Trials@uspto.gov
571-272-7822

Paper 10
Date: January 14, 2016

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SYMANTEC CORP.,
Petitioner,
v.

FINJAN, INC.,
Patent Owner

Case IPR2015-01545
Patent 7,756,996 B2

Before THOMAS L. GIANNETTI, RICHARD E. RICE, and MIRIAM L. QUINN, *Administrative Patent Judges.*

GIANNETTI, *Administrative Patent Judge*.

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

Symantec Corporation ("Petitioner") filed a Petition pursuant to 35 U.S.C. §§ 311–319 to institute an *inter partes* review of claims 1–7 (all claims) of U.S. Patent No 7,756,996 B2, issued on July 13, 2010 (Ex. 1001, "the '996 patent"). Paper 1 ("Pet."). Finjan, Inc. ("Patent Owner") filed a Preliminary Response. Paper 8 ("Prelim. Resp."). Applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim, we deny Petitioner's request and deny institution of an *inter partes* review of all challenged claims.

I. BACKGROUND

A. The '996 Patent (Ex. 1001)

The '996 patent is titled "Embedding Management Data Within HTTP Messages." The Abstract describes the invention as follows:

> A system for embedding messages within HTTP streams, including a gateway communicator, situated within a network gateway computer that communicates with at least one client computer, for receiving management data intended for the at least one client computer from a management server computer that communicates with the network gateway computer, a gateway data embedder situated within the network gateway computer for inserting non-HTTP management data within an HTTP message, and a client data extractor situated within each of the at least one client computer for extracting non-HTTP management data from within an HTTP message. A method and a computer readable storage medium are also described and claimed.

Ex. 1001, Abstract.

The invention is illustrated by Figures 1 and 2 of the patent, reproduced here:

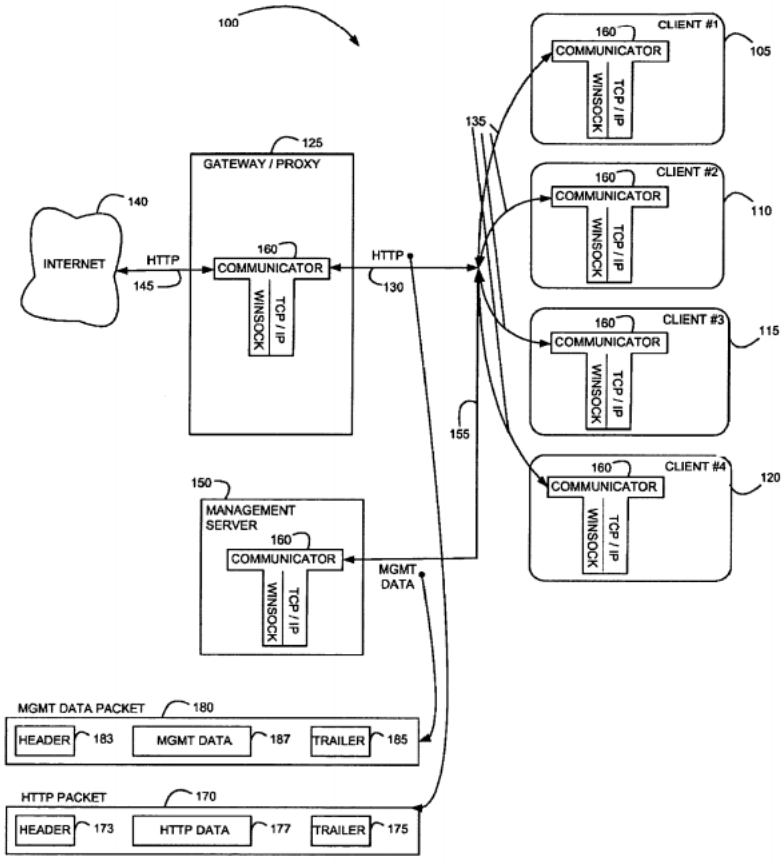

FIG. 1
(PRIOR ART)

