

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

HEWLETT PACKARD ENTERPRISE COMPANY,

Petitioner

v.

K.MIZRA LLC,

Patent Owner.

IPR2022-00843

U.S. Patent No. 9,516,048

Before NATHAN A. ENGELS, AARON W. MOORE, and
IFTIKHAR AHMED, *Administrative Patent Judges*.

MOORE, *Administrative Patent Judge*.

DECISION

Denying Institution of Inter Partes Review

35 U.S.C. § 314

I. INTRODUCTION

Hewlett Packard Enterprise Company (“Petitioner”) filed a Petition (Paper 1, “Pet.”) for *inter partes* review of claims 1–20 of U.S. Patent No. 9,516,048 B2 (Ex. 1001, “the ’048 patent”). K.Mizra LLC (“Patent Owner”) filed a Preliminary Response (Paper 13, “Prelim. Resp.”).

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314; 37 C.F.R. § 42.4(a).

Having considered the parties’ submissions, and for the reasons explained below, we do not institute *inter partes* review.

A. *Related Matters*

Petitioner states that the ’048 patent “is or was involved in the following cases”:

K.Mizra LLC v. Hewlett Packard Enterprise Co., E.D. Tex. No. 2-21-cv-00305, filed August 9, 2021;

K.Mizra LLC v. Forescout Technologies, Inc., E.D. Tex. No. 2-21-cv-00248, filed July 8, 2021;

K.Mizra LLC v. Fortinet, Inc., E.D. Tex. No. 2-21-cv-00249, filed July 8, 2021;

Network Security Technologies, LLC v. Bradford Networks, Inc., D. Del. No. 1-17-cv-01487, filed October 24, 2017;

Network Security Technologies, LLC v. ForeScout Technologies, Inc., D. Del. No. 1-17-cv-01488, filed October 24, 2017;

Network Security Technologies, LLC v. McAfee, Inc., D. Del. No. 1-17-cv-01489, filed October 24, 2017; and

Network Security Technologies, LLC v. Pulse Secure, LLC, D. Del. No. 1-17-cv-01490, filed October 24, 2017.

Pet. 1–2. Patent Owner’s mandatory notices identify the Eastern District of Texas cases. *See* Paper 5, 1.

Petitioner also states that “[i]n IPR2021-00593, the Board instituted an IPR against a patent closely related to the ’048 patent, U.S. Patent No. 8,234,705 (‘the ’705 patent,’ Ex. 1019), based on the same prior-art combination presented in this petition” and that “the challenged claims are materially the same as the ’705 patent’s claims.” Pet. 1. On September 19, 2022, we issued a Final Written Decision in that IPR, finding no claims of the ’705 patent unpatentable. *See* IPR2021-00593, Paper 41.

B. Background

1. Summary of the ’048 Patent

The ’048 patent is titled “Contagion Isolation and Inoculation Via Quarantine.” It explains that then-current technologies for dealing with unauthorized and/or unwanted network communications “focus[ed] on filtering messages at a point in the communication path close to the recipient system, such as anti-spam and/or other security software installed on the destination host and/or a local mail (or other messaging) server to which communications to the destination host are directed for delivery to the destination host.” Ex. 1001, 1:29–37. The patent states that such an approach could be “an effective way to protect an individual host or a group of destination hosts served by a local server,” but that it “does not address the network congestion problem and leaves vulnerable hosts not protected by destination (or destination mail or messaging server) based filtering software.” *Id.* at 1:37–42. The patent further explains that “in many cases an attacker causes each of one or more compromised hosts to send multiple instances of a malicious communication, often simultaneously or nearly so, magnifying the effect on the network.” *Id.* at 1:42–46. The patent concludes that there is a “need for an effective way to intercept and take

corrective action with respect to unauthorized, unwanted, and/or otherwise malicious electronic mail and/or other network communications that better protects the network and provides protection to destination hosts that are not protected by destination or destination mail or messaging server based filtering software.” *Id.* at 1:46–52.

The independent claims of the ’048 patent are all directed to systems that employ a quarantine server, such as that shown in Figure 10B, reproduced below.

