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

Paper 35
Entered: October 21, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION,
Petitioner,

v.

INTELLECTUAL VENTURES II LLC,
Patent Owner.

Case IPR2014-00682
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, International Business Machines Corporation, filed a Corrected Petition (Paper 4, "Petition" or "Pet.") requesting an *inter partes* review of claims 19, 20, and 22–33 of U.S. Patent No. 6,715,084 B2 (Ex. 1004, "the '084 patent"). On October 30, 2014, we instituted a review (Paper 11, "Decision to Institute" or "Dec.") based upon Petitioner's assertion that (1) claims 26, 28, and 30–33 are unpatentable, under 35 U.S.C. § 103(a), over the combination of Porras[1] and Cheswick,[2] and (2) claims 26 and 30–32 are unpatentable, under 35 U.S.C. § 102(b), as anticipated by NetRanger.[3] Dec. 22. Petitioner provides a Declaration from Dr. Steven M. Bellovin (Ex. 1001), and Patent Owner provides a Declaration from Dr. David Goldschlag (Ex. 2017).

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 30–33 are unpatentable.

B. Related Matters

At the time of filing the Petition in this proceeding, IBM filed another petition for *inter partes* review in IPR2014-00681 challenging claims 1–9

---

[1] Phillip A. Porras & Alfonso Valdes, *Live Traffic Analysis of TCP/IP Gateways*, In Proceedings of the 1998 ISOC Symposium on Network and Distributed Sys. Security 1–13, (Dec. 12, 1997) (Ex. 1005) ("Porras").

[2] William R. Cheswick & Steven M. Bellovin, *Firewalls and Internet Security* 001–005, (1st ed. 1994) (Ex. 1008) ("Cheswick").

[3] NetRanger™ User's Guide Version 1.3.1, WheelGroup Corp. 001–327, (1997) (Ex. 1007) ("NetRanger").

and 12–18 of the '084 patent. We denied institution in that proceeding and denied Petitioner's subsequent request for rehearing. *See* IPR2014-00681, Papers 11, 14.

Subsequent to IBM's filings, another petitioner also filed two petitions challenging claims of the '084 patent in IPR2014-00793 and IPR2014-00801. We denied institution and a subsequent request for rehearing in IPR2014-00793. *See* IPR2014-00793, Papers 7, 9. We instituted *inter partes* review in IPR2014-00801 on December 1, 2015. IPR2014-00801, Paper 7 (final written decision being issued concurrently).

IBM indicates that the '084 patent is the subject of concurrent proceedings in various district courts, none of which name IBM as a defendant. *See* Paper 32 (Petitioner's Amended Mandatory Notices) 2–3; Paper 9 (Petitioner's Amended Mandatory Notices) 2–3.

C. The '084 Patent

The '084 patent relates to network-based intrusion detection systems. Ex. 1004, 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.

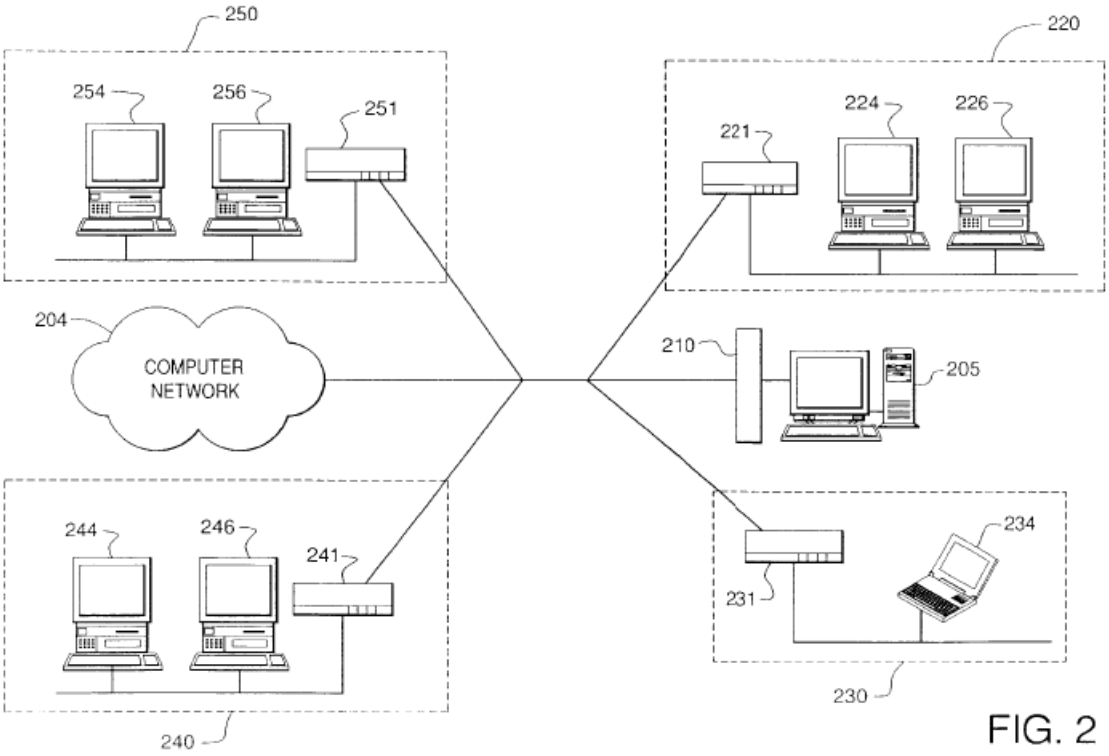

FIG. 2

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. 1004, 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.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.