Trials@uspto.gov
571-272-7822

Paper 41
Date: September 19, 2022

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
FORESCOUT TECHNOLOGIES, INC., and
HEWLETT PACKARD ENTERPRISE COMPANY,
Petitioner,

v.

K.MIZRA LLC,
Patent Owner.

IPR2021-00593[1]
Patent 8,234,705 B1

Before MINN CHUNG, AARON W. MOORE, and IFTIKHAR AHMED, *Administrative Patent Judges*.

CHUNG, *Administrative Patent Judge*.

JUDGMENT
Final Written Decision
Determining No Challenged Claims Unpatentable
35 U.S.C. § 318(a)

[1] Forescout Technologies, Inc., which filed a petition in IPR2022-00081, and Hewlett Packard Enterprise Company, which filed a petition in IPR2022-00084, have been joined as a petitioner in this proceeding.

I. INTRODUCTION

In this *inter partes* review ("IPR"), Cisco Systems, Inc., Forescout Technologies, Inc., and Hewlett Packard Enterprise Company (collectively "Petitioner") challenge the patentability of claims 1–3, 5–13, and 15–19 (the "challenged claims") of U.S. Patent No. 8,234,705 B1 (Ex. 1001, "the '705 patent"), owned by K.Mizra LLC ("Patent Owner"). This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73. Based on the record before us, Petitioner has not shown, by a preponderance of the evidence, that claims 1–3, 5–13, and 15–19 of the '705 patent are unpatentable.

II. BACKGROUND

A. Procedural History

Cisco Systems, Inc. ("Cisco") filed a Petition (Paper 2, "Pet.") requesting an *inter partes* review of claims 1–3, 5–13, and 15–19 of the '705 patent. Patent Owner filed a Preliminary Response. Paper 8 ("Prelim. Resp.").

On September 24, 2021, applying the standard set forth in 35 U.S.C. § 314(a), which requires demonstration of a reasonable likelihood that a petitioner would prevail with respect to at least one challenged claim, we instituted an *inter partes* review of all challenged claims of the '705 patent based on the ground presented in the Petition. Paper 9 ("Inst. Dec."), 59.

After institution, Patent Owner filed a Patent Owner Response (Paper 23, "PO Resp."), Cisco filed a Reply to the Patent Owner Response (Paper 28, "Pet. Reply"), and Patent Owner filed a Sur-reply (Paper 34, "PO Sur-reply").

On October 22, 2021, Forescout Technologies, Inc. ("Forescout") filed a petition for *inter partes* review and a Motion for Joinder in IPR2022-00081, requesting that Forescout be joined as a petitioner in IPR2021-00593. *Forescout Technologies, Inc. v. K.Mizra LLC*, IPR2022-00081 ("'081 IPR"), Papers 1, 3 (PTAB Oct. 22, 2021). On the same day, Hewlett Packard Enterprise Company ("HPE") filed a petition for *inter partes* review and a Motion for Joinder in IPR2022-00084, requesting that HPE be joined as a petitioner in IPR2021-00593. *Hewlett Packard Enterprise Co. v. K.Mizra LLC*, IPR2022-00084 ("'084 IPR"), Papers 1, 3 (PTAB Oct. 22, 2021). Patent Owner did not file a Preliminary Response or an opposition to the Joinder Motions in '081 IPR and '084 IPR. Upon considering the information presented, we instituted trial in '081 IPR and '084 IPR, granted Forescout's and HPE's Motions for Joinder, and added each of Forescout and HPE as a petitioner to IPR2021-00593. '081 IPR, Paper 14; '084 IPR, Paper 10. A copy of each of these decisions was entered in this record. Papers 30, 31. These decisions were entered after Cisco filed the Reply, and no further substantive papers were filed by Cisco, Forescout, or HPE.

An oral hearing was held on June 16, 2022, and a copy of the hearing transcript has been entered into the record. Paper 39 ("Tr.").