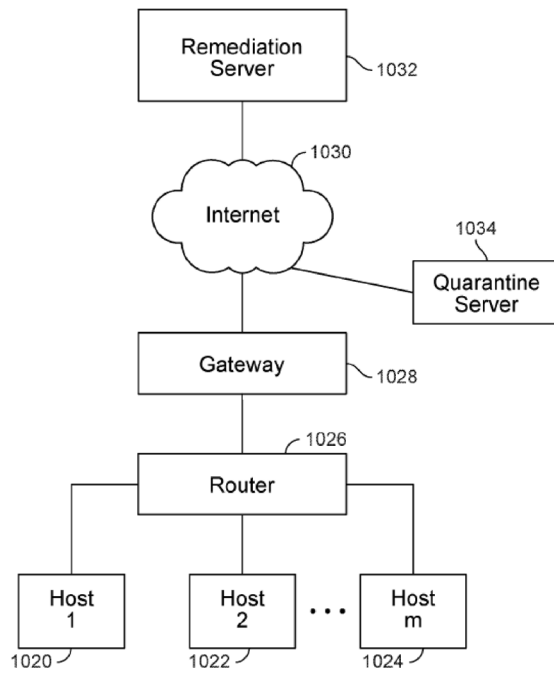


Figure 10B is “a block diagram illustrating a network environment in which infected hosts and/or networks are quarantined.” Ex. 1001, 2:25–27.

In this embodiment, hosts 1020 to 1024 “connect via a router 1026 and a gateway 1028 to the Internet 1030.” Ex. 1001, 12:13–15. Gateway 1028 “comprises a gateway, router, firewall, or other device configured to

provide and control access between a protected network and the Internet and/or another public or private network.” *Id.* at 12:18–21.

“[I]n the event of quarantine of one or more of hosts 1020-1024 . . . a quarantined host (or a host associated with a quarantined network or sub-network) is permitted to access a remediation server 1032, e.g., to download a patch, more current threat definition, etc.” Ex. 1001, 12:22–28.

“[R]equests to connection to a host other than the remediation server 1032 are redirected to a quarantine server 1034 configured to provide a notice and/or other information and/or instructions to a user of the quarantined host.” *Id.* at 12:29–33.

Figure 13 of the '048 patent, reproduced below, illustrates a flow diagram for infestation monitoring:

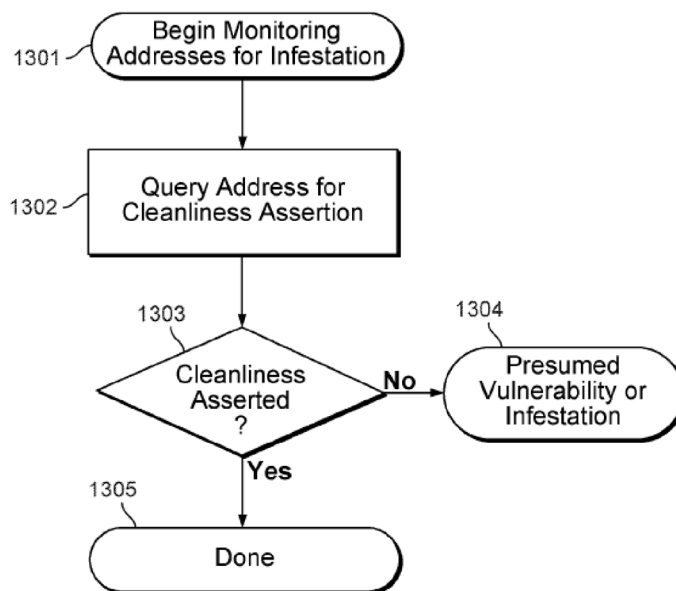


Figure 13 is “a flow diagram of a method for monitoring one or more computers for infestation.” Ex. 1001, 2:32–34.