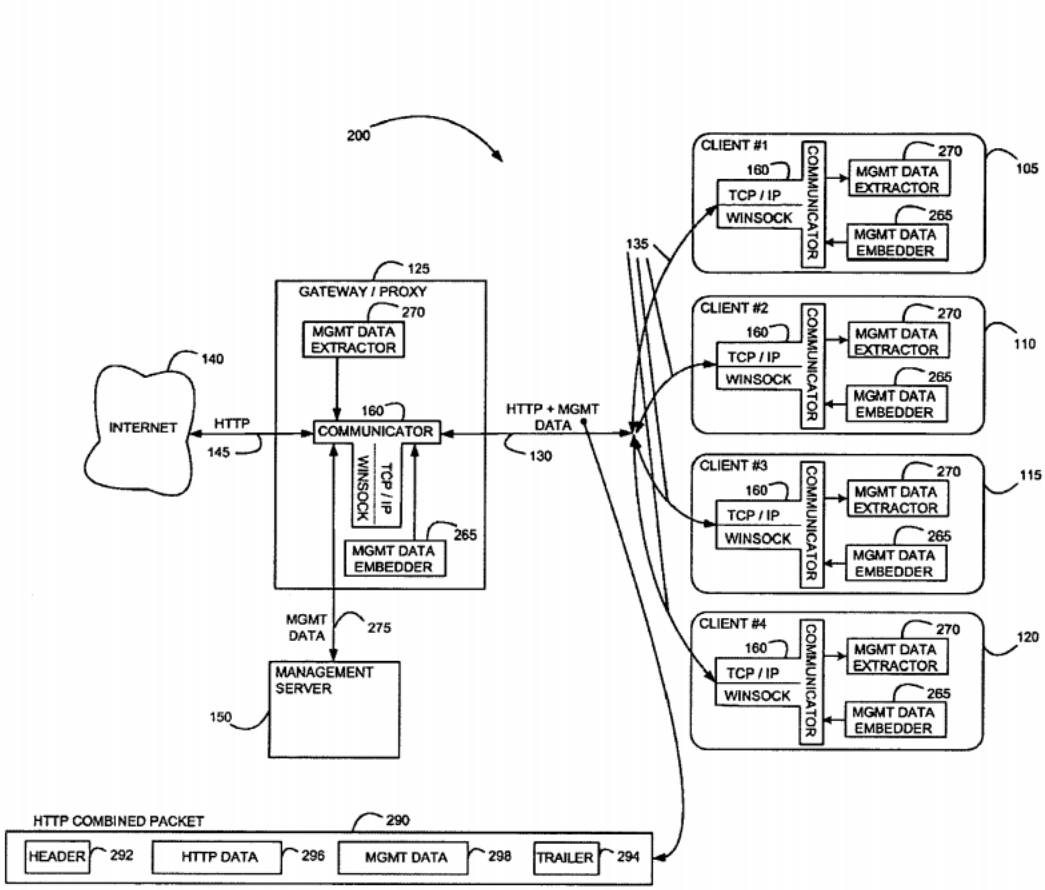

FIG. 2

Figure 1 is a simplified block diagram of prior art system 100 for transmitting management data back and forth between a management server computer and a plurality of client computers. Ex. 1001, col. 3, ll. 4–7. Figure 2 is a simplified block diagram of system 200 for embedding messages within HTTP streams, in accordance with a preferred embodiment of the invention of the '996 patent. *Id.* at col. 3, l. 66–col. 4, l. 2. The patent states that for the sake of clarifying the improvement that system 200 offers

over prior art system 100, like numerals, in the 100-199 range, are used in both figures for common components, and numerals in the 200-299 range are used for components that are unique to Figure 2. *Id.* at col. 4, ll. 2–7.

Shown in Figure 1 are client computers 105, 110, 115, and 120, within a corporate intranet, connected to corporate gateway computer 125 via communication lines 130 and 135. Gateway computer 125 may alternatively be a proxy computer. *Id.* at col. 3, ll. 7–12. Gateway computer 125 connects to Internet 140 via communication line 145. Client computers 105, 110, 115, and 120 typically use web browsers to send requests and responses across the corporate intranet, and across the Internet. *Id.* at col. 3, ll. 12–16.

Also shown in Figure 1 is management server 150, connected to clients 105, 110, 115, and 120 via communication line 155. *Id.* at col. 3, ll. 17–19. Management server 150 and clients 105, 110, 115, and 120 regularly transmit management data back and forth. Such management data may include, for example, network resource queries and responses, queries and responses to ascertain current versions of anti-virus signature files, and updated signature files. *Id.* at col. 3, ll. 26–31.

Figure 2 shows a similar network architecture, in which client computers 105, 110, 115, and 120 are connected to gateway computer 125 and to management server computer 150 within a corporate intranet. *Id.* at col. 4, ll. 8–11. However, in distinction to Figure 1, management server 150 sends and receives its management data through gateway 125. Generally, management data is formatted for transmission using a proprietary, non-HTTP protocol. *Id.* at 11–15.

In Figure 2, clients 105, 110, 115, and 120, and gateway 125 include management data embedders 265 and management data extractors 270. Management data embedder 265 embeds management data within HTTP messages, and management extractor 270 extracts management data from the HTTP messages. *Id.* at col. 4, ll. 16–21.

Management server 150 in Figure 2 sends and receives management data over communication line 275 between management server 150 and gateway 125, instead of directly over communication lines 135, as in Figure 1. As shown in Figure 2, HTTP packets 290, containing combined HTTP data plus management data and travelling over communication lines 130 and 135, include also TCP/IP header data 292, TCP/IP trailer data 294, and a body that includes both HTTP data 296 and management data 298. Thus, packets 290 of Figure 2 replace packets 170 and 180 of Figure 1. *Id.* at col. 4, ll. 41–51.

B. Illustrative Claim

The '996 patent has three independent claims: claims 1 (directed to a system), 4 (directed to a method), and 7 (directed to a computer storage medium). Claim 4 illustrates the relevant subject matter of the patent:

> 4. A method for embedding management data within HTTP messages, comprising:
>
> receiving server-originated non-HTTP management data from a management server computer intended for at least one client computer;
>
> inserting the server-originated non-HTTP management data within a server-originated HTTP message prior to the server-originated HTTP message being transmitted to the at least one client computer;

extracting the server-originated non-HTTP management data from within the server-originated HTTP message subsequent to the server-originated HTTP message being received by the at least one client computer;

receiving a client-originated HTTP message, the client originated HTTP message having client-originated non HTTP management data embedded therewithin;

extracting the client-originated non-HTTP management data from the client-originated HTTP message; and

transmitting the client-originated non-HTTP management data to the management server computer.