B. Related Matters

According to the parties, the '705 patent has been asserted in *K.Mizra LLC v. Cisco Systems, Inc.*, No. 6:20-cv-01031 (W.D. Tex.); *K.Mizra LLC v. Forescout Technologies, Inc.*, No. 2:21-cv-00248 (E.D. Tex.); *K.Mizra LLC v. Hewlett Packard Enterprise Co.*, No. 2:21-cv-00305 (E.D. Tex.); and *K.Mizra LLC v. Fortinet*, No. 2:21-cv-00249 (E.D. Tex.). Pet. 7–8; Paper 3, 1; '081 IPR Papers 1, 5; '084 IPR, Papers 1, 5.

C. The '705 Patent

The '705 patent issued July 31, 2012 from U.S. Patent Application No. 11/237,003, filed September 27, 2005. Ex. 1001, codes (21), (22), (45).

The '705 patent describes contagion isolation and inoculation in a protected computer network. *Id.* at code (57). As background, the '705 patent describes as follows:

> Laptop and wireless computers and other mobile systems pose a threat to elements comprising and/or connected to a network service provider, enterprise, or other protected networks to which they reconnect after a period of connection to one or more networks and/or systems that are not part of the service provider, enterprise, or other protected network. By roaming to unknown domains, such as the Internet, and/or connecting to such domains through public, wireless, and/or otherwise less secure access nodes, such mobile systems may become infected by computer viruses, worms, backdoors, and/or countless other threats and/or exploits and/or have unauthorized software installed . . . and/or have configurations, settings, security data, and/or other data added, removed, and/or changed in unauthorized ways and/or by unauthorized person.

Id. at 1:14–31. The '705 patent describes that "[u]pon connecting to a protected network, a system may infect or otherwise harm resources associated with the protected network before measures can be taken to detect and prevent the spread of such infections or harm." *Id.* at 1:34–38. The '705 patent states that "[t]herefore, there is a need for a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network." *Id.* at 1:38–41.

Against this backdrop, the '705 patent describes embodiments to determine whether a host (e.g., a computer) should be quarantined when the host attempts to connect to a protected network. *Id.* at code (57). If the host

is required to be quarantined, the host is provided only limited access to the protected network. *Id.* According to the '705 patent, in some embodiments, a quarantined host is permitted to access the protected network only to the extent necessary to remedy a condition that caused the quarantine to be imposed "such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed." *Id.* For example, a quarantined host is allowed to access a remediation server (e.g., to "download a patch, more current threat definition, etc.") but all other access requests are redirected to a quarantine server. *Id.* at 12:3–9.

Figure 10B of the '705 patent is reproduced below.

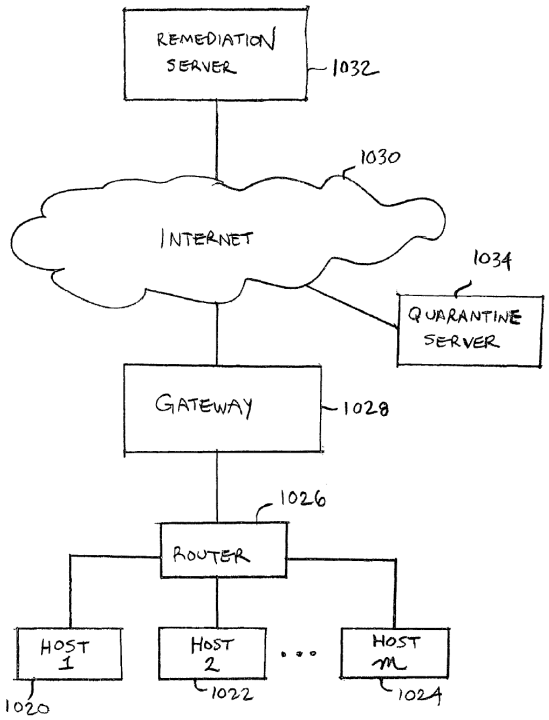


FIG. 10B

Figure 10B is a block diagram illustrating a network environment in which infected hosts and/or networks are quarantined. *Id.* at 2:14–16.

As shown in Figure 10B, hosts 1020 to 1024 connect via router 1026 and gateway 1028 to Internet 1030. *Id.* at 11:59–62. In an embodiment, 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 11:63–67. In the event of quarantine of one or more of hosts 1020–1024, a quarantined host is permitted to access remediation server 1032 to download a patch, more current threat definition, etc. *Id.* at 12:1–7. Requests to connect to a host other than remediation server 1032 are redirected to quarantine server 1034 configured to provide a notice and/or other information and/or instructions to a user of the quarantined host. *Id.* at 12:8–11.