In this example, “monitoring of a computer for infestation begins (1301) . . . by retrieving a list of one or more addresses of computers, such

as addresses of participating subscribers.” Ex. 1001, 14:13–16. In the next step (1302), “[a] computer associated with an address identified in a list is queried for a cleanliness assertion (1302), for example by contacting a trusted computing base within a computer, and requesting an authenticated infestation scan by trusted software.” *Id.* at 14:22–26. According to the patent, an “example of a trusted computing base is described in various TCG specifications, such as the TCG Architecture Overview, published by the Trusted Computing Group.” *Id.* at 14:29–32. “Trusted code bases may . . . execute antivirus scans of the remainder of the computer, including untrusted portions of the disk and/or operating system” and “may digitally sign assertions about the cleanliness (e.g. infestation status) and/ or state of their computers.” *Id.* at 14:32–37. In some embodiments, “the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus software, with assertions about the currency of a scan, such as the last time a scan was performed.” *Id.* at 14:37–41.

As shown in Figure 13, “[i]f a computer asserts it is clean (1303) then monitoring may be complete (1305),” but “[i]f a cleanliness assertion is not provided (1303) then an infestation or vulnerability is presumed (1304).” Ex. 1001, 14:47–51.

In some embodiments, “a quarantined host (or a host associated with a quarantined network or sub-network) is permitted to access a remediation server 1032, e.g., to download a patch, more current threat definition, etc.” *Id.* at 12:25–28. For example, a device such as a router may forward outbound traffic from a quarantined computer to a quarantine server. *See id.* at 12:28–33.

The use of a quarantine server is shown in Figure 16, “a flow diagram of a method for a quarantine server to respond to requests according to some embodiments.” Ex. 100, 16:17–18. In that example, “a quarantine server is started (1601)” and “waits for a request (1602), for example by listening on a port and waiting for a connection. *Id.* at 16:19–23. “If a received connection is a web server request (1603), such as an HTTP request, then the server responds with a quarantine notification page (1604).” *Id.* at 16:26–29. “If the request is not a web server request (1603), then it is tested to see if it is a DNS inquiry (1605)” and “[i]f the request is not a DNS inquiry (1605) then it may be discarded or responded to as “unreachable” (1606).” *Id.* at 16:39–44. If the request is a DNS inquiry, “the inquiry is tested to see if it is a DNS request for a remediation host name (1608)” and, if so, “the request is proxied to an external DNS service provider (1609).” *Id.* at 16:44–53. And, “[i]f the DNS inquiry was not for a remediation host name (1608) then an IP address for a quarantine server is provided (1607).” *Id.* at 16:56–58.

2. *The Challenged Claims*

The petition challenges claims 1–20. Of those, claims 1, 10, and 17 are independent. Claim 1 is directed to a method, claim 10 is to a system corresponding to the method of claim 1, and claim 17 is to a computer program product with instructions for performing a method corresponding to that of claim 1. Claim 1 is thus representative of the subject matter at issue:

1. A method, comprising:
 - detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network, wherein detecting the insecure condition includes contacting a trusted computing base associated with a

trusted platform module within the first host, receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness, wherein the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network, wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host, determining whether the service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request, wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and

permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.

Ex. 1001, 20:25–64.

3. *Asserted Grounds of Unpatentability*

Petitioner alleges that the challenged claims are unpatentable based on the following ground:

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1–20	§ 103	Gleichauf, ¹ Ovadia, ² Lewis ³

See Pet. 11. Petitioner also relies on a declaration of Mark T. Jones, Ph.D., filed as Exhibit 1003.

II. DISCUSSION

We discuss the level of ordinary skill in the art, claim construction, and then the merits of the proposed combination.

A. *Level of Skill in the Art*

The level of skill in the art is a factual determination that provides a primary guarantee of objectivity in an obviousness analysis. *See Al-Site Corp. v. VSI Int’l Inc.*, 174 F.3d 1308, 1323 (Fed. Cir. 1999) (citing *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966)).

Petitioner asserts that a person of ordinary skill in the art would have had “a working knowledge of the network communication art that is pertinent to the ’048 patent, including network security methodologies” and “a bachelor’s degree in computer science, computer engineering, electrical engineering, or an equivalent training, and approximately two years of

¹ U.S. Patent No. 9,436,820 B1 (Ex. 1005)

² U.S. Patent No. 7,747,862 B2 (Ex.1006).