C. Related Proceedings

Patent Owner and Petitioner are involved in ongoing litigation, *Finjan, Inc. v. Symantec Corp.,* Case No. 3:14-cv-02998-RS (N.D. Cal.), in which the '996 patent has been asserted. Petitioner also has filed a second Petition for *inter partes* review of the '996 patent in Case No. IPR2015-01546. We express no views here on the challenges to patentability of the '996 patent in that case, as those are addressed in a separate Decision on Institution we are issuing concurrently in IPR2015-01546.

D. Real Party-in-Interest

The Petition names one real party-in-interest: Symantec Corporation. The Preliminary Response does not challenge this. However, Patent Owner had advised the Board of its contention that all real parties-in-interest have not been named. Paper 9. In view of our decision not to institute trial, we do not reach this issue.

E. Claim Construction

In an *inter partes* review, claim terms in an unexpired patent are construed according to their broadest reasonable interpretation in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b); Office Trial Practice Guide, 77 Fed. Reg. 48,756, 48,766 (Aug. 14, 2012); *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1275–79 (Fed. Cir. 2015). Under that standard, claim terms are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). However, the claims should always be read in light of the specification and the teachings of the underlying patent. *Microsoft Corp. v. Proxyconn, Inc*., 789 F.3d 1292, 1298 (Fed. Cir. 2015). Thus, the claims "cannot be divorced from the specification and the record evidence." *Id.* (internal quotes omitted).

Petitioner has requested construction of two terms: "non-HTTP management data" and "network gateway computer." Pet. 10–12. Patent Owner has responded that the terms need no construction and that the plain and ordinary meaning of the terms should apply. Prelim. Resp. 8–13.

We agree with Patent Owner that Petitioner's proffered construction of "non-HTTP management data" ("data that the management server transmits and receives using a non-HTTP transport protocol") is unnecessary. Prelim. Resp. 8–9. We therefore adopt the plain meaning suggested by Patent Owner: "management data that is not HTTP." *Id*. at 8. In reaching this conclusion, we note that the '996 patent makes a distinction between management data (e.g., security management data from a

management server) and "regular HTTP traffic that runs back and forth between client web browsers and a corporate gateway or HTTP proxy." Ex. 1001, col. 1, ll. 49–52.

We agree also that no special construction of "network gateway computer" is necessary. We adopt, instead, the plain meaning of the term. In that regard, we are guided by the definition in THE IEEE STANDARD DICTIONARY OF ELECTRICAL AND ELECTRONICS TERMS 449 (Sixth ed. 1996): "In networking, a device that connects two systems that use different protocols." Ex. 3001.

F. References

Petitioner relies on the following three references:

1. Bavadekar Pub. No. US 2003/0009571 A1, published Jan. 9, 2003 (Ex. 1002)
2. Binding et al. U.S. Patent No. 6,775,772 B1, filed Oct. 12, 1999 (Ex. 1004)
3. Greaves et al. Pub. No. US 2003/0225883 A1, published Dec. 4, 2003 (Ex. 1003)

G. Grounds Asserted

The Petition asserts the following grounds of unpatentability:

References	Basis	Claim(s) Challenged
Bavadekar	§ 102(b)	4, 5, and 7
Bavadekar	§ 103(a)	1–3, 5, and 6
Binding	§ 103(a)	1–7
Greaves	§ 103(a)	1–7

In addition to the supporting argument for these grounds in the Petition, Petitioner presents expert testimony. Ex. 1005, Declaration of Clifford Neuman ("Neuman Decl.").

II. ANALYSIS

A. Asserted Grounds Based on Bavadekar

1. Bavadekar Overview

Bavadekar is titled "System and Method for Providing Tunnel Connections Between Entities in a Messaging System." The reference describes using an HTTP tunnel connection to facilitate messaging between clients and brokers. According to the Abstract:

> An HTTP tunnel connection layer is described that may be used to provide reliable, full duplex virtual connections between entities (e.g. clients and brokers) in a distributed application environment using a messaging system. Also described is a novel HTTP tunneling protocol that may be used by the HTTP tunnel connection layer. The HTTP tunnel connection layer may be used by clients to access messaging servers through proxy servers and firewalls, thus expanding the scope of from where clients can access brokers. Using this layer, brokers as well as clients may initiate messaging system messages. This layer may also provide guaranteed data delivery with correct sequencing even in case of a failure on the network. This layer may also provide end-to-end flow control.

Ex. 1002, Abstract.

