

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

MPH TECHNOLOGIES OY,
Patent Owner.

IPR2019-00824
Patent 9,712,502 B2

Before SALLY C. MEDLEY, KAMRAN JIVANI, and
JOHN D. HAMANN, *Administrative Patent Judges*.

HAMANN, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

In this *inter partes* review, instituted pursuant to 35 U.S.C. § 314, Apple Inc. (“Petitioner”) challenges the patentability of claims 1–10 (“the challenged claims”) of U.S. Patent No. 9,712,502 B2 (Ex. 2002, “the ’502 patent”), owned by MPH Technologies Oy (“Patent Owner”). We have jurisdiction under 35 U.S.C § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons discussed herein, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–6 and 10 are unpatentable, but Petitioner has not shown by a preponderance of the evidence that claims 7–9 are unpatentable.

II. BACKGROUND

A. Procedural History

Petitioner filed a Petition requesting *inter partes* review of the challenged claims of the ’502 patent. Paper 2 (“Pet.”). The Petition is supported by the Declaration of David Goldschlag, Ph.D. (Ex. 1002). Patent Owner filed a Preliminary Response. Paper 6 (“Prelim. Resp.”).

We instituted *inter partes* review of all of the challenged claims of the ’502 patent on all of the grounds raised in the Petition. Paper 7 (“Dec. on Inst.”), 6–7, 34. Patent Owner filed a Response to the Petition. Paper 13 (“PO Resp.”). The Response is supported by the Declaration of Professor George N. Rouskas, Ph.D. (Ex. 2003) and the Declaration of Michael S. Borella (Ex. 2010). Petitioner filed a Reply to Patent Owner’s Response. Paper 16 (“Pet. Reply”). The Reply is supported by an additional Declaration of David Goldschlag, Ph.D. (Ex. 1022). Patent Owner filed a Sur-Reply to Petitioner’s Reply. Paper 23 (“PO Sur-Reply”).

An oral hearing was held on August 11, 2020. A transcript of the oral hearing is included in the record. Paper 24 (“Tr.”).

B. Related Matter

The parties identify *MPH Techs. Oy v. Apple Inc.*, Case No. 4:18-cv-05935-PJH (N.D. Cal.), as a matter that may affect or would be affected by a decision in this proceeding. Pet. 2; Paper 4, 1. The parties also identify as related matters the following *inter partes* reviews: IPR2019-00822, IPR2019-00823, IPR2019-00825, and IPR2019-00826, which involve the parties and patents related to the ’502 patent. Pet. 2; Paper 4, 1.

C. The Challenged Patent (Ex. 2002)

The ’502 patent relates to the “secure forwarding of a message from a first computer to a second computer via an intermediate computer in a telecommunication network.” Ex. 2002, 6:38–41. According to the ’502 patent, “[a]n essential idea of [its] invention is to use the standard [Internet Protocol (‘IP’) Security (‘IPSec’)] protocol . . . between the intermediate computer and the second computer and an ‘enhanced IPSec protocol’ between the first computer and the intermediate computer.” *Id.* at 7:38–41, 1:54. More specifically, the ’502 patent states that “[t]he advantage of [its] invention is that [a] logical IPSec connection shared by the first and the second computer can be enhanced by the first and the intermediate computer without involvement of the second computer.” *Id.* at 10:38–41. The ’502 patent adds: “[i]n particular[,] the so-called ‘ingress filtering’ performed by some routers [(e.g., the second computer)] does not pose any problems when translations of addresses are used.” *Id.* at 10:41–44.

Figure 1, shown below, “illustrates an example of a telecommunication network of the invention” of the ’502 patent. *Id.* at 9:55–56.

