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*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Petitioner, Apple Inc., filed a Petition (Paper 1, "Pet.") seeking an *inter partes* review of claims 1–30 of U.S. Patent No. 8,560,705 B2 (Ex. 1050, "the '705 patent") pursuant to 35 U.S.C. §§ 311–319. Pet. 2–3. After VirnetX Inc., Patent Owner, filed a Preliminary Response (Paper 6, "Prelim. Resp."), we instituted an *inter partes* review of claims 1–30 (Paper 8, "Institution Decision" or "Inst. Dec."). Inst. Dec. 2.

Subsequent to institution, Patent Owner filed a Patent Owner Response (Paper 23, "PO Resp."), and Petitioner filed a Reply (Paper 26, "Pet. Reply"). Patent Owner also filed a Motion to Exclude evidence (Paper 30), Petitioner filed an Opposition (Paper 33), and Patent Owner filed a Reply to the Opposition (Paper 34). Petitioner relies on, *inter alia*, the "Declaration of Roberto Tamassia Regarding U.S. Patent Nos. 8,458,341, 8,516,131, and 8,560,705." Ex. 1005 (the "Tamassia Declaration"). Patent Owner relies on, *inter alia*, the "Declaration of Fabian Monrose, Ph.D." Ex. 2018 (the "Monrose Declaration"). The Board filed a transcription of the Oral Hearing held on June 27, 2016. Paper 38. This Final Written Decision issues concurrently with the final written decision involving the '705 patent in *Apple Inc. v. VirnetX Inc.*, IPR2015-00870 (PTAB Sept. 28, 2016) (Paper No. 39, "'870 FWD") (generally "'870 IPR").

The Board has jurisdiction under 35 U.S.C. § 6(c). This Final Written Decision issues pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. For the reasons that follow, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–30 of the '705 patent are unpatentable.

A. The '705 Patent (Ex. 1050)

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.

"A modified DNS server 2602 includes a conventional DNS server function 2609 and a DNS proxy 2610," which may "combined into a single server for convenience." *Id.* at 39:67–40:2, 40:45–46. 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, determines 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 between the user's computer and the secure target site. *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.

The VPN is "preferably implemented using . . . IP address 'hopping' features," (changing IP addresses based upon an agreed upon algorithm) described in the '705 patent, "such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted." *See id.* at 39:52–56. The system may hide the identities (i.e., anonymity, a form of security) by encrypting parts of packets. *See id.* at 1:50–56, 9:41–10:17. Routers along the hopping path determine the "next-hop in a series of . . . router hops" (*id.* at 9:52–53) in the path, by authenticating or decrypting transmitted encrypted parts of packets to find the "next-hop" router address. *See id.* at 3:23–25, 10:2–17. Data messages in the packets also may be encrypted. *See id.* at 1:50–56, 4:10–12, 11:1–9.

B. Illustrative Challenged 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 device based on a domain name associated with the target device, and
> (ii) a determination as a result of the request that the target device is a device with which a secure communication link can be established;
> (b) an application program configured and arranged so as to allow participation in audio/video communications with the target device over the secure communication link once the secure communication link is established; and

> (c) a signal processing configuration arranged to execute the application program.

Ex. 1050, 55:52–65.

C. Instituted Grounds of Unpatentability

We instituted on the following grounds asserted by Petitioner under 35 U.S.C. § 103 for obviousness: claims 1–23 and 25–30 of the '705 patent based on the combination of Aventail[1] (Ex. 1009–11), RFC 2401[2] (Ex. 1008), and RFC 2543[3] (Ex. 1013), and claim 24 as unpatentable based on the combination of Aventail (Ex. 1009–11), RFC 2401 (Ex. 1008), RFC 2543 (Ex. 1010), and Brand (Ex. 1012).[4] Inst. Dec. 21.

II. ANALYSIS

A. Claim Construction

In an *inter partes* review, the Board construes claim terms in an unexpired patent under their broadest reasonable construction in light of the specification of the patent in which they appear. *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–46 (2016); 37 C.F.R. § 42.100(b). Under this standard, absent any special definitions, claim terms or phrases carry their

---

[1] Exhibits 1009–1011 correspond to manuals that collectively describe an Aventail Connect client and ExtraNet Server software application. We refer collectively to the three manuals as "Aventail" unless otherwise noted. *See* Aventail Connect v3.01/v2.51 Administrator's Guide (Ex. 1009), Aventail Connect v3.01/v2.51 User's Guide (1996–1999) (Ex. 1010), and Aventail ExtraNet Center v3.0 Administrator's Guide (NT and UNIX) ("Aventail ExtraNet Admin. Guide") (Ex. 1011).

[2] S. Kent and Randall Atkinson, RFC 2401, *Security Architecture for the Internet Protocol,* Network Working Group, Request for Comments (Nov. 1998).

[3] Handley et al., RFC 2543, *SIP: Session Initiation Protocol*, Network Working Group, Request for Comments (Mar. 1999).

[4] U.S. Pat. No. 5,237,566 (Aug. 17, 1993).

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.

fastcase®
Smarter legal research.