According to Bavadekar, using a transport protocol tunnel connection layer, if a client is separated from a broker by a firewall, messaging may be run on top of transport protocol connections that are normally allowed

through the firewalls. *Id.* ¶ 71. On the client side, a transport protocol transport driver may encapsulate messages into transport protocol packets and also may ensure that these packets are sent to the Web server in the correct sequence. *Id.* This is illustrated in Figure 3A of Bavadekar, reproduced here:

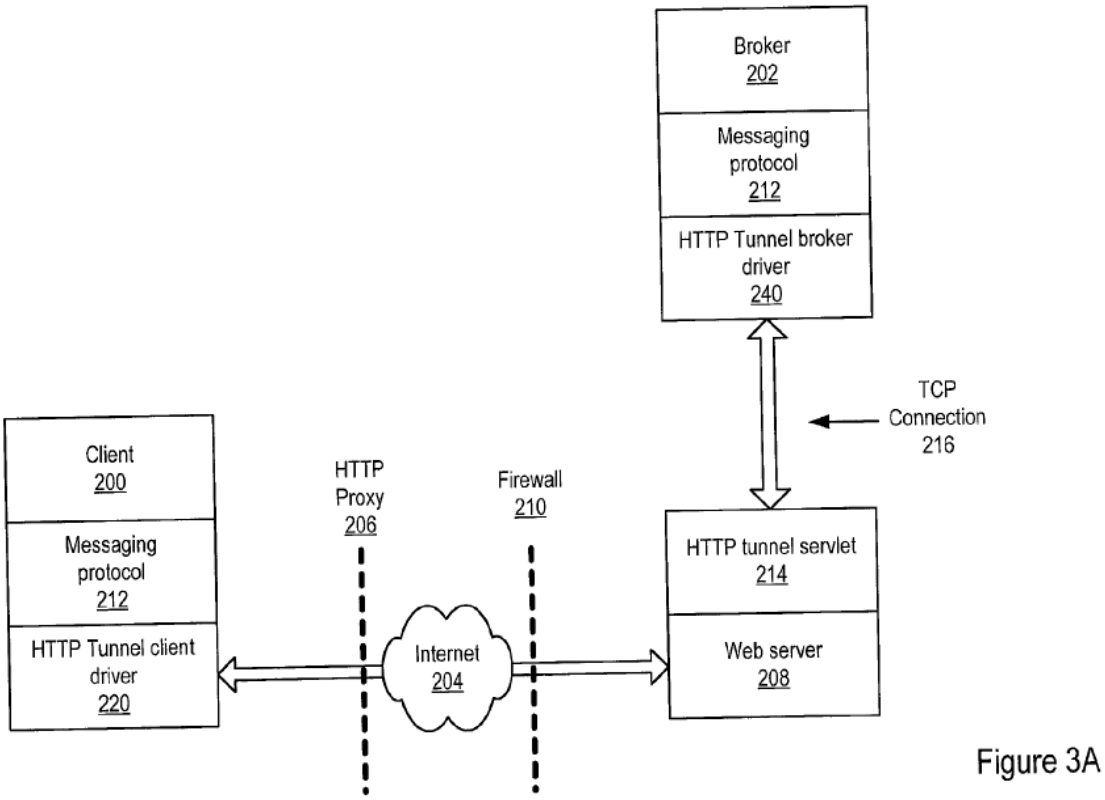

Figure 3A

Figure 3A from Bavadekar illustrates a client-server messaging system implementing an HTTP tunnel connection layer. Ex. 1002 ¶ 73. As shown in Figure 3A, client 200 may generate messages using messaging protocol 212. Such generated messages may then be passed to HTTP tunnel

client driver 220. Client driver 220 may then send the messages as HTTP POST-request payloads. *Id.* ¶ 74. The HTTP request may be sent through HTTP proxy 206, Internet 204, and firewall 210, to Web server 208. On Web server 208, HTTP tunnel servlet 214 may act as a transceiver, and may multiplex the HTTP request from multiple clients into a single TCP connection 216 with broker 202. HTTP tunnel broker device 240 may receive the HTTP requests from Web server 210 over TCP connection 216. *Id.*

Using the HTTP tunneling protocol layer, broker 202, as well as clients 200, may initiate messaging system messages. *Id*. ¶ 89. Broker 202 may generate HTTP packets that include message data as payloads, and transmit the HTTP packets to Web server 208 over a TCP connection. *Id.*

2. Anticipation of Claims 4, 5, and 7

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987).

Petitioner asserts that Bavadekar anticipates claims 4, 5, and 7. Pet. 14–21. Petitioner, however, has not provided element-by-element claim charts demonstrating how each claim limitation is met by Bavadekar, or for any of the other references relied upon in the Petition. Such claim charts, although encouraged, are not required. But the absence of claim charts does not relieve Petitioner from having to provide a "full statement of the reasons for the relief requested." 37 C.F.R. § 42.22(a)(2). We must, therefore,

consider whether the information in the Petition is sufficient to demonstrate a reasonable likelihood of prevailing on this challenge. 35 U.S.C. § 314(a).

Petitioner has provided a chart for independent claims 1, 4, and 7, showing the limitations of those three claims in a side-by-side format. Pet. 7–8. Petitioner assigns labels to each limitation, and equates many of the limitations that appear in all three independent claims. For example, according to the chart, claim element [B] ("receiving server-originated non-HTTP management data from a management server computer intended for at least one client computer") or equivalent is present in all three independent claims.

