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

Paper 8
Entered: September 11, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2015-00812
Patent 8,850,009 B2

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

BISK, *Administrative Patent Judge*.

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

INTRODUCTION

A. Background

Petitioner, Apple Inc., filed a Petition (Paper 1, "Pet.") requesting an *inter partes* review of claims 1–8, 10–20, and 22–25 (the "challenged claims") of U.S. Patent No. 8,850,009 B2 (Ex. 1003, "the '009 patent"). Patent Owner, VirnetX Inc.,[1] filed a Preliminary Response. Paper 6 ("Prelim. Resp.").

We have authority to determine whether to institute an *inter partes* review. 35 U.S.C. § 314(b); 37 C.F.R. § 42.4(a). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted "unless the Director determines . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition."

After considering the Petition and Preliminary Response, we determine that Petitioner has established a reasonable likelihood of prevailing in showing the unpatentability of at least one of the challenged claims. Accordingly, we institute *inter partes* review.

B. Related Matters

The parties indicate that the '009 patent "and/or" related patents are involved in several proceedings in the United States District Court for the

[1] The Petition also names Science Application International Corporation as Patent Owner. However, the Patent Owner Preliminary Response names only VirnetX.

Eastern District of Texas.[2] Pet. 6–7; Paper 5, 12–13. Petitioner also filed another petition seeking *inter partes* review of the '009 patent—IPR2015-00813. 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.[3]

C. The Asserted Grounds of Unpatentability

Petitioner contends that claims 1–8, 10–20, and 22–25 of the '009 patent are unpatentable under 35 U.S.C. § 103 based on the combination of Beser[4] and RFC 2401.[5] Petitioner also provides testimony from Dr. Roberto Tamassia. Ex. 1005.

D. The '009 Patent

The '009 patent describes secure methods for communicating over the Internet. Ex. 1003, 10:16–17. Specifically, the '009 patent describes "the automatic creation of a virtual private network (VPN) in response to a

[2] In the future, Petitioner is advised that referring to "numerous lawsuits," without specifically identifying the court in which the lawsuit is taking place and other information necessary to identify the proceeding may be considered a violation of 37 C.F.R. § 42.8. *See* Pet. 6–7. Similarly, Patent Owner is advised to be specific in addressing whether the challenged patent is actually the subject of the enumerated related litigation. *See* Paper 5, 12–13.

[3] In this section, the Petition did not identify specifically any other proceeding before the Office other than IPR2015-00813. Pet. 2. In the future, such omission may be construed as a violation of 37 C.F.R. § 42.8.

[4] U.S. Patent No. 6,496,867 B1 (Ex. 1007) ("Beser").

[5] S. Kent and R. Atkinson, *Security Architecture for the Internet Protocol*, Request for Comments: 2401, BBN Corp., November 1998 (Ex. 1008) ("RFC 2401").

domain-name server look-up function." *Id.* at 39:36–38. This automatic creation makes use of a modified Domain Name Server as opposed to a conventional Domain Name Server (DNS), which is described as follows:

> 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 39:39–45.

The modified DNS server may include both a conventional DNS and a DNS proxy. *Id.* at 40:33–35. 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, whether the user has sufficient security privileges to access the requested site. *Id.* at 40:39–45. 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 40:62–65. 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 40:45–51. 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 40:51–57.

The VPN is "preferably implemented using the IP address 'hopping' features," (changing IP addresses based upon an agreed

upon algorithm) described elsewhere in the ’009 patent, “such that the true identity of the two nodes cannot be determined even if packets during the communication are intercepted.” *Id.* at 40:18–22.

E. Illustrative Claim

Claims 1 and 14 of the ’009 patent are independent. Claim 1 is illustrative of the claimed subject matter and recites:

1. A network device, comprising:

a storage device storing an application program for a secure communications service; and

at least one processor configured to execute the application program for the secure communications service so as to enable the network device to:

send a domain name service (DNS) request to look up a network address of a second network device based on an identifier associated with the second network device;

receive, following interception of the DNS request and a determination that the second network device is available for the secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link;

connect to the second network device over the encrypted communication link, using the received network address of the second network device and the provisioning information for the encrypted communication link; and

communicate data with the second network device using the secure communications service via the encrypted communication link,

the network device being a device at which a user uses the secure communications service to access the encrypted communication link.

Ex. 1003, 56:22–48.

ANALYSIS

A. Claim Construction

We interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); *see In re Cuozzo Speed Techs., LLC.*, No. 2014-1301, 2015 WL 4097949, at *5–*8 (Fed. Cir. July 8, 2015), *reh'g en banc denied*, 2015 WL 4100060 (Fed. Cir. July 8, 2015). We presume a claim term carries its "ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question" at the time of the invention. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007) (citation and quotations omitted).