Figure 13 of the '705 patent is reproduced below.

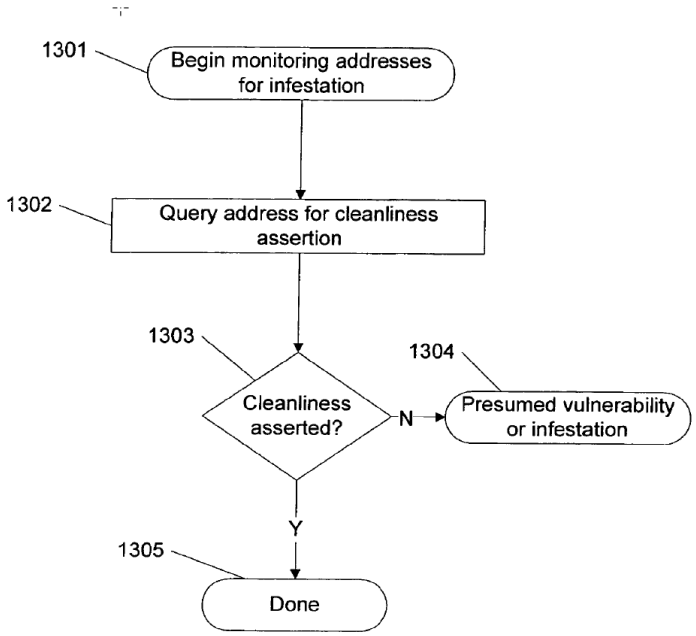


Figure 13

Figure 13 is a flow diagram of an exemplary method for monitoring one or more computers for infestation. *Id.* at 2:21–23.

In the example shown in Figure 13, monitoring of a computer for infestation begins (step 1301) by retrieving a list of one or more addresses of computers, such as addresses of participating subscribers. *Id.* at 13:56–59. In the next step (step 1302), a computer associated with an address identified in a list is queried for a cleanliness assertion, e.g., by contacting a trusted computing base within a computer, and requesting an authenticated infestation scan by trusted software. *Id.* at 13:64–14:1. According to the '705 patent, an example of a trusted computing base is described in various Trusted Computing Group ("TCG") specifications, such as the TCG Architecture Overview. *Id.* at 14:4–7. Trusted code bases may execute antivirus scans of the remainder of the computer, including untrusted portions of the disk and/or operating system. *Id.* at 14:7–10. In addition, trusted code bases may digitally sign assertions about the cleanliness (e.g., infestation status) and/or state of their computers. *Id.* at 14:10–12. In some embodiments, the query for cleanliness 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 14:12–16.

If a computer asserts it is clean (step 1303), then monitoring is complete (step 1305) in this example. *Id.* at 14:22–24. If, on the other hand, a cleanliness assertion is not provided (step 1303), then an infestation or vulnerability is presumed (step 1304). *Id.* at 14:24–25.

As discussed above, according to an embodiment of the '705 patent, a quarantined host is allowed to access a remediation server (e.g., to "download a patch, more current threat definition, etc.") but all other access requests are redirected to a quarantine server. *Id.* at 12:3–9. For example, a

device such as a router may forward outbound traffic from a quarantined computer to a quarantine server. *Id.* at 15:63–65.

If a received connection is a web server request, such as an HTTP request, then the server responds with a quarantine notification page. *Id.* at 15:66–16:2. An example of a quarantine notification page is a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain. *Id.* at 16:2–7. The links on the quarantine notification page may be examples of HTTP addresses that are for use in remediation. *Id.* at 16:8–9.

If the request is a DNS inquiry, the inquiry is tested to see if it is a DNS request for a remediation host name, i.e., the host name corresponding to the IP address of the remediation host. *Id.* at 16:16–23. If the DNS inquiry was not for a remediation host name, then an IP address for a quarantine server is provided as a redirected IP address. *Id.* at 16:28–32. If the DNS inquiry was for a remediation host name, then the access request is permitted by providing the actual IP address of the remediation server or allowing the access through a proxy service and/or an external DNS service. *Id.* at 16:23–28.

