

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

VIRNETX INC.,
Patent Owner.

Case IPR2014-00238
Patent 8,504,697 B2

Before MICHAEL P. TIERNEY, KARL D. EASTHOM, and
STEPHEN C. SIU, *Administrative Patent Judges*.

SIU, *Administrative Patent Judge*.

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

I. BACKGROUND

Apple Inc. (“Petitioner”) filed a Petition (Paper 1) (“Pet.”) seeking an *inter partes* review of claims 1–11, 14–25, and 28–30 of U.S. Patent No. 8,504,697 B2 (Ex. 1001, “the ’697 patent”) pursuant to 35 U.S.C. §§ 311–319. On May 14, 2014, the Board instituted an *inter partes* review of claims 1–11, 14–25, and 28–30 (Paper 15) (“Dec. on Inst.”).

Subsequent to institution, VirnetX (“Patent Owner”) filed a Patent Owner Response (Paper 30) (“PO Resp.”), and Petitioner filed a Reply (Paper 33) (“Pet. Reply”). An Oral Hearing was conducted on February 9, 2015.

The Board has jurisdiction under 35 U.S.C. § 6(c). This final written decision is issued 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 1–11, 14–25, and 28–30 of the ’697 patent are unpatentable.

A. The ’697 Patent (Ex. 1001)

The ’697 patent describes methods for communicating over the internet. Ex. 1001, 10:7–8.

B. Illustrative Claim

Claim 1 of the ’697 patent is reproduced below:

1. A method of connecting a first network device and a second network device, the method comprising:
 - intercepting, from the first network device, a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device;
 - determining, in response to the request, whether the second network device is available for a secure communications service; and
 - initiating a secure communication link between the first network device and the second network device based on a determination that the second network device is available for the secure communications service;

wherein the secure communications service uses the secure communication link to communicate at least one of video data and audio data between the first network device and the second network device.

C. Cited Prior Art

Wesinger US 5,898,830 Apr. 27, 1999 (Ex. 1008)

H. Schulzrinne, et al., *SIP: Session Initiation Protocol*, Network Working Group, Request for Comments: 2543, Bell Labs, March, 1999 (“RFC 2543” Ex. 1012).

D. Instituted Grounds of Unpatentability

References	Basis	Claims Challenged
Wesinger	§102	1–3, 8–11, 14–17, 22–25, and 28–30
Wesinger and RFC 2543	§103	4–7 and 18–21

E. Claim Interpretation

Secure communication link

Patent Owner argues that the term “secure communication link” must include encryption. *See, e.g.*, PO Resp. 11, 13–19. Patent Owner, however, does not demonstrate sufficiently that the construction of this term impacts any issue in this proceeding. Therefore, we decline to construe this term.

Virtual Private Network

In the Decision, we construed the term “Virtual Private Network” to include a secure communication link that includes a portion of a public network. Dec. on Inst. 9–10. Patent Owner argues that “the Board need not construe this term . . . and [the construction of this term] does not appear to impact any of the issues in this case.” PO Resp. 21. In view of Patent

Owner's observation that the construction of this term does not impact any of the issues in this case, we decline to construe this term.

Intercepting a request

In the Decision, we construed the term "intercepting" a request as receiving a request pertaining to a first entity at another entity. Dec. on Inst. 12. Patent Owner states that "it does not appear that the construction of 'intercepting' will bear on the outcome of the issues in this *inter partes* review." PO Resp. 23. In view of Patent Owner's observation that the construction of the term "intercepting" has no bearing on the issues in this proceeding, we decline to construe this term.

Determining in response to the request

Patent Owner disputes the construction of this term in related IPR2014-00237. Patent Owner does not specify how the construction of the term "determining" is relevant in the present proceeding. Because the relevance of the construction of this term with any particular issue in this proceeding has not been established, we decline to construe the term "determining" in this proceeding.

Neither party has expressed disagreement with the constructions of other claim terms of the '697 patent, and we see no reason to modify these constructions based on the evidence introduced during trial. We maintain these constructions for this Final Written Decision.

II. ANALYSIS

A. *Wesinger*

For at least the foregoing reasons, we find that Petitioner has demonstrated that claims 1–3, 8–11, 14–17, 22–25, and 28–30 are anticipated by *Wesinger* under 35 U.S.C. § 102.

Claim 1, for example, recites “determining, in response to the request, whether the second network device is available for a secure communication service.” Claim 16 recites a similar feature. Patent Owner argues that *Wesinger* fails to disclose this feature. PO Resp. 37.

