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

Paper 8
Entered: September 11, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00812
Patent 8,850,009 B2

Before KARL D. EASTHOM, JENNIFER S. BISK, and GREGG I. ANDERSON, *Administrative Patent Judges.*

BISK, *Administrative Patent Judge*.

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

INTRODUCTION

A. Background

Petitioner, Apple Inc., filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of claims 1–8, 10–20, and 22–25 (the "challenged claims") of U.S. Patent No. 8,850,009 B2 (Ex. 1003, "the '009 patent"). Patent Owner, VirnetX Inc.,[1] 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 in showing the unpatentability of at least one of the challenged claims. Accordingly, we institute *inter partes* review.

B. Related Matters

The parties indicate that the '009 patent "and/or" related patents are involved in several proceedings in the United States District Court for the

[1] The Petition also names Science Application International Corporation as Patent Owner. However, the Patent Owner Preliminary Response names only VirnetX.

Eastern District of Texas.[2] Pet. 6–7; Paper 5, 12–13. Petitioner also filed another petition seeking *inter partes* review of the '009 patent—IPR2015-00813. Pet. 2. In addition, many other *inter partes* review and *inter partes* reexamination proceedings challenging related patents are currently, or have been recently, before the Office.[3]

C. The Asserted Grounds of Unpatentability

Petitioner contends that claims 1–8, 10–20, and 22–25 of the '009 patent are unpatentable under 35 U.S.C. § 103 based on the combination of Beser[4] and RFC 2401.[5] Petitioner also provides testimony from Dr. Roberto Tamassia. Ex. 1005.

D. The '009 Patent

The '009 patent describes secure methods for communicating over the Internet. Ex. 1003, 10:16–17. Specifically, the '009 patent describes "the automatic creation of a virtual private network (VPN) in response to a

---

[2] In the future, Petitioner is advised that referring to "numerous lawsuits," without specifically identifying the court in which the lawsuit is taking place and other information necessary to identify the proceeding may be considered a violation of 37 C.F.R. § 42.8. *See* Pet. 6–7. Similarly, Patent Owner is advised to be specific in addressing whether the challenged patent is actually the subject of the enumerated related litigation. *See* Paper 5, 12–13.

[3] In this section, the Petition did not identify specifically any other proceeding before the Office other than IPR2015-00813. Pet. 2. In the future, such omission may be construed as a violation of 37 C.F.R. § 42.8.

[4] U.S. Patent No. 6,496,867 B1 (Ex. 1007) ("Beser").

[5] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998 (Ex. 1008) ("RFC 2401").

domain-name server look-up function." *Id.* at 39:36–38. This automatic creation makes use of a modified Domain Name Server as opposed to a conventional Domain Name Server (DNS), which is described as follows:

> Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP address of a requested computer or host. For example, when a computer user types in the web name "Yahoo.com," the user's web browser transmits a request to a DNS, which converts the name into a four-part IP address that is returned to the user's browser and then used by the browser to contact the destination web site.

Id. at 39:39–45.

The modified DNS server may include both a conventional DNS and a DNS proxy. *Id.* at 40:33–35. The DNS proxy of the modified DNS server intercepts all DNS lookup requests, determines whether the user has requested access to a secure site (using for example, a domain name extension or an internal table of secure sites) and if so, whether the user has sufficient security privileges to access the requested site. *Id.* at 40:39–45. If the user has requested access to a secure site to which it has insufficient security privileges, the DNS proxy returns a "'host unknown'" error to the user. *Id.* at 40:62–65. If the user has requested access to a secure site to which it has sufficient security privileges, the DNS proxy requests a gatekeeper to create a VPN between the user's computer and the secure target site. *Id.* at 40:45–51. The DNS proxy then returns to the user the resolved address passed to it by the gatekeeper, which need not be the actual address of the destination computer. *Id.* at 40:51–57.

The VPN is "preferably implemented using the IP address 'hopping' features," (changing IP addresses based upon an agreed

upon algorithm) described elsewhere in the '009 patent, "such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted." *Id.* at 40:18–22.

E. Illustrative Claim

Claims 1 and 14 of the '009 patent are independent. Claim 1 is illustrative of the claimed subject matter and recites:

1. A network device, comprising:

a storage device storing an application program for a secure communications service; and

at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:

send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device;

receive, following interception of the DNS request and a determination that the second network device is available for the secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link;

connect to the second network device over the encrypted communication link, using the received network address of the second network device and the provisioning information for the encrypted communication link; and

communicate data with the second network device using the secure communications service via the encrypted communication link,

the network device being a device at which a user uses the secure communications service to access the encrypted communication link.

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.