Trials@uspto.gov
571-272-7822

Paper No. 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 IPR2015-00811
Patent 8,868,705 B2

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

ANDERSON, *Administrative Patent Judge*.

DECISION

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

I. INTRODUCTION

Apple Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–34 of U.S. Patent No. 8,868,705 B2 (Ex. 1001, "the '705 patent"). VirnetX Inc. ("Patent Owner")[1] filed a Preliminary Response. Paper 6 ("Prelim. Resp."). We have jurisdiction under 35 U.S.C. § 314.

For the reasons explained below, we institute an *inter partes* review of claims 1–34 of the '705 patent. We have not yet made a final determination with respect to the patentability of any claim.

A. Related Matters

Petitioner fails to identify directly or generally any lawsuits where the '705 patent has been asserted against it.[2] Patent Owner has asserted the '705 patent, or patents in the same family as the application, which resulted in the '705 patent, against Petitioner in four different lawsuits. Paper 5, 12–13.[3]

---

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

[2] Petitioner is advised that its failure to identify any judicial or all administrative matters relating to the '705 patent which would affect or be affected by a decision here may be considered a violation of 37 C.F.R. § 42.8. *See* Pet. 2.

[3] Patent Owner is advised to be specific in addressing whether the challenged patent is actually the subject of the enumerated related litigation instead of stating the '705 patent "and/or other patents that stem from the same applications that led to the '705 patent." In the future, general statements such as this may be considered a violation of 37 C.F.R. § 42.8. *See* Paper 5, 12–13.

Petitioner also filed another petition seeking *inter partes* review of the '705 patent—IPR2015-00810 ("the '810 IPR"). Pet. 2.[4] In addition, many other *inter partes* review and *inter partes* reexamination proceedings challenging related patents are currently, or have been recently, before the Office. Paper 5, 3–10.

B. The '705 Patent

The '705 patent describes a system and method for transparently creating an encrypted communications channel between a client device and a target device. Ex. 1001, Abstract, Figs. 26, 27 (elements 2601, 2604). Secure communication is based on a protocol called the "Tunneled Agile Routing Protocol" or "TARP." *Id.* at 3:16–19. Once the encrypted communications channel is created, the devices are configured to allow encrypted communications between themselves over the encrypted communications channel. *Id.* at 40:65–41:9.

[4] Again, Petitioner potentially failed to meet its obligation under 37 C.F.R. § 42.8. There are numerous other proceedings regarding related patents which may be affected by the decision in this proceeding which are not listed in the Petition. *See* Paper 5.

Figure 26 is reproduced below.

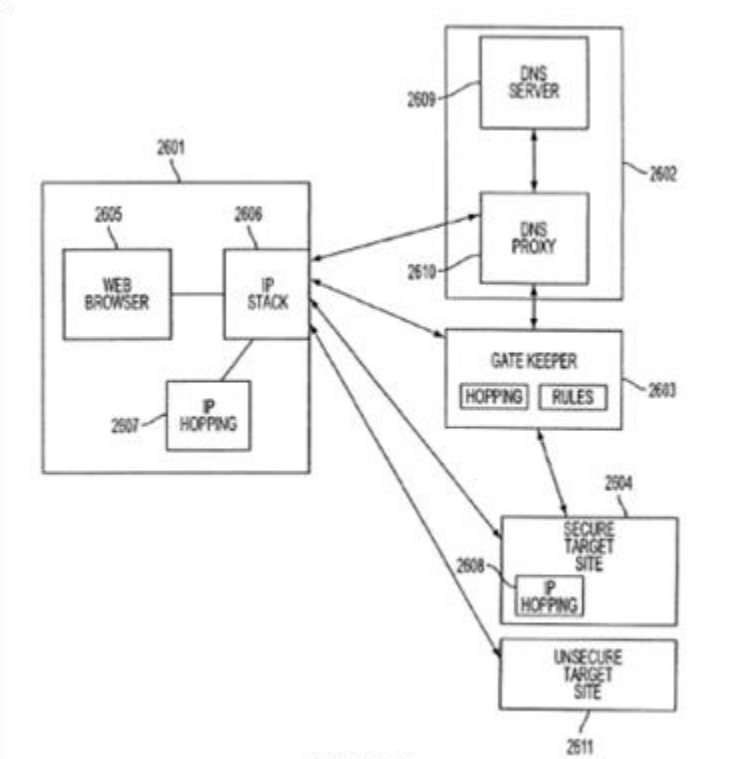

FIG. 26

Referring to Figure 26, user's computer 2601 is a conventional client, e.g., a web browser. Ex. 1001, 39:58–60. Gatekeeper server 2603 is interposed between modified Domain Name Server ("DNS") 2602 and secure target site 2604. *Id.* at 39:62–66. The DNS includes both conventional DNS server function 2609 and DNS proxy 2610. *Id.* Conventional IP protocols allow access to unsecure target site 2611. *Id.* at 39:66–67.

In one described embodiment, establishing the encrypted communications channel includes intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device. Ex. 1001, 40:1–19. It further includes determining whether the request to look up the IP address corresponds to a device that accepts an encrypted channel connection with

the client device. *Id.* at 40:1–29. Gatekeeper 2603 facilitates and allocates the exchange of information for secure communication, such as using "hopped" IP addresses. *Id.* at 40:32–35.

The DNS proxy server handles requests for DNS look-up for secure hosts. Ex. 1001, 40:43–45. If the host is secure, then it is determined whether the user is authorized to connect with the host. *Id.* at 40:51–53. If the user is authorized to connect, a secure Virtual Private Network (VPN) is established between the user's computer and the secure target site. *Id.* at 40:65–41:2.

C. Illustrative Claim

Petitioner challenges claims 1–34 of the '705 patent. Claim 1 is an independent method claim and claim 21 is an independent system claim. All remaining claims depend directly or indirectly from claim 1 or 21. Claim 1 is reproduced below.

> 1. A method of transparently creating an encrypted communications channel between a client device and a target device, each device being configured to allow secure data communications between the client device and the target device over the encrypted communications channel once the encrypted communications channel is created, the method comprising:
>
> (1) intercepting from the client device a request to look up an Internet Protocol (IP) address corresponding to a domain name associated with the target device;
>
> (2) determining whether the request to look up the IP address transmitted[5] in step (1) corresponds to a device that

[5] Patent Owner asserts "transmitted" was printed in error and that the limitation was amended to include "intercepted" instead of "transmitted." Prelim. Resp. 30, n.3 (citing Ex. 1002, 638–639, 641, 655–656). Patent Owner represents the error will be corrected after this decision. *Id.* Petitioner uses the printed version, i.e., "transmitted." Pet. 29, 35. The

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.