Petitioner's analysis treats these common elements together. Petitioner acknowledges: "[o]ther than the claim format (*i.e.*, system, method and computer-readable storage medium), independent claims 1, 4, and 7 recite substantially similar limitations." Pet. 6–7. According to Petitioner, "[t]he only meaningful difference is that claim 1 is directed to a system and further requires a 'network gateway computer storing a network gateway communicator,' to communicate with a client, management server, and HTTP server, and data 'embedders' and 'extractors' on the client and gateway." *Id.* at 7. Consequently, we will discuss the claims separately only where differences are relied on by Petitioner.

Petitioner asserts that Bavadekar discloses "each and every limitation of claims 4, 5, and 7." Pet. 14. For example, Petitioner equates Bavadekar's "tunneling" with "embedding management data within HTTP messages" in '996 patent claim 4. *Id.* Petitioner additionally equates Bavadekar's

"brokers" with the management server computer in the '996 patent claims. *Id.* at 15–16.

Patent Owner takes issue with this analysis and asserts that several claim elements are missing from Bavadekar. Prelim. Resp. 13–22. For example, Patent Owner argues that Bavadekar is directed to enabling clients to access brokers through firewalls. Prelim. Resp. 15. As a result, according to Patent Owner, Bavadekar fails to disclose "several key features of the challenged claims, including (1) receiving non-HTTP management data intended for at least one client computer and (2) inserting the non-HTTP management data within an HTTP message prior to the HTTP message being transmitted to the at least one client computer." *Id.*

Patent Owner points out that in Bavadekar, the same computer that generates the message also generates the HTTP packet with the message as the payload. *Id.* at 16. As a result, message data is never "received from" the management server computer as these claims require. *Id.* at 17. We find this argument persuasive. In the '996 patent, the management server is separate from the gateway that receives the management data. *See* Fig. 3, reproduced *supra*. The claims reflect this by reciting "receiving server-originated non-HTTP management data from a management server computer intended for at least one client computer." Petitioner has failed to show that this element is met by Bavadekar.

Patent Owner also argues that Petitioner fails to identify where Bavadekar describes inserting management data into HTTP messages. Prelim. Resp. 19. Patent Owner argues that there is a distinction between the "message data" described in Bavadekar and "management data" in the

'996 patent claims. As Patent Owner explains, "Bavadekar generates traditional HTTP packets for the sole purpose of transferring its payload while the '996 Patent claims inserting management data in HTTP messages for procuring management related functionality." Prelim. Resp. 19–20.

We agree with Patent Owner. As we noted *supra*, the '996 patent makes a distinction between normal HTTP messages generated by browsers and Web servers and management data:

> Management data is typically transmitted back and forth over a network typically using a proprietary non-HTTP protocol, and thus creates additional traffic, above and beyond the HTTP traffic. Such additional traffic increases the number of packets traveling on the network, and the processing required to handle them.

Ex. 1001, col. 1, ll. 29–34. We further agree with Patent Owner that the claims reflect this difference by specifying that management data is "server originated," and is sent and received by the management server using a non-HTTP protocol.

We are persuaded that Petitioner has failed to show that the "payload" messages in Bavadekar are "management data" or are "server originated." *Id.* at 20. That difference is understandable, for, unlike the '996 patent, Bavadekar is not directed to optimizing bandwidth by enabling management and security systems to "piggy back" on top of regular HTTP traffic that runs back and forth between client web browsers and a corporate gateway or HTTP proxy. Ex. 1001, col. 1, ll. 49–52. Bavadekar is directed to the different problem of providing an HTTP tunnel connection layer that may be used to provide reliable, full-duplex virtual connections between entities

(e.g. clients and brokers) in a distributed application environment. Ex. 1002, Abstract. "The HTTP tunnel connection layer may be used by clients to access messaging servers through proxy servers and firewalls, thus expanding the scope of from where clients can access brokers." *Id.*

We conclude, for the foregoing reasons, that Petitioner has not demonstrated that it is reasonably likely to prevail on this challenge to claims 4 and 7 based on anticipation.

Petitioner provides a separate anticipation analysis for Claim 5. Pet. 21–22. Claim 5 depends from claim 4. For this reason, our analysis of claim 4, *supra*, applies also to claim 5. We conclude that Petitioner has not demonstrated that it is reasonably likely to prevail on this challenge.

3. Obviousness of Claims 1–3, 5, and 6

Under 35 U.S.C. § 103(a), an invention is not patentable if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and, (4) where in evidence, so-called secondary considerations, including commercial success, long-felt but unsolved needs, failure of others, and unexpected results. *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

A holding of obviousness can be based on a showing that "there was an apparent reason to combine the known elements in the fashion claimed." *KSR,* 550 U.S. at 418. However, such a showing requires:

> "[s]ome articulated reasoning with some rational underpinning to support the legal conclusion of obviousness" . . . [H]owever, the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ. *Id.* (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

In determining obviousness, the references must be considered as a whole. Thus, picking and choosing from a reference only the favorable parts and ignoring the rest is prohibited. *In re Hedges*, 783 F.2d 1038, 1041 (Fed. Cir. 1986). The court in *Hedges* elaborates:

> It is impermissible within the framework of section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art.