³ U.S. Patent No. 7,533,407 B2 (Ex.1007).

professional experience in the field of network communications, and more specifically, network security.” Pet. 3–4 (citing Ex. 1003 ¶ 16). Petitioner also asserts that a “[l]ack of professional experience [could] be remedied by additional education, and vice versa.” *Id.* Patent Owner “reserves the right to dispute Petitioner’s definition if an IPR is instituted.” Prelim. Resp. 8.

For purposes of this analysis, we adopt Petitioner’s proposal, which we find generally consistent with the disclosures of the ’048 patent.

B. Claim Construction

The parties agree on a construction of “trusted computing base” but disagree on the meaning of “trusted platform module.” *See* Pet. 4–11; Prelim. Resp. 9–10.

In view of the analysis below, we find that we need not resolve the dispute over “trusted platform module,” and that no other claim construction is necessary. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (explaining that construction is needed only for terms that are in dispute, and only as necessary to resolve the controversy).

C. Obviousness

A claim is unpatentable under 35 U.S.C. § 103(a) 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 the subject matter pertains. *See 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, primarily: (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 ordinary skill in the art; and (4) objective evidence of nonobviousness. *Graham*, 383 U.S. at 17–18. Patent Owner does not offer objective evidence of nonobviousness or argue any secondary considerations.

Petitioner contends that claims 1–20 are unpatentable under § 103(a) over the combination of Gleichauf, Ovadia, and Lewis.

1. *Overview of Gleichauf (Ex. 1005)*

Gleichauf describes a system for controlling access to a network when a device attempts to connect to the network based on the “security posture” of the device. Ex. 1005, 3:7–9.

Figure 1 of Gleichauf is reproduced below.

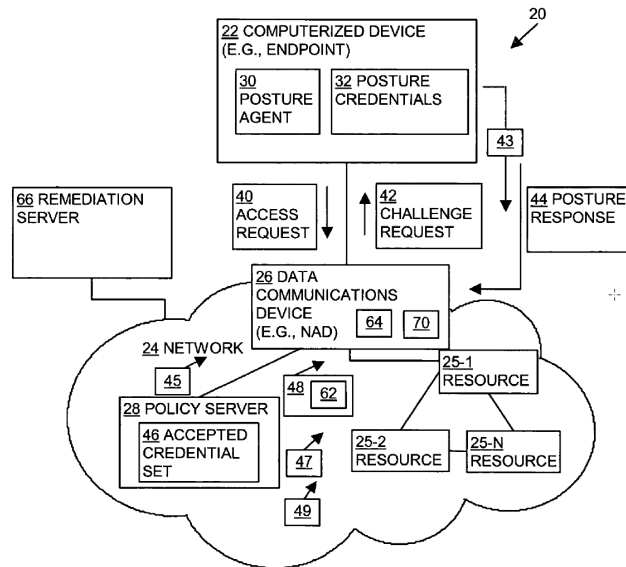


Figure 1 depicts “a data distribution system.” Ex. 1005, 7:30–31.

Data communication system 20 includes user device 22 and network 24, which includes network resources 25, data communications device 26, and policy server 28. Ex. 1005, 8:33–37. User device 22 may be a personal

computer, a cellular telephone, a personal digital assistant (“PDA”), etc. *Id.* at 8:40–43.

Gleichauf describes the “security posture” of user device 22 as the device status relating to the user device’s ability to resist reception or transmission of malware (e.g., viruses), content (spam and/or data theft), or access by unauthorized users. Ex. 1005, 8:52–56. Gleichauf also describes “posture credentials” as information associated with the “security posture” of a computing device. *Id.* at 3:30–32. According to Gleichauf, “posture credentials” can include the status of anti-virus applications on user device 22, the status of intrusion prevention applications (e.g., firewalls) associated with the user device, and the version and the update patch level associated with the operating system running on the user device. *Id.* at 8:61–9:1.

In one embodiment, a computerized device, e.g., a personal computer, transmits an access request to the data communications device in an attempt to access the network resources within the network. Ex. 1005, 3:50–56. The data communications device that detects the presence of the new device initiates a challenge-response sequence by sending a challenge request to the computer device. *Id.* at 3:60–67. In response, the posture agent running on that computer device retrieves posture credentials describing the security posture of the computerized device and transmits an initial challenge response back to the data communications device, which forwards the challenge response onto the policy server. *Id.* at 3:60–4:3.

