Trials@uspto.gov
571-272-7822

Paper 8
Entered: July 25, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FINJAN, INC.,
Petitioner,

v.

FIREEYE, INC.,
Patent Owner.

Case IPR2014-00492
Patent 8,171,553 B2

Before BRYAN F. MOORE, LYNNE E. PETTIGREW, and FRANCES L. IPPOLITO, *Administrative Patent Judges.*

IPPOLITO, *Administrative Patent Judge.*

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

I. INTRODUCTION

Finjan, Inc. filed a Corrected Petition ("Pet.") on March 21, 2014, requesting an *inter partes* review of claims 1–30 of U.S. Patent No. 8,171,553 B2 ("the '553 patent"). Paper 4. Patent Owner FireEye, Inc. filed a Preliminary Response ("Prelim. Resp.") to the Petition. Paper 7. We have jurisdiction under 35 U.S.C. § 314.

Pursuant to 35 U.S.C. § 314, we conclude there is a reasonable likelihood that Petitioner would prevail with respect to claims 1, 3–8, 12–14, 16–20, and 22–30 of the '553 patent. Additionally, we conclude that Petitioner has not shown a reasonable likelihood that it would prevail with respect to claims 2, 9–11, 15, and 21 on the asserted grounds.

A. Related Proceedings

Related U.S. Patent No. 8,291,499 ("the '499 patent") is involved in an *inter partes* review designated IPR2014-00344. The '499 patent is a continuation of the '553 patent.

B. The '553 Patent

The '553 patent describes an authorized activity capture or detection system that analyzes copied network data with a heuristic to determine if the copied network data has the characteristics of a computer worm. *See* Ex. 1001, Claim 1. If the compared network data has a characteristic of a computer worm, the system flags the compared network data for replay in an analysis environment. *Id*. Figure 7 of the '553 patent is reproduced below.

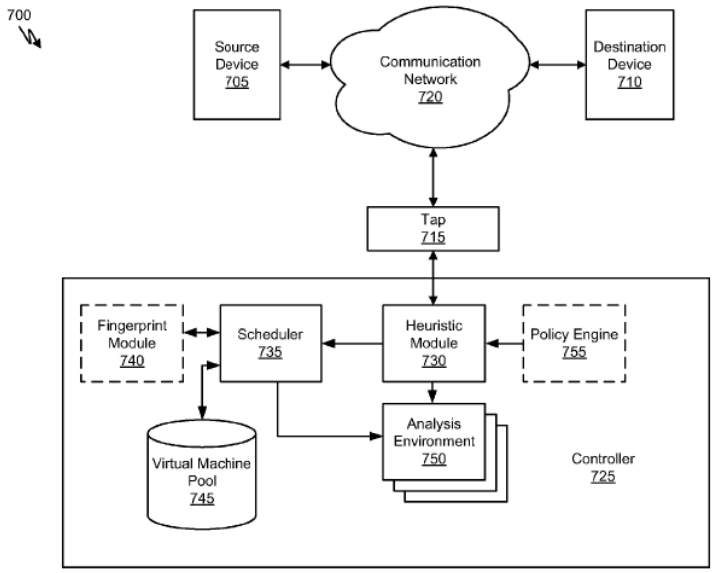

FIG. 7

Figure 7 depicts an embodiment of an unauthorized activity detection system described in the '553 patent. Unauthorized activity detection system 700 includes source device 705, destination device 710, and tap 715, each of which is coupled to communication network 720. *Id*. at col. 26, ll. 21–26. Tap 715 is further coupled to controller 725. *Id*. at col. 26, ll. 25–26. In operation, tap 715 monitors network data and provides a copy of the network data to controller 725. *Id*. at col. 26, ll. 35–37.

Figure 7 also shows controller 725, which "can be any digital device or software that receives network data from the tap 715." Ex. 1001, col. 27, ll. 1–2. "In some embodiments, controller 725 is contained within computer worm sensor 105." *Id*. at col. 27, ll. 2–4. Controller 725 may also be contained within separate traffic analysis device 135 or may be a stand-alone digital device. *Id*. at col. 27, ll. 4–6. Controller 725 can comprise virtual machine pool 745, analysis environment 750, heuristic module 730, and policy engine 755. Ex. 1001, col. 27, ll. 6–9. "[V]irtual machine pool 745 is

configured to store virtual machines [and] . . . can be any storage capable of storing software." *Id*. at col. 28, ll. 51–52. Additionally, "analysis environment 750 simulates transmission of the network data between the source device 705 and the destination device 710 to analyze the effects of the network data upon the destination device 710." *Id*. at col. 28, ll. 59–62. Heuristic module 730 can receive copied network data from tap 715 and apply heuristic and/or probability analysis to determine if the network data contains suspicious activity. *Id*. at col. 27, ll. 12–15.

C. Illustrative Claim

Of the challenged claims, claims 1, 8, 17, and 28 are independent. Claim 1, reproduced below, is illustrative of the subject matter of the '553 patent:

> 1. An unauthorized activity capture system comprising:
>
> a tap configured to copy network data from a communication network; and
>
> a controller coupled to the tap and configured to receive the copy of the network data from the tap, analyze the copy of the network data with a heuristic to determine if the copy of the network data has one or more characteristics of a computer worm, flag at least a portion of the copy of the network data as suspicious by flagging the at least a portion of the copy of the network data for replay in an analysis environment based upon the heuristic determination that the at least a portion of the analyzed copy of the network data has one or more characteristics of a computer worm, and replay transmission of the suspicious, flagged network data copied from the communication network to a destination device.

D. The Prior Art

Petitioner relies on the following prior art:

1. Peter M. Chen, et al., *When Virtual Is Better Than Real*, Department of Electrical Engineering and Computer

Science, University of Michigan (May 21, 2001) (Ex. 1009, "Chen").

2. George W. Dunlap, et al., *ReVirt: Enabling Intrusion Analysis through Virtual-Machine Logging and Replay*, Proceeding of the 5th Symposium on Operating Systems Design and Implementation, USENIX Association (Dec. 9, 2002) (Ex. 1008, "Dunlap");
3. Paul Venezia, *NetDetector Captures Intrusions*, InfoWorld Issue 27 (July 14, 2003) (Ex. 1005, "Venezia");
4. Michael Liljenstam, et al., *Simulating Realistic Network Worm Traffic for Worm Warning System Design and Testing*, Institute for Security Technology Studies, Dartmouth College (Oct. 27, 2003) (Ex. 1007, "Liljenstam"); and
5. Merike Kaeo, *Designing Network Security*, Cisco Press (Nov. 2003) (Ex. 1006, "Kaeo").

E. The Asserted Grounds

Petitioner asserts that the challenged claims are unpatentable based on the following grounds:

Reference[s]	**Basis**	**Claims Challenged**
Venezia	§ 102	17, 22, 24, 25, 26, 28
Kaeo and Venezia	§ 103	1–5, 7, 17, 21, 22, 25–28, 30
Kaeo, Venezia, and Dunlap	§ 103	8–13, 15, 16, 18, 20, 29
Kaeo, Venezia, and Chen	§ 103	6, 8–14, 16, 18, 19, 29
Kaeo and Liljenstam	§ 103	1–5, 7, 17, 21–28
Kaeo, Liljenstam, and Dunlap	§ 103	8–13, 15, 16, 18, 20, 29, 30
Kaeo and Chen	§ 103	1–14, 16–19, 21–30

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.