D. Illustrative Claim

Of the challenged claims, claims 1, 12, and 19 are independent. Claim 1 is illustrative of the challenged claims and is reproduced below with bracketing used by Petitioner.

1. A method for protecting a network, comprising:

[1.1] 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 [1.2] contacting a trusted computing base associated with a trusted platform module within the first host, [1.3] receiving a response, and [1.4] determining whether the response includes a valid digitally signed attestation of cleanliness, [1.5] wherein the valid digitally signed attestation of cleanliness includes at least one 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;

[1.6] 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 [1.7] receiving a service request sent by the first host, [1.8] serving a quarantine notification page to the first host when the service request comprises a web server request, [1.9] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

[1.10] permitting the first host to communicate with the remediation host.

Ex. 1001, 19:57–20:22.

E. Evidence

1. Applied References

Petitioner relies upon the following references in its challenge to patentability.

Reference	Date	Designation	Exhibit No.
U.S. Patent No. 9,436,820 B1	Filed Aug. 2, 2004	Gleichauf[2]	1005
U.S. Patent No. 7,747,862 B2	Filed June 28, 2004	Ovadia	1006
U.S. Patent No. 7,533,407 B2	Filed Apr. 14, 2004	Lewis	1007

2. Testimonial Evidence

Petitioner supports its challenge with a Declaration from A. L. Narasimha Reddy, Ph.D. Ex. 1003 ("Reddy Declaration"). Patent Owner relies on a Declaration of Nenad Medvidovic, Ph.D., to support its Response. Ex. 2009 ("Medvidovic Declaration").

Dr. Reddy and Dr. Medvidovic were cross-examined during trial, and transcripts of Dr. Reddy's deposition (Ex. 2012) and Dr. Medvidovic's deposition (Ex. 1024) are included in the record.

[2] For clarity and ease of reference, we only list the first named inventor.

F. Instituted Ground of Unpatentability

Petitioner asserts the following ground of unpatentability (Pet. 17).

Claim(s) Challenged	35 U.S.C. §	Reference(s)/Basis
1–3, 5–13, 15–19	103(a)[3]	Gleichauf, Ovadia, Lewis

III. ANALYSIS

A. Relevant Principles of Law

To prevail in challenging Patent Owner's claims, Petitioner must demonstrate by a preponderance of the evidence that the claims are unpatentable. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). "In an [*inter partes* review], the petitioner has the burden from the onset to show with particularity why the patent it challenges is unpatentable." *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (citing 35 U.S.C. § 312(a)(3) (requiring inter partes review petitions to identify "with particularity . . . the evidence that supports the grounds for the challenge to each claim")). This burden never shifts to Patent Owner. *See Dynamic Drinkware, LLC v. Nat'l Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1326–27 (Fed. Cir. 2008)) (discussing the burden of proof in *inter partes* review).

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

[3] The Leahy-Smith America Invents Act, Pub. L. No. 112-29, 125 Stat. 284 (2011), amended 35 U.S.C. § 103 effective March 16, 2013. Because the '705 patent has an effective filing date prior to the effective date of the applicable AIA amendment, we refer to the pre-AIA version of § 103.

made to a person having ordinary skill in the art to which the 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.[4] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

In addition, an invention "composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." *KSR*, 550 U.S. at 418. Rather, "it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *Id.* An obviousness determination "cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *Id.* (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)); *see In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

We analyze Petitioner's asserted ground based on obviousness with the principles identified above in mind.

B. Level of Ordinary Skill in the Art

We begin our analysis by addressing the level of ordinary skill in the art. Supported by the testimony of Dr. Reddy, Petitioner proposes that a

[4] The parties do not address secondary considerations, which therefore do not constitute part of our analysis.

person of ordinary skill in the art "would have had a bachelor's degree in computer science, computer engineering, electrical engineering, or an equivalent training, and approximately two years of professional experience in the field of network communications, and more specifically, network security." Pet. 10 (citing Ex. 1003 ¶ 18). Petitioner asserts that "[l]ack of professional experience can be remedied by additional education, and vice versa." *Id.* (citing Ex. 1003 ¶ 18).