Based upon an analysis of the posture credentials returned by the computerized device, the policy server determines what type of admission policy and level of network access and privileges should be extended to the computer device. Ex. 1005, 4:15–19. Devices that are compliant with the

network admission policy would typically be given full network access. *Id.* at 4:19–21. Devices that are only mildly out of compliance may be simply issued a warning that they are in danger of falling out of compliance with corporate policy. *Id.* at 4:21–24. Devices that are more significantly out of compliance may be placed on an isolated, or “quarantine,” network segment where they can be brought into compliance. *Id.* at 4:24–27. And devices that violate core admission requirements may be denied network access entirely. *Id.* at 4:27–28.

At the same time the policy server determines access, the policy server can transmit one or more notification messages to the posture agent or posture plug-ins running on the computer device attempting to gain access to the network. Ex. 1005, 4:56–60. The notifications may include the results of the posture check, remediation actions (if any), and an informational message to be displayed to the user, or written to a local log file. *Id.* at 4:60–63.

The notification message may contain text messages for display to a user, including any remediation actions to be performed. Ex. 1005, 21:1–5. For example, if a user device is non-compliant, the message may be displayed to the user indicating that the device has been quarantined and needs to be remediated. *Id.* at 21:6–8. The notification message may also include a link to a remediation server or the IP address of the remediation server. *Id.* at 21:8–10. If displayed to a user, the user may click on the link or the IP address to be redirected to the remediation server. *Id.* at 21:10–11.

The remediation server is configured to upgrade or provide up-to-date patches to the operating system or applications, such as anti-virus applications, associated with the computerized device. Ex. 1005, 5:8–11. If

the remediation process was successful, the device is admitted back to the original network. *Id.* at 5:11–13.

2. *Overview of Ovidia (Ex. 1006)*

Ovidia describes methods and apparatuses to authenticate base and subscriber stations and maintaining secure sessions for broadband wireless networks. *See* Ex. 1006, 3:62–64.

Ovidia describes an embodiment in which a Trusted Computing Group (TCG) security scheme (promulgated by the TCG) is implemented to generate, store, and retrieve security-related data in a manner that facilitates privacy and security in broadband wireless networks. Ex. 1006, 4:16–21. Ovidia further describes that a TCG token comprising a trusted platform module (TPM) is employed. *Id.* at 4:22–24. According to Ovidia, TCG is a standards organization and an industry consortium concerned with platform and network security. *Id.* at 4:17–21, 4:31–32. Ovidia describes that “[t]he TCG main specification (Version 1.2, October, 2003—hereinafter referred to as the ‘version 1.2 Specification’) is a platform-independent industry specification that covers trust in computing platforms in general.” *Id.* at 4:32–35.

Ovidia further explains that the TCG main specification defines a trusted platform sub system that employs cryptographic methods when establishing trust. Ex. 1006, 4:36–38. The trusted platform enables an authentication agent to determine the state of a platform environment and seal data particular to that platform environment. *Id.* at 4:40–43. Subsequently, authentication data (e.g., integrity metrics) stored in a TPM may be returned in response to an authentication challenge to authenticate the platform. *Id.* at 4:43–45.

In addition, Ovadia describes the details of Version 1.2-compliant TPM functions relating to security and privacy. Ex. 1006, 4:46–48. Figure 2 of Ovadia is reproduced below.

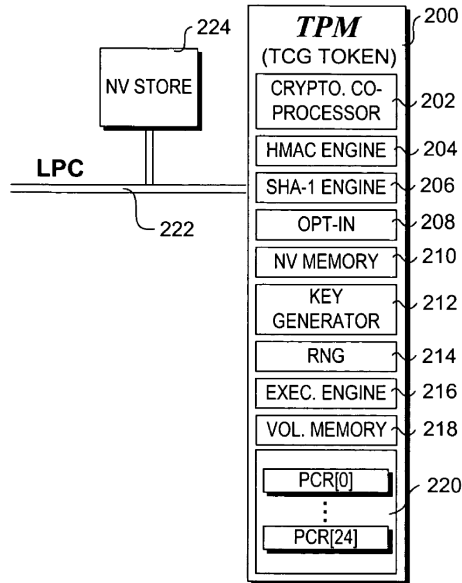


Figure 2 is “a schematic diagram of a trusted platform module.” Ex. 1006, 3:7–8.