In particular, Patent Owner argues that *Wesinger* discloses “two distinct requests: a ‘DNS [query]’ and ‘an ensuing connection request.’” PO Resp. 40. Patent Owner further alleges that *Wesinger* discloses the “DNS query” is “for the network address of the destination D” but that “*Wesinger’s* firewall decides whether to allow or deny a requested connection upon receiving a connection request” and “does not perform its firewall allow/disallow processing . . . in response to [the] DNS request [or query].” PO Resp. 38, 39. We are not persuaded by Patent Owner’s argument.

Even if Patent Owner’s contention that *Wesinger* discloses a “connection request” is correct, Patent Owner does not demonstrate sufficiently that *Wesinger* fails to disclose that the “connection request” is, in fact, not associated with the “look up [of] an internet protocol (IP) address of the second network device based on a domain name associated with the second network device.” For example, *Wesinger* explicitly discloses that, responsive to the “connection request,” an IP address (e.g., “virtual host X.X.X.X., where X.X.X.X. represents an IP address,” Ex. 1008, 10:60–61)

of a network device is provided based on a domain name (e.g., “homer.odyssey.com,” Ex. 1008, 10:59, 10:64–65) that is included in the “connection request.” Hence, Wesinger discloses a request (e.g., “connection request”) to look up an internet protocol (IP) address of a device based on a domain name associated with the device, as recited in claim 1.

Wesinger also discloses “two mappings are required in order to handle a connection request” in which “a first mapping maps from the host name received in the connection request to the IP address of a virtual host.” Ex. 1008, 10: 51–54. In other words, Wesinger discloses a “connection request” that contains a “host name” that is mapped to a corresponding “IP address of a virtual host.” Patent Owner does not explain sufficiently a difference between the “connection request” of Wesinger that contains a host name and is used to look up a corresponding IP address and the disputed claim feature of a request to look up an IP address of a device based on a domain name.

Wesinger also discloses, for example, that the “connection request” is received (Ex. 1008, 16:22) and, in response, “[f]irst the address and name . . . are obtained of the virtual host for which a connection is requested . . . [and] identified . . . by IP address” (Ex. 1008, 16:29–31), that “[o]nce the process has determined which host it is . . . the process changes to a user profile . . .” (Ex. 1008, 16:43–44) and “[i]f the remote host satisfied the required level of access scrutiny . . . then the connection is allowed.” Ex. 1008, 16:57–58, 66–67. Hence, Wesinger discloses receiving a “connection request” (or “request”) to look up an IP address of a device based on a domain name (e.g., identified by an IP address), as recited in claim 1.

Patent Owner argues that “the DNS query [of Wesinger] does not invoke the firewall allow/disallow decision” and “does not perform its firewall allow/disallow processing . . . in response to a DNS request.” PO Resp. 38, 39. To the extent that the so-called “DNS query” to which Patent Owner refers is the “request to look up an internet protocol (IP) address of” a device based on a domain name, as recited in claim 1, for example, we are not persuaded by Patent Owner’s contention that Wesinger fails to disclose this feature for at least the previously discussed reasons pertaining to Wesinger’s disclosure of the “connection request.”

Wesinger discloses that “[i]f all the rules are satisfied, then the connection [with the virtual host] is allowed” and that “[o]nce the connection has been allowed, the virtual host process . . . performs . . . connection processing.” Ex. 1008, 16:66 – 17:3. Patent Owner argues that Wesinger discloses determining “whether the incoming connection request . . . is allowed,” but fails to disclose “determin[ing] whether the . . . ‘second device’ is available for a secure communications service,” as recited in claim 1. PO Resp. 46–47.

Patent Owner does not explain sufficiently a difference between the determination of whether a requested connection with a device is “allowed” or not and the determination of whether a device is “available” for a connection. One of ordinary skill in the art would have understood that if a connection with a virtual host is determined to be allowed if all rules are satisfied (as Wesinger discloses), then the virtual host would be determined to be “available” for the connection, the connection being formed with the virtual host based on the determination. Under an ordinary and customary construction of the term “available” as would have been understood by one

of ordinary skill in the art in light of the Specification as being accessible for use, at hand, or usable,¹ we do not discern a substantial difference between determining whether a device is allowed to connect (and connecting only if the device is allowed) and determining whether a device is available (or accessible for use, at hand, or usable) for a connection (and connecting only if the device is accessible for use, at hand, or usable). In both cases, a determination is made as to whether a connection will be made with a device and the connection is created based on this determination.