Id. (internal quotes and citation omitted).

Petitioner contends that claims1–3, 5, and 6 would have been obvious over Bavadekar. Pet. 22–34. Focusing first on claim 1, Petitioner contends that Bavadekar discloses "substantially all" of the limitations of that claim. Pet. 23. According to Petitioner:

> [t]o the extent Bavadekar does not explicitly disclose that the network gateway computer "receives a server-originated HTTP message intended for at least one client computer from an HTTP server" and inserts the non-HTTP server message (*i.e.*, management data) within this "received" HTTP message before

> it is sent to the client, these features would have been obvious based on the teachings in Bavadekar.

Pet. 23. To support this argument Petitioner relies on the Neuman Declaration. *Id.*

Patent Owner responds by arguing that Petitioner has failed to show that Bavadekar discloses a "network gateway" as the claims require. Prelim. Resp. 23. According to Patent Owner, the disclosure in Bavadekar relied on by Petitioner for this element in claim 1 does not teach the claimed feature. *Id.* Patent Owner contends further that other elements of claim 1 are missing from Petitioner's analysis. *Id.* at 23–26. Patent Owner also challenges Dr. Neuman's testimony concerning the rationale to modify Bavadekar. *Id.* at 25–30.

We agree that Petitioner has failed to show that Bavadekar discloses a "network gateway." Petitioner's discussion of this element refers to paragraphs 2, 40, and 41 of Bavadekar. These are general descriptions of Bavadekar's system and do not satisfy the requirement of our rules that the petition "specify where each element of the claim is found in the prior art." 37 C.F.R. § 104(b)(4). Likewise, Petitioner's references to Figs. 3A and 3B of Bavadekar and paragraph 111 of the Neuman Declaration—and the subsequent discussion of whether the gateway is a separate computer—do not satisfy our rules or help us in identifying where the network gateway is found in Bavadekar. The Petition (Pet. 25) and the Neuman Declaration (¶ 111) refer to the "HTTP tunneling components" acting as a "point of contact" between the clients and messaging server. This reference, however,

does not meet the requirement of showing that the gateway connects different networks.

We also agree with Patent Owner that Dr. Neuman has not provided a persuasive rationale for modifying Bavadekar. Prelim. Resp. 25–26; Neuman Decl. ¶¶ 104–09. Dr. Neuman's analysis does not take into account the fact that Bavadekar and the '996 patent are directed to solving different problems, as discussed *supra*. This is a factor which must be considered but was not addressed by Dr. Neuman. *Broadcom Corp. v. Emulex Corp.*, 732 F.3d 1325, 1334 (Fed. Cir. 2013):

> While a prior art reference may support any finding apparent to a person of ordinary skill in the art, prior art references that address different problems may not, depending on the art and circumstances, support an inference that the skilled artisan would consult both of them simultaneously.

Id.

We conclude that Petitioner has not demonstrated that it is reasonably likely to prevail on this challenge to claim 1.

Claims 2 and 3 depend from claim 1. For the reasons stated above for claim 1, we conclude that Petitioner has not demonstrated that it is reasonably likely to prevail on this challenge to those claims. Claims 5 and 6 depend from claim 4. Petitioner's analysis equates claim 2 with claim 5 and claim 3 with claim 6. Pet. 33–34. For the reasons stated, therefore, Petitioner has not demonstrated that it is reasonably likely to prevail on its challenge to those claims.

B. Asserted Ground Based on Binding

1. Binding Overview

Binding is titled "Piggy-Backed Key Exchange Protocol for Providing Secure Low-Overhead Browser Connections from a Client to a Server using a Trusted Third Party." The patent describes a "piggy-back" key exchange system for setting up a secure browser connection.

According to the Abstract the patent describes:

> A method, system, and computer program product for establishing security parameters that are used to exchange data on a secure connection. A piggy-backed key exchange protocol is defined, with which these security parameters are advantageously exchanged. By piggy-backing the key exchange onto other already-required messages (such as a client's HTTP GET request, or the server's response thereto), the overhead associated with setting up a secure browser-to-server connection is minimized. This technique is defined for a number of different scenarios, where the client and server may or may not share an encoding scheme, and is designed to maintain the integrity of application layer communication protocols. In one scenario, a client and a server exchange secure messages using a trusted third party.

Ex. 1004, Abstract.