Petitioner and Patent Owner each proffer proposed constructions of several claim terms. At this stage of the proceeding, neither party has identified a term for construction that is dispositive on any of the challenges. For the purposes of this Decision, and on this record, we determine that no claim term needs express interpretation. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (only those terms which are in controversy need to be construed, and only to the extent necessary to resolve the controversy).

B. Prior Art Printed Publication Status of RFC 2401

Patent Owner asserts that Petitioner "does not provide evidence to establish that RFC 2401 would have been sufficiently accessible to the public interested in the art" on November 1998, the date recited on each of its pages. Prelim. Resp. 3. According to Patent Owner, Petitioner fails to show that RFC 2401 constitutes a prior art printed publication and is

therefore not properly relied upon for purposes of showing obviousness. *Id.* at 3–6. On this basis, Patent Owner argues that Petitioner has not satisfied its burden of showing a reasonable likelihood of prevailing with respect to any challenged claim of the '009 patent.

The determination of whether a given reference qualifies as a prior art "printed publication" involves a case-by-case inquiry into the facts and circumstances surrounding the reference's disclosure to members of the public. *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). We acknowledge Patent Owner's argument regarding RFC 2401. On its face, however, RFC 2401 is a dated "Request for Comments" from the "Network Working Group," discussing a particular standardized security protocol for the Internet. Ex. 1008. Moreover, RFC 2401 describes itself as a "document [that] specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. . . . Distribution of this memo is unlimited." *Id.* at 1; *see also* Ex. 1005 ¶¶ 148–155 (discussing Request for Comment ("RFC") publications). These indicia suggest that there is a reasonable likelihood the document was made available to the public (over the Internet), in order to obtain feedback prior to implementation of the standard it describes.

On this record,[6] we are persuaded that Petitioner has made a threshold showing that RFC 2401 constitutes a prior art printed publication.

[6] To the extent that Patent Owner objects to the admissibility of this evidence, it will have the opportunity, after trial is instituted, to enter any objections to evidence. 37 C.F.R. § 42.64(b)(1). To the extent that Patent Owner continues to assert that Petitioner has not met its burden of showing that RFC 2401 is a "printed publication," it will have the opportunity to make this argument in its Patent Owner Response.

Accordingly, we consider the disclosure of RFC 2401 for the purposes of this decision.

C. Obviousness Over Beser and RFC 2401

1. Overview of Beser

Beser describes a system that establishes an IP (internet protocol) tunneling association on a public network between two end devices. *See* Ex. 1007, Abs. Figure 1 of Beser is reproduced below.

FIG. 1

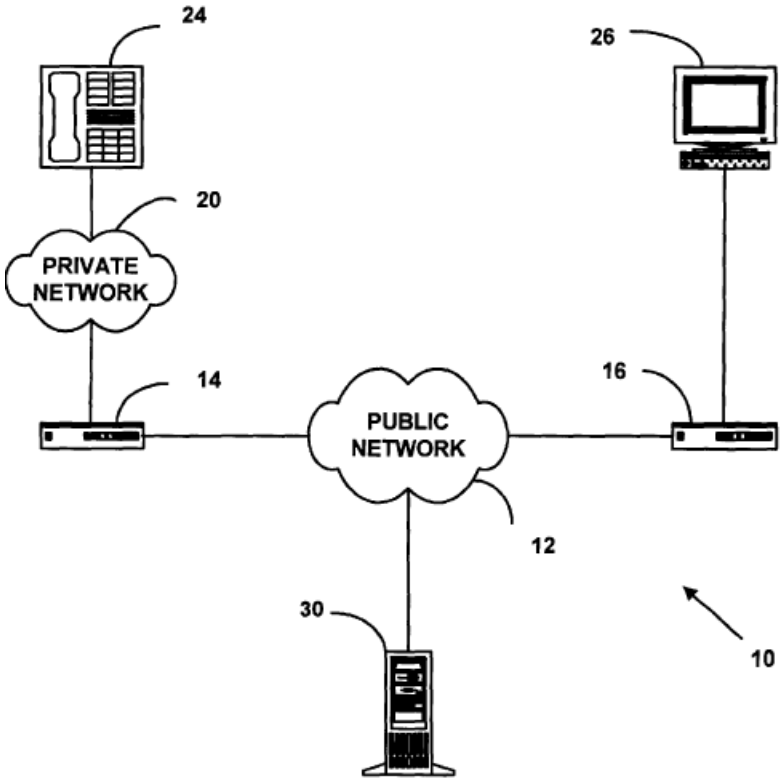

Figure 1 of Beser illustrates a network system, including public network 12, network devices 24 and 26, private network 20, trusted third-party network

device 30, and modified routers or gateways 14 and 16. Ex. 1007, 3:60–4:19. Beser describes network devices 24 and 26 as telephony devices, multimedia devices, VoIP devices, or personal computers. *Id.* at 4:43–52.