Patent Owner does not argue that the Specification provides a specialized definition of the term “available.” Nor do we identify a specialized definition of the term in the Specification. However, we note that the Specification discloses that “DNS proxy . . . determines whether the user has sufficient security privileges to access the site. If so, DNS proxy . . . request[s] that a virtual private network be created between user computer . . . and secure target site.” Ex. 1001, 40:31–42. In another embodiment in the Specification, a check is made “to determine whether the user is authorized to connect to the secure host” by “reference to an internally stored list” and “[i]f the user has sufficient security privileges, then . . . a secure VPN is established between the user’s computer and the secure target site.” Ex. 1001, 41:14–27. In yet another embodiment in the Specification, a “[c]lient has permission to access target computer” and “the client’s DNS request would be . . . forward[ed] . . . to gatekeeper 2603 [which] would establish a VPN between the client and the requested target.” Ex. 1001, 41:47–51. In another embodiment, the “[c]lient does not have permission to

¹ THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 90 (1975) (Ex. 3001).

access target computer” and the “gatekeeper would reject the request.”

Ex. 1001, 41:57–61.

In each of the identified embodiments in the Specification, availability of the second network device (i.e., a secure target site) for a secure communication service is determined based on whether the user (of the first network device) has “sufficient security privileges” or “permission to access” the target computer. We do not identify, and Patent Owner does not point out, an embodiment in the Specification in which the availability of the second network device is determined by other methods or criteria. To the extent that determining whether the second network device is available for a secure communications service, as recited in claim 1, is determining that the user of the first network device has sufficient security privileges or permission to access the second network device (i.e., the criteria disclosed in the Specification), Wesinger discloses this feature. For example, Wesinger discloses that if “the remote host” (i.e., first network device) “satisfies the required level of access scrutiny,” is on an “Allow database,” and is not on a “Deny database,” then “the connection is allowed.” See, e.g., Ex. 1008, 16:57–67.

Patent Owner argues that Wesinger fails to disclose intercepting a request to look up an internet protocol (IP) address of the second network device, as recited in claim 1, for example. In particular, Patent Owner argues that Wesinger discloses “prompts from the firewall in the prior art ‘custom’ embodiment” but “does not disclose that they function as or result in a request to look up an IP address as claimed” and “does not disclose combining the name prompts . . . of the prior art embodiment with its allegedly inventive disclosed embodiments.” PO Resp. 49, 50. We are not

persuaded by Patent Owner's argument. Even if the alleged "prompts" from the firewall of Wesinger do not "function as or result in a request to look up an IP address," as Patent Owner contends, Patent Owner does not demonstrate that the request from the user also does not "function as or result in a request to look up an IP address." As previously discussed above, Wesinger discloses that "the firewall . . . receives from the user a *request* pertaining to a first entity." For at least the previously discussed reasons, we are not persuaded by Patent Owner that the request from the user in Wesinger materially differs from the claimed "request."

Patent Owner argues that Wesinger fails to disclose "intercepting" under the construction that "intercepting" must include "evaluating the request in relation to establishing a secure communication link." PO Resp. 51. Claim 1 recites intercepting a request to look up an internet protocol (IP) address of the second network device based on a domain name associated with the second network device and determining (in response to the request) whether the second network device is available for a secure communications service. Patent Owner appears to re-iterate arguments that Wesinger fails to disclose intercepting a request to look up an IP address of the second network device based on a domain name and determining, in response to the request, whether the second network device is available for a secure communications service, as recited in claim 1, for example. For at least the previously discussed reasons, we are not persuaded by Patent Owner's argument.

Regarding claims 8, 9, 22, and 23, Patent Owner argues that Wesinger discloses devices that "need not be a mobile device, such as the claimed notebook computer." PO Resp. 53. Thus, Patent Owner argues that

Wesinger fails to disclose a notebook computer. We are not persuaded by Patent Owner's argument. Patent Owner does not contest that Wesinger discloses a "computer." One of ordinary skill in the art at the time of the invention would have understood that a "notebook computer" is a "computer" and immediately would have envisioned Wesinger as describing both desktop and notebook computers as both types of computers would have been used to connect to networks.

Regarding claims 10 and 29, Patent Owner argues that Wesinger fails to disclose receiving the request to determine whether the second network device is available for secure communications service, the request being the request to look up an internet protocol (IP address of the second network). PO Resp. 53–54. Patent Owner also argues that "the DNS query [of Wesinger] is not received . . . 'to determine whether the second network device is available for the secure communications service.'" PO Resp. 54. Regarding claims 14 and 28, Patent Owner argues that Wesinger discloses a "firewall [that] makes the . . . determination as a function of an 'ensuing' connection request following the DNS query and resolution process" but that the determination "is not a function of a domain name look up." PO Resp. 55. We are not persuaded by Patent Owner's arguments for at least the previously discussed reasons.

