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

Paper 8
Entered: Oct. 1, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00871
Patent 8,560,705 B2

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

EASTHOM, *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 1–30 of U.S. Patent No. 8,560,705 B2 (Ex. 1050, "the '705 patent"). VirnetX Inc. ("Patent Owner") 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 1–30 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.[1] Patent Owner has asserted the '705 patent, or patents in the same family as the application that resulted in the '705 patent, against Petitioner in four different lawsuits. Paper 5, 12–13.[2]

Petitioner also filed another petition seeking *inter partes* review of the '705 patent—IPR2015-00870 ("the '810 IPR"). 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. Paper 5, 3–10.

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

[2] 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, this may be considered a violation of 37 C.F.R. § 42.8. *See* Paper 5, 12–13.

B. The ’705 Patent

The ’705 patent describes secure methods for communicating over the Internet. Ex. 1050, 9:41–46. Specifically, the ’705 patent describes “the automatic creation of a virtual private network (VPN) in response to a domain-name server look-up function.” *Id.* at 39:4–6. This automatic creation employs a modified Domain Name Server, which may include a conventional Domain Name Server (DNS):

> 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 39:7–13.

In addition to conventional DNS functionality, a modified DNS may include a DNS proxy. *Id.* at 39:67–40:2. In a described embodiment pertaining to Figure 26 (reproduced below), DNS proxy 2610 intercepts requests from client 2601 to determine whether client 2601 requests access to a secure site by using a domain extension or an internal table of such sites. *Id*. at 40:6–11. If not, DNS proxy 2610 passes the request to DNS server 2609. *Id*. at 40:53–55. If client 2601 requests access to a secure site, gatekeeper 2603 may communicate with DNS proxy 2610 and facilitate a secure VPN link, such as by using “hopped” IP addresses. *Id.* at 41:14–22.

A reproduction of Figure 26 of the ’705 patent follows:

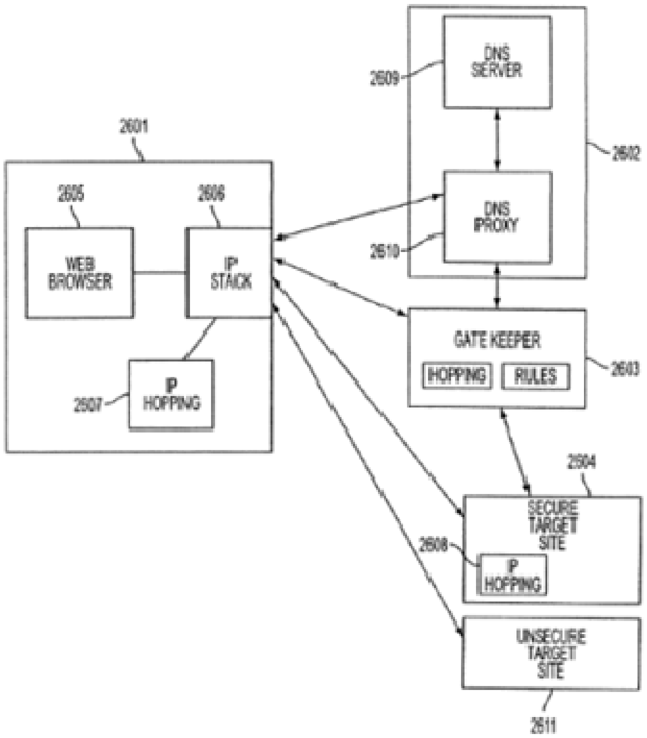

FIG. 26

Figure 26 shows user computer 2601 (which includes a web browser), gatekeeper server 2603, modified DNS 2602, secure target site 2604, and IP hopping modules 2607 and 2608. Modified DNS 2603 includes both a conventional DNS server function 2609 and DNS proxy 2610. Conventional IP protocols allow access to unsecure target site 2611. *Id.* at 39:63–40:5.

In general, DNS proxy 2610 intercepts DNS lookup requests, determines whether the user has requested access to a secure site, and if so, whether the user has sufficient security privileges to access the requested site. *Id.* at 40:6–16. 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 40:32–33. 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 link between the user's computer and the secure target site. *See id*. at 40:12–16. 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 40:19–25. A requesting user may be required to match the security level of a host. *Id*. at 40: 65–67.

The VPN communication link is "preferably implemented using the IP address 'hopping' features of the basic invention" (i.e., changing IP addresses based upon an agreed upon algorithm) "such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted." *Id.* at 39:52–56; *see id*. at 41:14–22, 50:58–14, Fig. 33 (describing IP hopping techniques used for VPN communication link 3319). According to one example, after establishing VPN link 3321 between computers 3301 and 3320 (*see* Fig. 33), "[f]urther communication occurs via the VPN, e.g., using a 'hopping' regime . . . . [over] VPN link 3321." *Id.* at 52:4–6.

C. Illustrative Claim

Claims 1 and 16 of the '705 patent are independent and of similar scope. Claim 1, illustrative of the challenged claims, follows:

> 1. A client device comprising:
>
> (a) memory configured and arranged to facilitate a connection of the client device with a target device over a secure communication link created based on
>
> (i) interception of a request, generated by the client device, to look up an internet protocol (IP) address of the target

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.