Ovadia describes the TPM’s security functions, including security key generation, encryption, and hashing operations. Ex. 1006, 4:61–67. Ovadia also describes generating Attestation Identity Keys (AIKs) from the unique security key embedded in the TPM, which are used to digitally sign attestation of the integrity measurements. *Id.* at 5:31–38, 13:63–65.

3. Overview of Lewis (Ex. 1007)

Lewis relates to network access management and, specifically, to checking the security state of clients before allowing them access to network resources. Ex. 1007, 1:9–12.

Lewis describes a system for ensuring that machines having invalid or corrupt states are restricted from accessing network resources by providing a quarantine server located on a trusted machine in a network and a quarantine agent located on a client computer. Ex. 1007, 4:7–13. The quarantine agent requests a bill of health (BoH) from the quarantine server, which responds with a manifest of checks that the client computer must perform. *Id.* at 4:13–16. The quarantine agent then sends a status report on the checks back to the quarantine server. *Id.* at 4:16–18. If the client computer is in a valid state, the BoH is issued to the client. *Id.* at 4:18–19. A valid state may be that all necessary patches are installed, or that necessary security software is installed. *Id.* at 4:19–21. If the client computer is in an invalid state, the client is directed to install the appropriate software/patches to achieve a valid state. *Id.* at 4:21–23.

Figure 4 of Lewis is reproduced below.

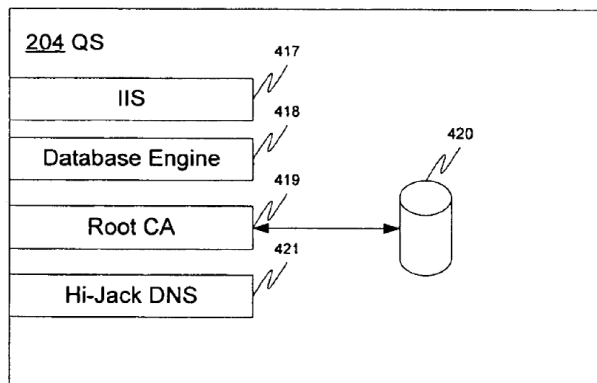


Figure 4 “illustrates a quarantine server.” Ex. 1007, 4:52–53.

Quarantine server (QS) 201⁴ comprises Internet Information Server (IIS) 417 for providing a default web page, database engine 418, and hijack DNS component 421. Ex. 1007, 10:61–11:17. When a client is in quarantine and a user opens a web browser on the client computer, QS 201 provides a web page to inform the user that the client machine is in quarantine and corrective action must be taken. *Id.* at 10:63–66. QS 201 also includes a hijack DNS component 421 for intercepting DNS queries from quarantined clients. *Id.* at 11:15–17.

4. *Analysis*

Petitioner contends that the combination of Gleichauf, Ovadia, and Lewis teaches the subject matter of claim 1. More specifically, Petitioner relies on Gleichauf to teach most of claim 1, except for (1) the “trusted platform module,” for which Petitioner relies on Ovadia, and (2) limitations relating to the operation of the recited “quarantine server,” for which Petitioner relies on Lewis. *See* Pet. 23–47 (claim 1 as a whole); 26–31 (adding Ovadia); 43–46 (adding Lewis).

Regarding the limitation “wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page,” Petitioner asserts that “Gleichauf discloses rerouting by responding to the service request sent by the first host with a redirect” but then relies on Lewis for the quarantine server, arguing that, in Lewis, “an

⁴ Although Figure 4 shows a quarantine server as QS 204, Lewis refers to the quarantine server as QS 201 in the textual description relating to Figure 4. *See* Ex. 1007, 10:61–11:17.

initial domain name service (DNS) request from the device is redirected to a quarantine server,” after which “the quarantine server supplies a default webpage on the quarantine server to the device.” Pet. 45; *see id.* at 44 (framing the change as “redirecting HTTP traffic from Gleichauf’s device to a quarantine server (per Lewis), rather than a remediation server.”).⁵

Petitioner also presents several reasons why a person of ordinary skill in the art would have combined Gleichauf, Ovadia, and Lewis in the manner proposed by Petitioner. *See id.* at 15–23; *see* Ex. 1003 ¶¶ 55–72.