B. Wesinger and RFC 2543 – Claims 4–7 and 18–21

Patent Owner argues that it would not have been obvious to one of ordinary skill in the art to have combined the teachings of Wesinger and RFC 2543 because "Wesinger teaches away from . . . RFC 2543." PO Resp. 56–57.

As previously discussed, Wesinger discloses a system in which a client sends a connection request for connection with a device and, if access is granted and “[i]f all the rules are satisfied, then the connection [with the device] is allowed.” Ex. 1008, 16:66–67. Petitioner does not indicate that Wesinger discloses a specific type of connection or session between devices. The RFC 2543 reference discloses a similar system in which a client “send[s] a request” in order to “establish . . . multimedia sessions or calls.” Ex. 1012 at 7, 13. Thus, RFC discloses that one of ordinary skill in the art would have known that different types of connections or sessions that may be established between devices include, for example, multimedia session or calls. We agree with Petitioner that the combination of such known features, performing their known functions, would have resulted in the mere predictable result of a system in which a connection or session is established between devices (Wesinger and RFC 2543), the connection or session being, for example, a multimedia session or call (RFC 2543).

Patent Owner argues that it would not have been obvious to one of ordinary skill in the art to have combined Wesinger and RFC 2543 because, according to Patent Owner, Wesinger discloses a “firewall [that] should ideally . . . not have any other user-accessible programs running on it” to avoid “security risks.” PO Resp. 56, 57 (citing Ex. 1008, 3:25–41, 7:1–5).

As an initial matter, Wesinger discloses one possible scenario in which the firewall “ideally” does not have other user-accessible programs running on it. Ex. 1008, 7:2. Wesinger merely discloses one potential option but does not disclose that the firewall *must not* have any other user-accessible programs running on it. For at least this reason, we are not persuaded by Patent Owner’s arguments.

Also, Patent Owner does not demonstrate sufficiently that the established session between devices in Wesinger requires “any other user-accessible programs running on it” beyond applications needed to establish the desired connection or that if the session in Wesinger is a known “multimedia session or call,” that such a session would require such additional “user-accessible programs.” One of ordinary skill in the art would have understood that a “multimedia session or call” connection between devices established in Wesinger would involve applications needed for the establishment of the desired connection and not include extraneous, unnecessary applications because, at least, the non-inclusion of unnecessary elements would be a matter of common sense, the unnecessary elements not being of any use. Hence, even if Wesinger discloses that the firewall *must not* have “other user-accessible programs running on it” (Patent Owner does not demonstrate or allege that Wesinger discloses or suggests this alleged requirement, however), Patent Owner does not show persuasively that a firewall for establishing a specifically desired type of connection between devices requires such “other user-accessible programs.”

Patent Owner argues that there an “express teaching in Wesinger that merging these applications [of RFC 2543] with Wesinger’s architecture or system is undesirable because it may lead to further security risks.” PO Resp. 57 (citing Ex. 2025 ¶ 69). While Patent Owner points out that Wesinger discloses that the firewall “ideally” does not have other user-accessible programs running on it (Ex. 1008, 7:2), Patent Owner does not demonstrate persuasively that Wesinger, in fact, also provides an “express teaching” that “merging” applications is undesirable, that such “merging” actions would lead to “further security risks,” or that “merging applications”

is necessary to provide for a multimedia connection between devices, for example.

C. Declaration of Michael Fratto

Patent Owner argues that the Declaration of Michael Fratto Regarding U.S. Patent No. 8,504,697 (Ex. 1003) should not be given any weight. *See, e.g.*, PO Resp. 1–8. We did not rely on the testimony of Mr. Fratto in this decision. Therefore, Patent Owner’s argument is moot.

ORDER

Petitioner has demonstrated, by a preponderance of the evidence, that claims 1–3, 8–11, 14–17, 22–25, and 28–30 are anticipated by Wesinger, under 35 U.S.C. § 102, and that claims 4–7 and 18–21 are unpatentable over Wesinger and RFC 2543, under 35 U.S.C. § 103(a).

In consideration of the foregoing, it is hereby:

ORDERED that claims 1–11, 14–25, and 28–30 of the ’697 patent have been shown to be unpatentable;

This is a final decision. Parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2014-00238
Patent 8,504,697 B2

PETITIONER:

Jeffrey P. Kushan
Joseph A. Micallef
SIDLEY AUSTIN LLP
jkushan@sidley.com
jmicallef@sidley.com

PATENT OWNER:

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

Jason E. Stach
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, LLP
jason.stach@finnegan.com