Patent Owner does not dispute Petitioner's articulation of the level of ordinary skill in the art. *See generally* PO Resp. Dr. Medvidovic, Patent Owner's declarant, states that "[f]or the purposes of the subject IPR proceedings," he "employ[s]" the level of ordinary skill in the art articulated by Dr. Reddy. Ex. 2009 ¶ 26.

Based on the complete record, for purposes of this Decision, we adopt Petitioner's unopposed position as to the level of ordinary skill in the art at the time of the claimed invention because Petitioner's proposal is consistent with the level of ordinary skill in the art reflected by the prior art of record. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001).

C. Claim Construction

In an *inter partes* review, we apply the same claim construction standard that would be used in a civil action under 35 U.S.C. § 282(b), following the standard articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). 37 C.F.R. § 42.100(b) (2020). In applying such standard, claim terms are generally given their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art, at the time of the invention and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13. "In determining the meaning of the disputed

claim limitation, we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence." *DePuy Spine, Inc. v. Medtronic Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).

The parties discuss two claim terms recited in independent claims—"trusted computing base" and "trusted platform module." Pet. 11–16; PO Resp. 5–6. Petitioner contends the term "trusted computing base" should be construed to mean "a piece of hardware or software that has been designed to be part of a mechanism that provides security to a computer system" based on the statement made by the applicant during prosecution. Pet. 12–13 (emphasis omitted). Patent Owner does not dispute Petitioner's proposed construction of this claim term. PO Resp. 5.

The parties dispute construction of "trusted platform module" (Pet. 13–16; PO Resp. 5–6) but do not identify any issue that would turn on the construction of this term. *See generally* Pet.; PO Resp.

Based on the complete record, for purposes of this Decision, we determine no claim terms require express construction. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (holding that only terms that are in controversy need to be construed, and "only to the extent necessary to resolve the controversy"); *see also Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (applying *Vivid Techs.* in the context of an *inter partes* review).

D. Obviousness over Gleichauf, Ovadia, and Lewis

Petitioner contends that claims 1–3, 5–13, and 15–19 are unpatentable under § 103(a) over the combination of Gleichauf, Ovadia, and Lewis.

Pet. 18–67. Patent Owner disputes Petitioner's contentions. PO Resp. 1–3, 8–29; PO Sur-reply 1–16. For the reasons discussed below, we determine Petitioner does not show, by a preponderance of the evidence, the subject matter of claims 1–3, 5–13, and 15–19 would have been obvious over the combination of Gleichauf, Ovadia, and Lewis because Petitioner does not explain sufficiently why a person of ordinary skill in the art would have been motivated to combine Gleichauf, Ovadia, and Lewis in the manner proposed by Petitioner to arrive at the subject matter recited in the claims. Our analysis below focuses on the deficiencies in Petitioner's proffered reasons to combine Gleichauf 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.

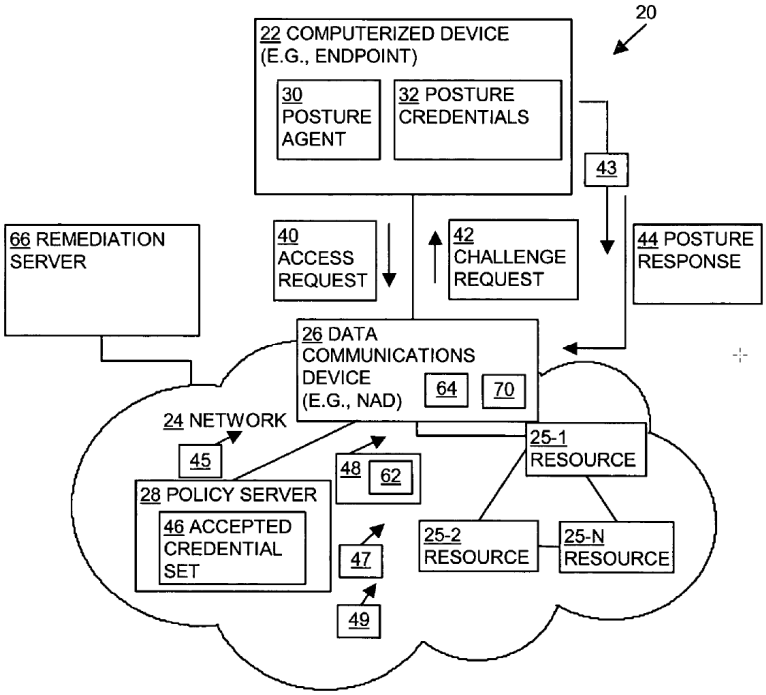


Figure 1 illustrates an exemplary data communication system. *Id.* at 8:32–33.