Having carefully considered Petitioner’s evidence and arguments, we find Petitioner’s motivations to combine Lewis with Gleichauf insufficient to support a finding of unpatentability.

Application of a Known Technique

Petitioner first contends that the combination of Lewis with Gleichauf would have been obvious because “it uses the known technique of redirection of device traffic to a quarantine server that serves a webpage to the device, as in Lewis, to improve a similar method of traffic redirection, as in Gleichauf, in the same way,” and “it is merely the application of Lewis’s known technique of serving a webpage to a quarantined device with information and remediation instructions to Gleichauf’s and Ovadia’s known methods of providing a notification message identifying reasons for quarantine, yielding predictable results.” Pet. 21 (citing Ex. 1003 ¶ 69).

We find these arguments insufficient because they do not show that the artisan *would* have made the combination. Instead, they show, at best, that Gleichauf and Lewis *could* have been combined to meet the subject

⁵ Petitioner does not argue, so we do not consider, whether Gleichauf’s remediation server might be considered a “quarantine server.”

limitations, which is not enough. *See Belden Inc. v. Berk-Tek LLC*, 805 F.3d 1064, 1073 (Fed. Cir. 2015) (“obviousness concerns whether a skilled artisan not only *could have made* but *would have been motivated to make* the combinations or modifications of prior art to arrive at the claimed invention”) (citing *InTouch Techs., Inc. v. VGO Commc’ns, Inc.*, 751 F.3d 1327, 1352 (Fed. Cir. 2014)).

Providing Information to the User

Petitioner next asserts that one of ordinary skill “would have known that serving a webpage with remediation instructions to a quarantined device from a quarantine server would *beneficially provide information to the user while simultaneously preventing the device from accessing protected network resources.*” Pet. 21 (emphasis added) (citing Ex. 1007, 10:61–66, 13:63–14:1; Ex. 1003 ¶ 69).

As Petitioner acknowledges, however, Gleichauf *already* provides this benefit. For example, Petitioner acknowledges that Gleichauf discloses “notification messages” displayed to the user indicating that the device has been quarantined. Pet. 43 (“Gleichauf describes providing ‘one or more notification messages’ for display to a user ‘indicating that the device has been quarantined.’”) (citing Ex. 1005, 4:56–63, 21:1–12)). In the cited portion of Gleichauf, it describes how

[t]he notification message may contain a text message for display to a user or for logging to a log file (e.g., messages to display to the user or a log or URL’s of the remediation server 66 and any remediation actions to be performed) [and that,] [f]or example, in the case that a user device 22 is non-compliant, the message may be displayed to the user or written to a log file indicating that the device has been quarantined and needs to be remediated.

Ex. 1005, 21:1–8.

Petitioner also concedes that Gleichauf discloses how placing a user device in quarantine causes the network (and more specifically, data communication device 26 acting on directions from the policy server) to “restrict or completely reject communications from the user device 22 to the resources 25 within the network 24.” Pet. 40 (citing Ex. 1005, 11:58–67; Ex. 1003 ¶ 126).

Thus, Petitioner acknowledges that Gleichauf alone, without Lewis’s quarantine server, provides the Petitioner-identified benefit of “provid[ing] [quarantine] information to the user while simultaneously preventing the device from accessing protected network resources.”

Avoiding the Need for Other Software

Petitioner next argues that “Lewis’s quarantine webpage would also be advantageous to Gleichauf’s . . . notification message” because “[t]he webpage served by the quarantine server would be displayed in the browser that the user already has opened, which would advantageously *avoid necessitating additional software components* running on the device to receive and display the notification message to the user.” Pet. 21 (emphasis added) (citing Ex. 1005, 4:56–60; Ex. 1006, 16:62–65; Ex. 1003 ¶ 69).