The basic architecture of the system is illustrated in Figure 3 from Binding, reproduced here:

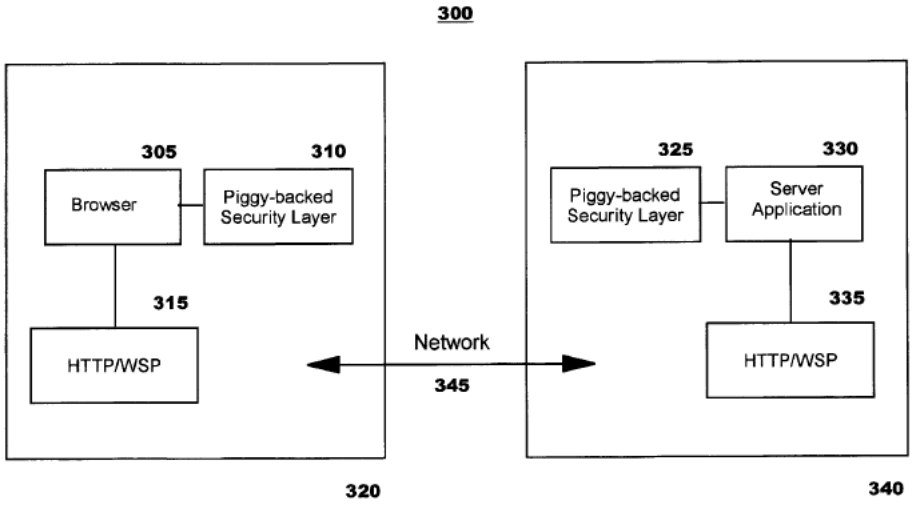

Fig. 3

Figure 3 from Binding depicts the basic architecture of system 300. Ex. 1004, col. 11, ll. 24–25. Client browser 305 is installed on client device 320. HTTP/WSP communication protocol engines 315, 335 operate as a lower layer in client device 320, as well as in server 340. *Id.* at col. 11, ll. 26–31.

Network connection 345, which may pass through a number of gateways and or transcoders, connects client communications protocol engine 315 to the server's corresponding communication protocol engine 335. Server application 330 operates at the application layer level of server 320. Binding states that the invention may be implemented using a client side HTTP proxy with a security plug-in, which handles encryption and decryption for client side HTTP applications. *Id.* at col. 11, ll. 32–42.

In one embodiment, the client and server do not have a common message and coding scheme with each other. They do, however, share an encoding scheme with a trusted third-party (TTP). *Id.* at col. 14, ll. 53–56. Binding discloses a novel key-exchange protocol, where secure information transmitted to a server is provided by piggy-backing security parameters onto existing message flows. *Id.* at col. 15, ll. 16–20. This exchange protocol is described in some detail in the patent at column 15, lines 16–63, and will be discussed further below.

2. Obviousness of Claims 1–7

Petitioner contends that these claims would have been obvious over Binding. Pet. 34–50. For example, Petitioner identifies the piggy-backed key exchange protocols in Binding as management data. Pet. 35. Petitioner identifies the trusted third party (TTP) in Binding as the management server. *Id.* Petitioner asserts that "Binding discloses substantially all of the limitations in the challenged claims." *Id.* Petitioner further asserts that

> to the extent Binding does not explicitly disclose that the management data embedded within an HTTP message and sent to a client is management data that has been received from the management computer, this feature would have been obvious based on the teachings in Binding.

Id.

Patent Owner responds that Petitioner's analysis of Binding is deficient in a number of respects. First, Patent Owner asserts that Binding's server 340 is not a "network gateway computer" to a person of ordinary skill. Prelim. Resp. 29. Patent Owner points out that Binding specifically mentions that network connection 345 may pass through a number of

gateways. *Id.* Thus a person of ordinary skill would be guided by that teaching in identifying the gateway in Binding.

Patent Owner's next argument is that Petitioner has failed to demonstrate that the encoding schemes and parameters in Binding are management data, or that the information is "intended for at least one client computer" as the claims require. *Id.* at 32. Patent Owner points out that the encoding schemes and "parameters" received at the server from the TTP in Binding are not intended for or received by the client. *Id.*

We are persuaded that Petitioner has failed to demonstrate that these requirements are met by Binding. We agree with Patent Owner that the parameters sent by the TTP to the server in Binding's example at column 15, lines 16–25, are not non-HTTP management data "intended for at least one client computer" for the reasons discussed by Patent Owner. Prelim. Resp. 31–33.

Moreover, we are not persuaded by the Petition or the Neuman Declaration that this would have been obvious in view of Binding. In discussing the TTP embodiment of Binding, the Neuman Declaration does not explain how the encoding information received at the server from the TTP would be intended for the client. In fact, the example in Binding and the Petition indicates that it is not, as Dr. Neuman acknowledges. Neuman Decl. ¶ 158 ("[E]ven if Binding does not explicitly disclose that management data that has been embedded within an HTTP message and sent to a client is management data that has been received from the management computer, this feature would have been obvious to a person of ordinary skill.").

Petitioner has not explained how the piggy-backed "parameters" sent from the TTP to the server in Binding ever reach the client. Prelim. Resp. 32–33; Ex. 1004, col. 15, ll. 16–25. Dr. Neuman discusses, instead, hypothetical "other parameters" (not the encoding information identified in the Petition) forwarded from the TTP to the server. Neuman Decl. ¶¶ 177–79. Dr. Neuman does not show where Binding teaches or suggests that such "other parameters from the TTP" exist, or that such information was intended for the client. We, therefore, are not persuaded by Petitioner's argument (Pet. 43–44) or Dr. Neuman's opinion (Neuman Decl. ¶¶ 177–80, 229) on this issue. Nor are we persuaded by Dr. Neuman's lengthy analysis of so-called APA (admitted prior art) (*id.* ¶¶ 202–53), or other matters that are not discussed in the Petition.

