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

Paper No. 10
Entered: October 7, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

MPH TECHNOLOGIES OY,
Patent Owner.

Case IPR2019-00820
Patent 7,937,581 B2

Before KAMRAN JIVANI, JOHN D. HAMANN, and STACY B. MARGOLIES, *Administrative Patent Judges.*

JIVANI, *Administrative Patent Judge.*

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Pursuant to 35 U.S.C. § 311, Petitioner Apple Inc. requests an *inter partes* review of claims 1–9 of U.S. Patent No. 7,937,581 B2 (Ex. 1001, "the '581 patent"). Paper 2 ("Petition" or "Pet."). Patent Owner MPH Technologies Oy opposes institution of the requested review. Paper 8 ("Preliminary Response" or "Prelim. Resp."). After receiving the Preliminary Response, Petitioner requested authorization to file a reply in support of its Petition; however, we denied the request for failure to show good cause, as required. Paper 9.

We have jurisdiction under 37 C.F.R. § 42.4(a) and 35 U.S.C. § 314, which provides that an *inter partes* review may not be instituted unless the information presented in the Petition "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." Having considered the arguments and evidence of record, we determine that Petitioner has shown a reasonable likelihood of prevailing with respect to at least one of the claims challenged in the Petition. Accordingly, we institute *inter partes* review of claims 1–9 based on all of the grounds identified in the Petition, as discussed herein.

II. BACKGROUND

A. The Challenged Patent (Ex. 1001)

The '581 patent states that "[t]he object of the invention is to ensure secure forwarding of messages from and to mobile terminals." Ex. 1001, 6:42–44. The '581 patent discloses that its invention is "[e]specially . . . meant for IPSec connections." *Id.* at 1:15–17.

According to the '581 patent, "IP security protocols (IPSec) provides the capability to secure communications between arbitrary hosts, e.g. across

a LAN, across private and public wide area networks (WANs) and across the internet." *Id*. at 1:59–62. More specifically, "IPSec can encrypt and/or authenticate traffic at IP level." *Id*. at 2:5. In so doing, "IPSec ensures confidentiality integrity, authentication, replay protection, limited traffic flow confidentiality, limited identity protection, and access control based on authenticated identities." *Id*. at 1:67–2:3. "In particular, identity protection is not completely handled by IPSec, and neither is denial-of-service protection." *Id*. at 1:56–58.

The '581 patent states that "IPSec is defined by certain documents, which contain rules for the IPSec architecture." *Id*. at 2:8–9. These rules describe, *inter alia*, providing "access control based on the distribution of cryptographic keys." *Id*. at 2:19–22. The '581 patent also describes the concept of a Security Association ("SA"), which according to the '581 patent is "a one-way relationship between a sender and a receiver that offers [negotiated] security services to the traffic carried on it." *Id*. at 2:24–26.

The '581 patent discloses that IPSec supports two modes of operation (i.e., transport mode and tunnel mode). *Id*. at 3:10–11. "Typically, transport mode is used for end-to-end communication between two hosts." *Id*. at 3:14–17. "Tunnel mode . . . is generally used for sending messages through more than two components," and is often used "when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec." *Id*. at 3:19–24.

"IPSec is intended to work with static network topolog[ies]," according to the '581 patent. *Id*. at 4:13–15. For example, IPSec can secure communications between hosts across a local area network ("LAN"), as well as across a private or public wide area network ("WAN"). *Id*. at 1:59–62.

Figure 1, shown below, "illustrates an example of a telecommunication network to be used in the invention" of the '581 patent. *Id*. at 8:37–38.

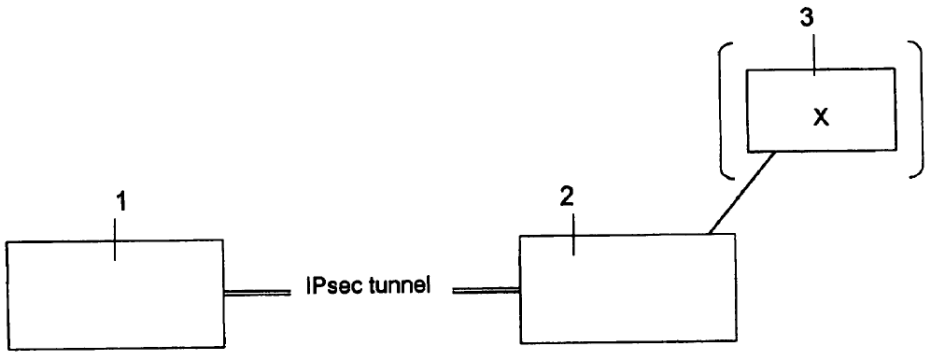

FIG. 1

Figure 1's example telecommunication network comprises "computer 1 . . .[,] a client computer[,] and computer 2[,] a destination computer, to which the secure messages are sent . . . by means of an IPSec tunnel established between computer 1 and computer 2." *Id*. at 8:51–55. The '581 patent adds: "Computer 2 [can] be a security gateway for a third computer 3. Then, the messages sent from computer 2 to computer 3 are sent in plaintext." *Id*. at 8:55–57.

The '581 patent discloses that in forming an IPSec tunnel under IPSec's default automated key management protocol (i.e., the Internet Key Exchange ("IKE") protocol), "the tunnel endpoints are fixed and remain constant." *Id*. at 4:6–19. The '581 patent adds: "If IPSec is used with a mobile host the IKE key exchange will have to be redone from every new[ly] visited network. This is problematic, because IKE key exchanges involve computationally expensive" calculations and require exchanging numerous messages between the endpoints, leading to higher latency. *Id*. at 4:19–30.

To address these problems, the '581 patent discloses avoiding a full re-negotiation between the tunnel endpoints, when computer 1 moves networks. *E.g.*, *id*. at 9:29–33 (describing prior art requires a full re-negotiation), 9:60–63. More specifically, the '581 patent discloses initially establishing an IPSec tunnel between computer 1 (address A) and computer 2 (address X) using IKE, as in the prior art. *Id*. at 9:45–10:5, Fig. 5 (illustrating steps 1a–9a for setting up the tunnel); *compare id*. at Fig. 5, *with id*. at Fig. 4 (showing the same nine steps as the prior art solution); *see also id*. at 9:12–39 (describing the prior art IKE establishment of the tunnel).

The '581 patent discloses that, when computer 1 moves from address A to address B, computer 1 sends from its new address (address B) to computer 2 (address X) at the other end of the established IPSec tunnel, a request for computer 2 to register its new address. *Id*. at 9:45–10:5. According to the '581 patent, this request can be "encrypt[ed] and/or authenticat[ed] . . . us[ing] the same IPSec SA [that is used] for protecting both data and registration traffic." *Id*. at 10:1–5.

The '581 patent thus discloses that the tunnel's IPSec SA is carried over to the new connection point, and computer 1 can send IPSec-protected messages to computer 2 after sending the request, which "essentially makes the handover latency zero." *Id*. at 10:24–36. "[T]he exact method of signaling is not important[;] the essence is to carry over the IPSec SA to the new connection point." *Id*. at 10:8–10.

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.