.* at 48–49 (citing Ex. 1004 ¶¶ 13, 22, 39, 44, 46, 50; Ex. 1003 ¶¶ 174–77).

Like its arguments with respect to claim 26, Patent Owner argues that Petitioner does not show that server 104 performs this function, as opposed to the distributed agents. PO Resp. 20–22 (citing Ex. 2011 ¶ 54–55). For claim 32, Patent Owner relies on the arguments it makes for claim 26 and

31. *Id.* at 23–25 (citing Ex. 2011 ¶ 59). Petitioner responds that claim 31 does not require the data collection and processing center to analyze the data packets firsthand or directly. Reply 9–10. Instead, Petitioner argues that claims 31 and 32 encompass situations where the data collection and processing center analyzes information about data packets it receives from distributed agents. *Id.* at 10–11.

For the reasons discussed above with respect to claim 26, we agree that claims 31 and 32 are broad enough to encompass the situation described by Aucsmith where distributed agents analyze data and forward the results on to server 104 for further analysis. Thus, we are persuaded that Petitioner has shown by a preponderance of the evidence that claims 31 and 32 are anticipated by Aucsmith.

6. Claim 33

Claim 33 depends from claim 26, adding that “the data collection and processing center adjusts anomaly detection sensitivity and alarm thresholds based on the detected anomaly.” Petitioner asserts that Aucsmith discloses this additional limitation because it discusses notifying the firewall of the anomaly and “modifying security procedures to account for the anomaly, or performing other similar tasks.” Pet. 49 (citing Ex. 1004 ¶¶ 52, 54, Fig. 2; Ex. 1003 ¶¶ 178–81).

Patent Owner argues that none of the portions of Aucsmith that Petitioner relies on show adjusting anomaly detection sensitivity and alarm thresholds as required. PO Resp. 25–27 (citing Ex. 2011 ¶¶ 62–64). Specifically, Patent Owner asserts that “modifying security procedures” would not have disclosed to one of ordinary skill in the art adjusting either anomaly detection sensitivity or alarm thresholds in particular. *Id.* at 26.

We agree with Patent Owner that Petitioner does not provide sufficient evidence that Aucsmith discloses “adjusting anomaly detection sensitivity and alarm thresholds” sufficient to show anticipation. Dr. Kesidis’s testimony just repeats the language from Aucsmith quoted above and concludes that “Aucsmith discloses each and every limitation of claim 33.” Ex. 1003 ¶¶ 178–81. Dr. Kesidis, however, does not explain why a person of ordinary skill would understand “modifying security procedures” to disclose “adjusts anomaly detection sensitivity and alarm thresholds.” *Id.* Dr. Goldschlag, on the other hand, states that “[o]ne of ordinary skill in the art would *not* have understood this term to disclose adjusting either anomaly detection sensitivity or alarm thresholds.” Ex. 2011 ¶ 62 (emphasis added).

Thus, we are not persuaded that Petitioner has shown by a preponderance of the evidence that claim 33 is anticipated by Aucsmith.

ORDER

Accordingly, it is:

ORDERED that claims 26, 28, and 30–32 of the ’084 patent are determined to be *unpatentable*; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2014-00801
Patent 6,715,084 B2

PETITIONER:

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 Strang
Lori Gordon
STERNE, KESSLER, GOLDSTEIN & FOX
jstrang-PTAB@skgf.com
lgordon-PTAB@skgf.com

Donald J. Coulman
Tim Seeley
INTELLECTUAL VENTURES
dcoulman@intven.com
tim@intven.com