Beser's system "increases the security of communication on the data network" by providing and hiding, in packets, "private addresses" for originating device 24 and terminating device 26 on the network. *See id.* at Abs., Fig. 1, Fig. 6. To begin a secure transaction, requesting device 24 sends a request to initiate a tunneling connection to network device 14. *Id.* at 8:21–47. This request includes a unique identifier for the terminating end of the tunneling association—terminating device 26. *Id.*at 7:64–8:3. The packets used to transfer this unique identifier across the public network "may require encryption or authentication to ensure that the unique identifier cannot be read on the public network." *Id.* at 11:22–25. Beser discloses, as background prior art, known forms of encryption for the information inside these packets, including IP Security ("'IPsec'"). *Id.* at 1:54–56. Once network device 14 receives the request, it passes the request on to trusted-third-party network device 30. *Id.* at 8:3–4, 8:48–9:5.

Trusted-third-party network device 30 contains a directory of users, such as a DNS, which retains a list of public IP addresses associated at least with second network device 16 and terminating devices 26. *See id.* at 11:32–58. DNS 30 associates terminating network device 26, based on its unique identifier in the request, with a public IP address for router device 16. *See id.* at 11:26–36. Trusted-third-party network device 30 then assigns, by negotiation, private IP addresses to requesting network device 24 and terminating device 26. *Id.* at 9:29–35, 12:17–19. The negotiated private IP

addresses are "isolated from a public network such as the Internet," and "are not globally routable." *Id.* at 11:62–65.

2. Overview of RFC 2401

RFC 2401 describes the security services offered by the IPsec protocols, including "access control, connectionless integrity, data origin authentication, [and] . . . confidentiality (encryption)." Ex. 1008, 3–4.

3. Claims 1 and 14

For this proceeding, Petitioner asserts that the "non-encrypted streaming audio/video example" described in Beser teaches each of the limitations of claims 1 and 14 except the required "encrypted communications link." Pet. 28–29, 34–50. Specifically, Petitioner argues that Beser's originating end device is equivalent to the claimed first network device and Beser's terminating end device is equivalent to the claimed second network device. Pet. 34–35. Petitioner also argues that Beser discloses the trusted-third-party network device, intercepting a DNS request and determining that the terminating end device is available. Pet. 35–44. According to Petitioner, it would have been obvious to a person of ordinary skill in the art to provide "'end-to-end'" encryption of the traffic being sent in Beser using the teachings of RFC 2401. *Id.* at 29–30.

a. Rationale to Combine

Petitioner argues that "a person of ordinary skill would have considered the teachings of Beser in conjunction with those in RFC 2401 because Beser expressly refers to the IPsec protocol (which is defined in RFC 2401) as being the conventional way that the IP tunnels described in Beser are established. Pet. 30 (citing Ex. 1007, 1:54–56; Ex. 1005 ¶¶ 383–

85, 395). Petitioner adds that Beser also indicates that "its IP tunneling schemes are compliant with standards-based processes and techniques (e.g., IPsec), and can be implemented using pre-existing equipment and systems" and that "IP tunnels are and should ordinarily be encrypted." *Id.* at 30–31 (citing Ex. 1007, 1:54–56, 4:55–5:2, 11:22–25, 18:2–5; Ex. 1005 ¶¶ 282–83, 185, 383–86, 389–90, 394, 398). Moreover, Petitioner adds that a person of ordinary skill would have recognized that IPsec readily could be integrated into Beser's systems. *Id.* at 31–32 (citing Ex. 1005 ¶¶ 391, 392, 398–400).

Patent Owner argues that Beser and RFC 2401 would not have been combined as asserted by Petitioner. Prelim. Resp. 12–17. According to Patent Owner, Beser teaches away from using the IPsec protocol of RFC 2401 for audio or data by explaining that streaming data flows, such as multimedia, require a great deal of computing power to encrypt or decrypt and the "strain of such computations 'may result in jitter, delay, or the loss of some packets.'" *Id.* at 13 (quoting Ex. 1007, 1:64–65). Thus, Patent Owner concludes that "one of ordinary skill in the art would understand that Beser is directed to providing a method for securing communications *other than* encryption." *Id.* at 14 (citing Ex. 2009 ¶ 56). Patent Owner adds that Beser "also teaches that encryption does not deter a determined hacker from deducing source and identity information, and so, once the tunnel is established, Beser eschews encryption in favor of hiding the identities within the tunnel" and, thus, adding encryption would "contravene Beser's express objective of increasing security without increasing computational burden." *Id.* at 15.

