United States Court of Appeals for the Federal Circuit

APPLE INC.,
Appellant

v.

MPH TECHNOLOGIES OY,
Appellee

2021-1532, 2021-1533, 2021-1534

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2019-00823, IPR2019-00824, IPR2019-00826.

Decided: March 9, 2022

JOSEPH R. PALMORE, Morrison & Foerster LLP, Washington, DC, argued for appellant. Also represented by SETH W. LLOYD, BRIAN ROBERT MATSUI; LENA HUGHES; New York, NY; RICHARD HUNG, San Francisco, CA; BITA RAHEBI, Los Angeles, CA.

BRIAN ERIK HAAN, Lee Sheikh Megley & Haan LLC, Chicago, IL, argued for appellee. Also represented by ASHLEY E. LAVALLEY, CHRISTOPHER LEE, RICHARD BURNS MEGLEY, JR.; JAMES CARMICHAEL, STEPHEN TERRY SCHREINER, Carmichael IP, PLLC, Tysons Corner, VA.

Before MOORE, *Chief Judge*, PROST and TARANTO, *Circuit Judges*.

MOORE, *Chief Judge*.

Apple appeals from three Patent Trial and Appeal Board *inter partes* review final written decisions collectively holding Apple failed to show claims 2, 4, 9, and 11 of U.S. Patent No. 9,712,494; claims 7–9 of U.S. Patent No. 9,712,502; and claims 3, 5, 10, and 12–16 of U.S. Patent No. 9,838,362 would have been obvious. For the following reasons, we affirm.

BACKGROUND

I

The challenged patents share a written description and purport to improve secure messaging between arbitrary hosts (e.g., messaging across local area networks (LANs), private and public wide area networks (WANs), or the internet) utilizing Internet Protocol (IP) security protocols. '494 patent at 1:54–57; 7:38–45.[1] IP security protocols require establishing a security association, *id.* at 2:39–49, that costs computation time and increases network latency, *id.* at 4:44–45. They are purportedly designed for static connections and, thus, not well suited for communications with mobile computers, leading to poor quality of service for communication over wireless links. *Id.* at 4:39–43; 5:7–14. To solve these problems, systems commonly utilize an intermediate host that facilitates communication between a mobile terminal and its communication target (e.g., a security gateway). *Id.* at 5:15–6:14. These common solutions, however, heavily rely on a concept known as tunneling. In tunneling, typically an entire data packet, including its outer header, is encapsulated and a new outer

[1] For simplicity, we cite to the '494 patent.

header is added. *Id.* at 3:21–49. The use of tunneling in the known solutions can cause extra packet size overhead, or require the intermediate computer to decrypt the packet, which could cause potential security problems. *Id.* at 6:21–24.

The patents disclose a method for secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network that purportedly avoids these disadvantages. *Id.* at Abstract; 6:28–31. Preferably, a first computer "processes [a] formed message using a security protocol and encapsulates the message at least in an outer IP header," which is sent to an intermediate computer. *Id.* at 6:54–59. The intermediate computer "matches the outer IP header address fields together with a unique identifier used by the security protocol, and performs a translation of the outer addresses and the unique identity used by the security profile." *Id.* at 6:59–63. The translated packet is then sent to a second computer, which processes it using a standard security protocol. This method does not use any "extra encapsulation overhead" typical of prior-art solutions. *Id.* at 6:65–67.

The claims of the '494 and '362 patents cover the intermediate computer. Claim 1 of the '494 patent is a representative independent claim for those patents:

> 1. An intermediate computer for secure forwarding of messages in a telecommunication network, comprising:
>
> an intermediate computer configured to connect to a telecommunication network;
>
> the intermediate computer configured to be assigned with a first network address in the telecommunication network;
>
> *the intermediate computer configured to receive from a mobile computer a secure message sent to the first network address*

> having an encrypted data payload of a message and a unique identity, the data payload encrypted with a cryptographic key derived from a key exchange protocol;
>
> the intermediate computer configured to read the unique identity from the secure message sent to the first network address; and
>
> the intermediate computer configured to access a translation table, to find a destination address from the translation table using the unique identity, and
>
> to securely forward the encrypted data payload to the destination address using a network address of the intermediate computer as a source address of a forwarded message containing the encrypted data payload wherein the intermediate computer does not have the cryptographic key to decrypt the encrypted data payload.

(emphasis added).

The '502 patent claims the mobile computer that sends the secure message to the intermediate computer. Claim 1 is a representative independent claim:

> 1. A computer for sending secure messages, and for enabling secure forwarding of messages in a telecommunication network by an intermediate computer to a recipient computer, comprising:
>
> a computer configured to connect to a telecommunication network;
>
> the computer configured to be assigned with a network address in the telecommunication network, wherein the computer is

> a mobile computer in that the address of the mobile computer changes;
>
> the computer configured to form a secure message by encrypting the data payload of a message and giving the message a unique identity and a destination address of an intermediate computer, wherein the unique identity and the destination address are capable of being used by the intermediate computer to find an address to a recipient computer;
>
> the computer configured to send the secure message to the intermediate computer for forwarding of the encrypted data payload to the recipient computer; and
>
> the computer configured to set up a secure connection using a key exchange protocol.

II

MPH asserted claims of the challenged patents against Apple in the Northern District of California. Apple petitioned for *inter partes* review of each claim of the three patents, relying primarily on a combination of Request for Comments 3104 (RFC3104)[2] and U.S. Patent No. 7,032,242 (Grabelsky) (collectively, the combination). The Board held that Apple failed to show that several dependent claims of each patent would have been obvious in view of the combination. Apple challenges each of these determinations. We have jurisdiction under 28 U.S.C. § 1295(a)(4)(A).

---

[2] G. Montenegro & M. Borella, *RSIP Support for End-to-end IPsec*, Request for Comments 3104, The Internet Society (Oct. 2001).

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.