Trials@uspto.gov
571-272-7822

Paper 7
Entered: March 29, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

FINJAN, INC.,
Patent Owner.

Case IPR2015-01974
Patent 7,647,633 B2

Before, THOMAS L. GIANNETTI, MIRIAM L. QUINN, and PATRICK M. BOUCHER *Administrative Patent Judges.*

QUINN, *Administrative Patent Judge.*

DECISION
Partial Institution of *Inter Partes* Review
37 C.F.R. § 42.108; 35 U.S.C. § 325(d)

Palo Alto Networks, Inc. ("Petitioner") filed a Petition to institute *inter partes* review of claims 1–4, 6–8, 13, 14, 19, 28, and 34 of U.S. Patent No. 7,647,633 B2 ("the '633 patent") pursuant to 35 U.S.C. § 311–319. Paper 1 ("Pet."). Finjan, Inc. ("Patent Owner") timely filed a Preliminary Response. Paper 6 ("Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314.

For the reasons that follow, we institute *inter partes* review of claims 14 and 19, and exercise our discretion under 35 U.S.C. § 325(d) to deny the asserted challenges to all other claims.

I. BACKGROUND

A. RELATED MATTERS

Petitioner identifies the '633 patent as the subject matter of various district court cases filed in the U.S. District Court for the Northern District of California (Case Nos. 3-14-cv-04908, 13-cv-03133, 13-cv-03999, 5-13-cv-04398, 13-cv-05808, and 5-15-cv-01353). Pet. 2. Petitioner also states that petitions for *inter partes* review have been filed regarding other patents assigned to Patent Owner. *Id.*

More importantly, certain claims of the '633 patent are undergoing *ex parte* reexamination. *Id.* at 2, 12–13; *See* Ex. 1003. The final rejection of the claims undergoing reexamination has been appealed to the Board. *See* Ex. 1029. The details of the reexamination are discussed in more detail below.

B. THE ’633 PATENT (EX. 1001)

The ’633 patent relates to a system and a method for protecting network-connectable devices from undesirable downloadable operation. Ex. 1001, 1:30–33. The patent describes that “Downloadable information comprising program code can include distributable components (e.g. JavaTM applets and JavaScript scripts, ActiveXTM controls, Visual Basic, add-ins and/or others).” *Id.* at 1:60–63. Protecting against only some distributable components does not protect against application programs, Trojan horses, or zip or meta files, which are other types of Downloadable Information. *Id.* at 1: 63–2:2. The ’633 patent “enables more reliable protection.” *Id.* at 2:27–28. According to the Summary of the Invention,

> In one aspect, embodiments of the invention provide for determining, within one or more network “servers” (e.g. firewalls, resources, gateways, email relays or other devices/processes that are capable of receiving-and-transferring a Downloadable) whether received information includes executable code (and is a “Downloadable”). Embodiments also provide for delivering static, configurable and/or extensible remotely operable protection policies to a Downloadable-destination, more typically as a sandboxed package including the mobile protection code, downloadable policies and one or more received Downloadables. Further client-based or remote protection code/policies can also be utilized in a distributed manner. Embodiments also provide for causing the mobile protection code to be executed within a Downloadable-destination in a manner that enables various Downloadable operations to be detected, intercepted or further responded to via protection operations. Additional server/information-destination device security or other protection is also enabled, among still further aspects.

Id. at 2:39–57.

C. Illustrative Claim

Challenged claims 1, 8, 13, 14, 28, and 34 are independent. Illustrative claims 1 and 14 are reproduced below.

> 1. A computer processor-based method, comprising:
> receiving, by a computer, downloadable-information;
> determining, by the computer, whether the downloadable-information includes executable code; and
> based upon the determination, transmitting from the computer mobile protection code to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.
>
> 14. A computer program product, comprising a computer usable medium having a computer readable program code therein, the computer readable program code adapted to be executed for computer security, the method comprising:
> providing a system, wherein the system comprises distinct software modules, and wherein the distinct software modules comprise an information re-communicator and a mobile code executor;
> receiving, at the information re-communicator, downloadable-information including executable code; and
> causing mobile protection code to be executed by the mobile code executor at a downloadable-information destination such that one or more operations of the executable code at the destination, if attempted, will be processed by the mobile protection code.

Id. at 20:54–62, 21:58–22:5

Reference(s)	Basis	Challenged Claims
Shin[1]	§ 103	1–4, 6–8, 13, 14, and 19
Poison Java[2]	§ 102	28
Poison Java and Shin	§ 103	1
Poison Java and Brown[3]	§ 103	14, 19, and 34

II. ANALYSIS

Petitioner acknowledges that claims 1–7 and 28–33 of the ’633 patent are (or were) subject to *ex parte* reexamination (Control No. 90/013,016), which resulted in a Final Office Action rejecting the claims over (at least in part) Ji.[4] Pet. 12–13. According to Patent Owner, Ji discloses the same “applet instrumentation prior art” that Petitioner asserts as prior art in this Petition, namely Poison Java. Prelim. Resp. 17–21. Patent Owner also asserts that the same techniques described in Ji are disclosed in Shin.

[1] Insik Shin, et al., *Java Bytecode Modification and Applet Security* (Technical Report, Computer Science Dept., Stanford University, 1998), https://web.archive.org/web/19980418130342/http://www-cs-students.stanford.edu/~ishin/reserach.html (Ex. 1009) (”Shin”).

[2] Eva Chen, *Poison Java*, IEEE SPECTRUM, August 1999 at 38 (Ex. 1004) (“Poison Java”).

[3] Mark W. Brown, et al., SPECIAL EDITION USING NETSCAPE 3, (Que Corp. 1996) (Ex. 1041) (“Brown”).

[4] U.S. Patent No. 5,983,348 (Ex. 2006) (“Ji”).

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.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.