Gleichauf’s notification messages, however, *already* provide that benefit, because Gleichauf discloses that the notification messages are generated in an “*application-independent*” form, such as the XML (extensible markup language) format. *See* Ex. 1005, 20:55–60 (emphasis added) (describing notification messages in the same embodiment cited by Petitioner). Gleichauf thus indicates that the notification messages may be displayed in a browser using XML, without the need for additional software running on the device to receive and display the notification message to the

user. Petitioner does not address this disclosure in Gleichauf or explain why a person of ordinary skill would have looked to Lewis to obtain the alleged benefit or advantage when Gleichauf already provides the same benefit or advantage.

Option To Terminate

Petitioner also argues that “[s]erving a webpage from a quarantine server would also provide the quarantined device’s user the option to proceed with the remediation or terminate the connection attempt” because, in the proposed combination, “the webpage would direct the user to a remediation server that can resolve the security issues” and, in the event “[a] user . . . does not have the time to remediate security issues,” the user “may opt to terminate the connection attempt.” Pet. 22 (citing Ex. 1003 ¶ 70). Petitioner contends that one of ordinary skill “would have understood the benefits of giving the user the option to choose their desired course of action.” *Id.* (citing Ex. 1003 ¶ 70).

We do not agree that this would have been an added benefit either, because Gleichauf already gives the user a choice of when to remediate. *See* Ex. 1005, 23:65–24:2 (explaining that “a user ‘may’ click on a link to a remediation server”). Gleichauf describes that “[t]he notification message may also include *a link to a remediation server* or the IP address of the remediation server [] that *a user may click on.*” Ex. 1005, 23:65–67 (emphases added). Thus, Gleichauf alone provides the benefit or advantage of giving the user a choice or option of remediating now or later by displaying a notification message to the user that includes a link to a remediation server that the user may or may not click on to remediate now or later.

* * *

Because we find that Gleichauf already has the benefits or advantages that the addition of Lewis would allegedly provide, we conclude that Petitioner fails to show that a skilled artisan would have been motivated to combine Lewis with Gleichauf. *Cf. In re Anova Hearing Labs, Inc.*, 809 F. App'x 840, 843 (Fed. Cir. 2020) (finding that general statements that a person of ordinary skill in the art would have combined the prior art references to address the problem of occlusion effect in hearing aids was insufficient absent an explanation of why a person of ordinary skill in the art would have been “motivated to modify Brown, which already includes vents, to address occlusion effect”).⁶ Petitioner does not adequately explain why one of skill in the art would have substituted Lewis’ quarantine server for Gleichauf’s remediation server.

Due to the lack of a sufficient motivation to combine, Petitioner has not shown a reasonable likelihood of proving claim 1 unpatentable over the combination of Gleichauf, Ovadia, and Lewis. And, for the same reasons, Petitioner has not shown a reasonable likelihood of proving independent claims 10 and 17 or dependent claims 2–9, 11–16, and 18–20 unpatentable.

⁶ Petitioner also argues that one of skill in the art “would have had a reasonable expectation of success.” Pet. 22. That alone, however, would be insufficient to support the combination because we don’t reach the question of whether there would have been an expectation of success without their first being a reasoned motivation to make the combination, which, as explained above, Petitioner has not provided.

III. CONCLUSION

Petitioner has not established a reasonable likelihood of proving that claims 1–20 would have been unpatentable over the combination of Gleichauf, Ovadia, and Lewis.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that an *inter partes* review is not instituted in this proceeding.

IPR2022-00843
U.S. Patent No. 9,516,048

FOR PETITIONER:

Hersh Mehta
Davis Chin
BENESCH FRIEDLANDER COPLAN & ARONOFF LLP
hmehta@beneschlaw.com
dchin@beneschlaw.com

FOR PATENT OWNER:

David Schumann
Palani Rahinasamy
Moses Xie
Timothy Dewberry
FOLIO LAW GROUP PLLC
david.schumann@foliolaw.com
palani@foliolaw.com
moses.xie@foliolaw.com
timothy.dewberry@foliolaw.com