Trials@uspto.gov
571-272-7822

Paper 15
Date: May 14, 2014

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.
Petitioner

v.

VIRNETX INC.
Patent Owner

Case IPR2014-00237
Patent 8,504,697 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and STEPHEN C. SIU, *Administrative Patent Judges.*

EASTHOM, *Administrative Patent Judge*.

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

I. BACKGROUND

A. Introduction

Apple Inc. ("Petitioner") filed a Petition requesting *inter partes* review of claims 1–11, 14–25, and 28–30 of U.S. Patent No. 8,504,697 B2 ("the '697 Patent," Ex. 1001) pursuant to 35 U.S.C. §§ 311-319.[1] Paper 1 ("Pet."). In response, VirnetX, Inc. ("Patent Owner") filed a Preliminary Response. Paper 12 ("Prelim. Resp.").

We have jurisdiction under 35 U.S.C. § 314. The standard for instituting *inter partes* review is set forth in 35 U.S.C. § 314 (a), which follows:

> THRESHOLD -- The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.

We determine, based on the record, that Petitioner has demonstrated, under 35 U.S.C. § 314(a), that there is a reasonable likelihood of unpatentability with respect to at least one of the challenged claims.

Petitioner relies on the following prior art:

U.S. Patent No. 6,496,867 B1 (issued Dec. 17, 2002, filed Aug. 27, 1999) ("Beser") Ex. 1009.

S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401 (Nov. 1998) ("RFC 2401"). Ex. 1010

[1] The '697 Patent lists continuation-in-part status back to October 29, 1999. The '697 Patent also lists related provisional applications, but does not claim continuity to those applications. Petitioner sets forth reasons why the '697 Patent only supports the independent claims back to February 15, 2000. *See* Pet. 3–5. Based on Petitioner's preliminary showing, for purposes of this decision, we assume that the earliest effective filing date is February 15, 2000. Patent Owner has not challenged this date on this record.

M. Handley et al., *SIP: Session Initiation Protocol*, Request for Comments: 2543 (Mar. 1999) ("RFC 2453"). Ex. 1012.

H. Schulzrinne et al., *RTP: A Transport Protocol for Real-Time Applications*, Request for Comments: 1889 (Jan. 1996) ("RFC 1889"). Ex. 1013.

M. Handley and V. Jacobson, *SDP: Session Description Protocol*, Request for Comments: 2327 (Apr. 1998) ("RFC 2327"). Ex. 1014.

Elin Wedlund and Henning Schulzrinne, *Mobility Support Using SIP*, WoWMoM 99, 76–82 (1999) ("Mobility Support"). Ex. 1015.

P. Mockapetris, *Domain Names – Concepts and Facilities*, Request for Comments: 1034 (Nov. 1987), http://www.ietf.org/rfc/rfc1034.txt (last visited on July 8, 2011) ("RFC 1034"). Ex. 1016.

P. Mockapetris, *Domain Names – Implementation and Specification*, Request for Comments: 1035 (Nov. 1987), http://tools.ietf.org/html/rfc1035 (last visited on July 8, 2011) ("RFC 1035"). Ex. 1017.

Petitioner contends that the challenged claims are unpatentable under 35 U.S.C. § 102 and § 103 based on the following specific grounds. Pet. 3.

Reference(s)	**Basis**	**Claims challenged**
Beser	§ 102 (e)	1–11, 14–25, and 28–30
RFC 2453	§ 102 (a)	1–11, 14–25, and 28–30
Beser and RFC 2401	§ 103(a)	1–11, 14–25, and 28–30
RFC 2453, RFC 1889, and RFC 2327	§ 103(a)	1–11, 14–25, and 28–30
RFC 2453 and Mobility Support	§ 103(a)	8, 9, 22, and 23

B. The ’697 Patent

To provide a secure network, the ’697 Patent system modifies conventional Domain Name Servers, which the ’697 Patent describes as follows:

> Conventional Domain Name Servers (DNSs) provide a look-up function that returns the IP [Internet Protocol] 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.

Ex. 1001, 39:32–38.

The ’697 Patent system establishes a secure communication link between a first computer and a second computer using a specialized DNS server that traps DNS requests. Prior to setting up the secure network or Virtual Private Network (“VPN”), a DNS proxy server determines, using a domain name extension, a table, or a rule, or by requesting further information from the user, whether the user has sufficient security privileges to access a desired target site. *See* Ex. 1001, 41:6–64. If so, the proxy DNS requests a gatekeeper to set up a secure communication link between the user and target by passing a “resolved” address or “hopblocks” for the addresses. *See* Ex. 1001, 40:37–65; Fig. 27. Any of various fields can be “hopped,” for example, “IP source/destination addresses” or “a field in the header.” Ex. 1001, 41:38–39. If the user lacks sufficient security privileges, the system returns a “HOST UNKNOWN” error message. Ex. 1001, Fig. 27.

In other words, to provide security, the proxy server does not send back the true IP address of the target computer. *See* Ex. 1001, 40:1–20. For example, the proxy server may receive the client’s DNS request, which forwards it to a gatekeeper, which returns a “resolved” destination address to the proxy based on a "resolved" name, which then forwards the "resolved address" back to the client "in a secure administrative VPN." *See* Ex. 1001, 41:49–56.

Claims 2–11, 14–25, and 28–30 depend from independent claims 1 or 16, which follow:

> 1. A method of connecting a first network device and a second network device, the method comprising:
>
> intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;
>
> determining, in response to the request, whether the second network device is available for a secure communications service; and
>
> initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;
>
> wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.
>
> 16. A system for connecting a first network device and a second network device, the system including one or more servers configured to:
>
> intercept, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;
>
> determine, in response to the request, whether the second network device is available for a secure communications service; and
>
> initiate a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service,
>
> wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

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.