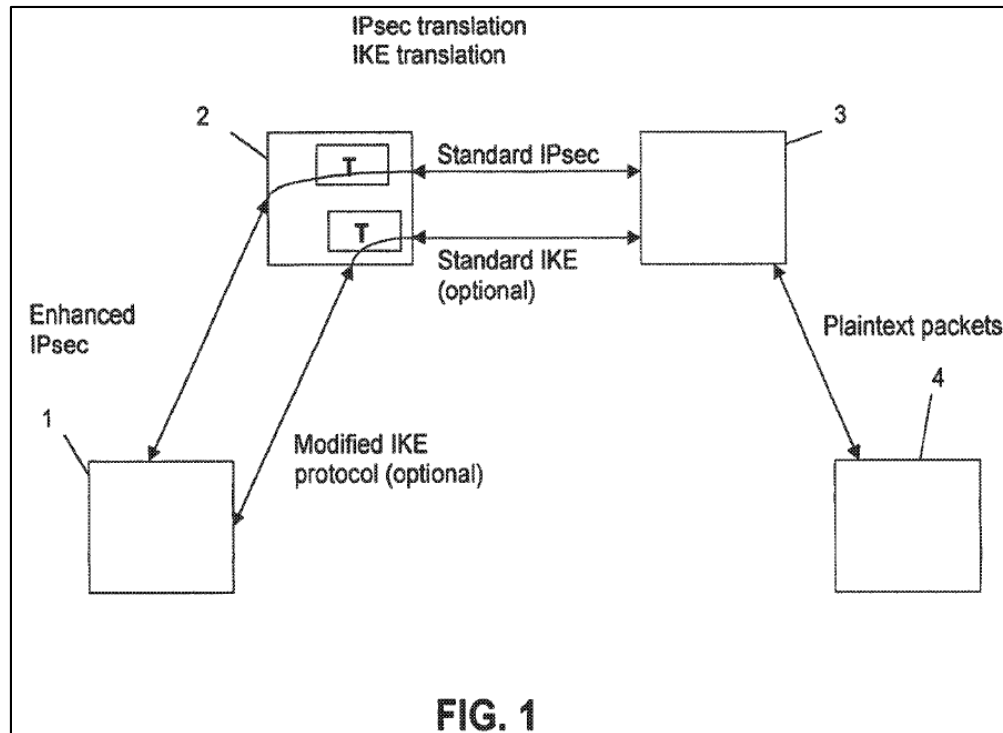


Figure 1 shows an example of a telecommunication network in accordance with the invention of the ’502 patent. *Id.* at 10:4–5. As illustrated, the network comprises: (i) a first computer (client computer 1) that is served by (ii) an intermediate computer (server 2), and (iii) host computer 4 that is served by (iv) a second computer (security gateway 3). *Id.* at 10:4–9. Security gateway 3 “supports the standard IPsec protocol,” while client computer 1 and server 2 support an enhanced IPsec protocol. *Id.* at 10:9–12. The ’502 patent discloses that the first computer (i.e., client computer 1) in Figure 1 is a mobile terminal. *Id.* at 11:5–7, 11:13–14.

“In the example of F[igure] 1, an IPsec connection is formed between . . . client computer 1 (the first computer) and . . . security gateway 3 (the second computer).” *Id.* at 10:46–48. The ’502 patent discloses that

“[m]essages to be sent to . . . host terminal 4 from . . . client computer 1 are first sent to . . . server 2, wherein an IPSec translation[, *inter alia*,] . . . takes place.” *Id.* at 10:60–62. Put differently, “[w]hen the intermediate computer receives the packet sent . . ., it performs an address and [Security Parameters Index (‘SPI’)] translation, ensuring that the security gateway (host 3 of F[igure] 1) can accept the packet.” *Id.* at 12:1–4, 2:40–41. The ’502 patent states that “translation[s can be] . . . performed[, for example,] by means of a translation table stored at the intermediate computer[, with t]he outer IP header address fields and/or the SPI-values [being] changed by the intermediate computer so that the message can be forwarded to the second computer.” *Id.* at 7:46–50.

According to the ’502 patent, “[m]ost of the packet is secured using IPSec, . . . [but] the intermediate computer . . . is able to use the outer IP addresses and the incoming SPI value to determine how to modify the outer address and the SPI to suite the second computer, which is the next destination.” *Id.* at 12:1–11. “[T]he confidentiality of the packets is not compromised, . . . [because t]he intermediate computer does not know the cryptographic keys used to encrypt and/or authenticate the packets, and can thus not reveal their contents,” according to the ’502 patent. *Id.* at 10:32–37. After translation, “the message can be sent to . . . security gateway 3, which sends the message further in plain text to . . . host terminal 4.” *Id.* at 10:62–64.

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.