We are not persuaded, at this point in the proceeding, that Beser teaches away from adding encryption to its system. Although Beser

recognizes that the use of encryption may cause challenges, it also suggests that such problems may be overcome by providing more computer power. Ex. 1007, 1:60–63. In addition, Beser characterizes some prior art systems as creating "security problems by preventing certain types of encryption from being used." Ex. 1007, 2:23–24. We are, therefore, persuaded that Petitioner's rationale that a person of ordinary skill would have found it obvious to combine the teachings of RFC 2401 with Beser is reasonable.

b. The Receiving Limitation

Patent Owner also argues that Petitioner improperly relies on two elements in Beser for three separate claimed features. Prelim. Resp. 17–20. Specifically, claims 1 and 14 recite a first network device

> receiv[e/ing], following interception of the DNS request and a determination that the second network device is available for a secure communications service: (1) an indication that the second network device is available for the secure communications service, (2) the requested network address of the second network device, and (3) provisioning information for an encrypted communication link.

("the receiving limitation"). According to Patent Owner, Petitioner improperly contends that the three enumerated features of the receiving limitation are satisfied by Beser's receipt, at the originating end device, of its own private IP address and the private IP address of the terminating end device. *Id.* at 18. Patent Owner appears to base this argument on some language in the Petition stating that the originating end device's private IP address could be used to satisfy both the "'indication'" feature and the "provisioning information" feature of the receiving limitation. *Id.* (quoting Pet. 46 (discussing not the receiving limitation, but the "connecting" limitation). Patent Owner adds that "Petitioner has not argued that one of

skill would have found it obvious to either replace the three separate claim features with two features that perform multiple functions or add an additional element to Beser to be received by the originating device." *Id.* at 19.

We do not agree with Patent Owner that Petitioner's arguments are so limited. In fact, Petitioner argues that, with respect to provisioning information, in the example being asserted, "Beser would not provide provisioning information for an encrypted communication link," but that providing such information "would have been an obvious variation of Beser in view of RFC 2401." Pet. 42–43. Moreover, Petitioner argues that "RFC 2401 also describes providing 'provisioning information'" in the form of key distribution and states that "[i]t would have been obvious to configure the trusted-third-party network device to play this role" and "provide an encryption key to be used to encrypt the communications between the end devices according to IPsec." *Id.* at 44. Patent Owner does not address these arguments in its Preliminary Response.

c. Conclusion

On this record, in view of Petitioner's reliance on the testimony of Dr. Tamassia, which we credit, we are persuaded Petitioner has established a reasonable likelihood of prevailing in its challenge that claims 1 and 14 would have been obvious over Beser combined with RFC 2401.

4. Claims 2–8, 10–13, 15–20, and 22–25

Petitioner asserts that the combination of Beser and RFC 2401 teaches each of the limitations of claims 2–8, 10–13, and 22–25. Pet. 50–59 (citing Ex. 1005). In its Preliminary Response, Patent Owner does not make specific arguments directed to these claims. On this record, we are

persuaded Petitioner has established a reasonable likelihood of prevailing in its challenge that claims 2–8, 10–13, and 22–25 would have been obvious over Beser combined with RFC 2401.

CONCLUSION

For the foregoing reasons, we determine that the information presented in the Petition establishes that there is a reasonable likelihood that Petitioner would prevail with respect to the challenged claims of the '009 patent.

Any discussion of facts in this decision are made only for the purposes of institution and are not dispositive of any issue related to any ground on which we institute review. The Board has not made a final determination on the patentability of any challenged claims. The Board's final determination will be based on the record as fully developed during trial.

ORDER

Accordingly, it is

ORDERED that pursuant to 35 U.S.C. § 314, we institute an *inter partes* review of claims 1–8, 10–20, and 22–25 of the '009 patent as obvious over Beser and RFC 2401.

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial;

FURTHER ORDERED that the trial is limited to the grounds identified above.

PETITIONER:
Jeffrey P. Kushan
Scott Border
Thomas A. Broughan, III
SIDLEY AUSTIN LLP
jkushan@sidley.com
sborder@sidley.com
tbroughan@sidley.com
iprnotices@sidley.com

PATENT OWNER:
Joseph E. Palys
Naveen Modi
PAUL HASTINGS LLP
josephpalys@paulhastings.com
naveenmodi@paulhastings.com

Jason Stach
FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.
jason.stach@finnegan.com