As each of claims 1–7 contains this limitation, we conclude that Petitioner has not demonstrated that it is reasonably likely to prevail on this challenge.

C. Asserted Ground Based on Greaves

1. Greaves Overview

Greaves is titled "System and Method for Reliable Delivery of Event Information." Petitioner describes Greaves as follows:

> Greaves is generally directed to monitoring and managing devices and/or appliances (referred to as "CMDs"), which may include networking and network security components such as routers/switches, gateways, servers, or firewalls. Greaves, ¶ 5, 17, 66. For example, a single unified datacenter can be used to aggregate information about and manage any number of devices on any number of sub-networks. *Id.*, ¶ 14. Neuman Decl., ¶ 254. Greaves explains, however, that

> these CMDs communicate using basic and somewhat unreliable protocols such as SNMP or Syslog. Greaves, ¶ 15. Accordingly, Greaves teaches a Control Tower Appliance (CTA) for communicating directly with these monitored devices using their respective native protocols. Greaves, ¶ 38. The CTA encodes the management data pertaining to the CMDs in an schema XML, and then further encapsulated the XML within an HTTP message, which is transmitted to a Control Tower Server (CTS) over the Internet. Greaves, ¶ 47, 42. The CTS receives the HTTP message, extracts the XML encoded message, and decrypts this XML to obtain the native management data. Greaves, ¶ 44-45. The CTS then processes this data directly or passes it along to further management tools, such as a backend network management system. Greaves, ¶ 48; *see also* Neuman Decl., ¶ 73-–74, 255-256.
>
> Similarly, Greaves teaches that the CTS and management system is able to communicate with the CTAs and CMDs (*e.g.*, by sending metadata, acknowledgements, sending polling requests, and/or remotely accessing them from a management server). Greaves, ¶ 37, 51, 55, 68. In other words, Greaves describes that the communications between the CTAs and management system through the CTS may be bidirectional. Neuman Decl., ¶ 256.

Pet. 49–50.

2. Obviousness of Claims 1–7

Petitioner argues that Greaves "teaches and/or suggests substantially all of the limitations of the challenged claims." Pet. 50. Petitioner further contends:

> [T]o the extent Greaves does not explicitly disclose that management data is sent back from the management server to clients via the same mechanisms Greaves describes for client-to-server communications (*i.e.*, by embedding the data within HTTP packets sent over the Internet), it would have been obvious to a POSITA to implement this bidirectional HTTP

> encapsulation, using the same HTTP encapsulation mechanism expressly taught in Greaves to send management data from the CTAs to the CTS. *Id.*, ¶ 271, 273–274

Id.

Patent Owner responds that the purpose of Greaves (secure and reliable delivery of event information provided by unreliable protocols over an Internet connection) "is completely unrelated to the purpose of the '996 patent." Prelim. Resp. 35.

Patent Owner points to several deficiencies in Petitioner's analysis of Greaves with respect to the '996 patent claims. First, Patent Owner contends that Petitioner's identification of the "network gateway computer" in the claims is wrong because it ignores the disclosure of separate gateway 329 in Greaves. *Id.* at 37; Ex. 1003 ¶ 68, Fig. 6. We agree that Petitioner's identification of the CTS in Greaves as the "network gateway" (Pet. 52) is contrary to the disclosure of Greaves. For at least this reason, we are not persuaded that this claim requirement is met.

Patent Owner contends that the analysis is deficient in other respects. Prelim. Resp. 37–40. For example, Patent Owner asserts: "Petitioner fails even to assert that Greaves teaches 'a server-originated HTTP message,' 'an HTTP server computer,' or that Greaves's CTS receives a server-originated HTTP message intended for the at least one client computer from an HTTP server computer." Prelim. Resp. 37. We agree with Patent Owner that Petitioner's analysis of these elements is conclusory and fails to persuade us that the elements are taught or suggested by Greaves.

We are unpersuaded by Petitioner's argument that such elements would have been obvious and agree with Patent Owner that Petitioner's

reliance on the Neuman Declaration to provide details that are missing from its Petition is misplaced. Dr. Neuman's testimony regarding Greaves is a repetition of the conclusory arguments presented in the Petition that we find to be unpersuasive. Neuman Decl. ¶¶ 254–57. Moreover, we agree with Patent Owner that Greaves is directed to solving a different problem. Dr. Neuman does not account for this in his analysis.

We conclude that Petitioner has not demonstrated that it is reasonably likely to prevail on this challenge.

III. ORDER

In view of the foregoing, it is

ORDERED that Petitioner's request for *inter partes* review of claims 1–7 of U.S. Patent No. 7,756,996 B2 is *denied*.

For Petitioner:

Joseph Richetti
Daniel Crowe
BRYAN CAVE LLP
joe.richetti@bryancave.com
dacrowe@bryancave.com

For Patent Owner:

James Hannah
Jeffrey Price
KRAMER LEVIN NAFTALIS & FRANKEL LLP
jhannah@kramerlevin.com
jprice@kramerlevin.com

Michael Kim
FINJAN INC.
mkim@finjan.com