As shown in Figure 1, data communication system 20 includes user device 22 and network 24, which includes network resources 25, data communications device 26, and policy server 28. *Id.* at 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. *Id.* at 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 installed 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 an exemplary operation of an 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. *Id.* at 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. *Id.* at 4:15–19. Devices that are compliant with 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. 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. *Id.* at 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.

In an embodiment, the notification message may contain text messages for display to a user, including any remediation actions to be performed. *Id.* at 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. *Id.* at 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 Ovadia (Ex. 1006)

Ovadia describes methods and apparatuses to authenticate base and subscriber stations and maintaining secure sessions for broadband wireless networks. Ex. 1006, code (57), 3:62–64.

In an embodiment, Ovadia describes that 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. *Id.* at 4:16–21. Ovadia further describes that a TCG token comprising a trusted platform module (TPM) is employed. *Id.* at 4:22–24. According to Ovadia, TCG is a standards organization and an industry consortium concerned with platform and network security. *Id.* at 4:17–21, 4:31–32. Ovadia 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.

Ovadia further describes that the TCG main specification defines a trusted platform sub system that employs cryptographic methods when establishing trust. *Id.* at 4:36–38. According to Ovadia, 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. *Id.* at 4:46–48. Figure 2 of Ovadia is reproduced below.

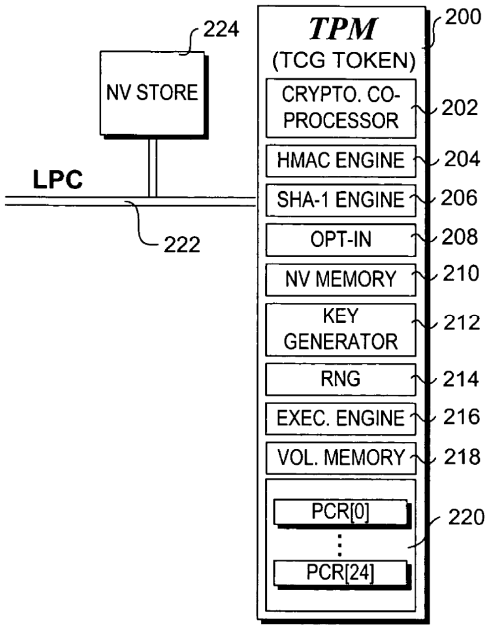


Figure 2 is a schematic diagram of a trusted platform module. *Id.* at 3:7–8.

Referencing Figure 2, Ovadia describes TPM's security functions, including security key generation, encryption, and hashing operations. *Id.* at 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. *Id.* at 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.

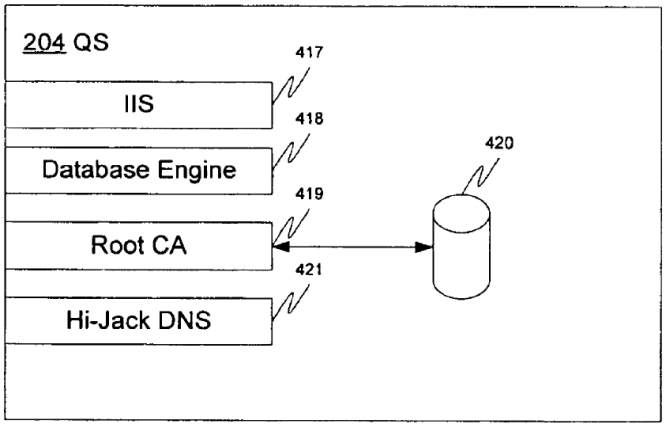


Figure 4 illustrates a quarantine server of Lewis. *Id.* at 4:52–53.

As shown in Figure 4, quarantine server (QS) 201[5] comprises Internet Information Server (IIS) 417 for proving a default web page, database engine 418, and hijack DNS component 421. *Id.* at 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

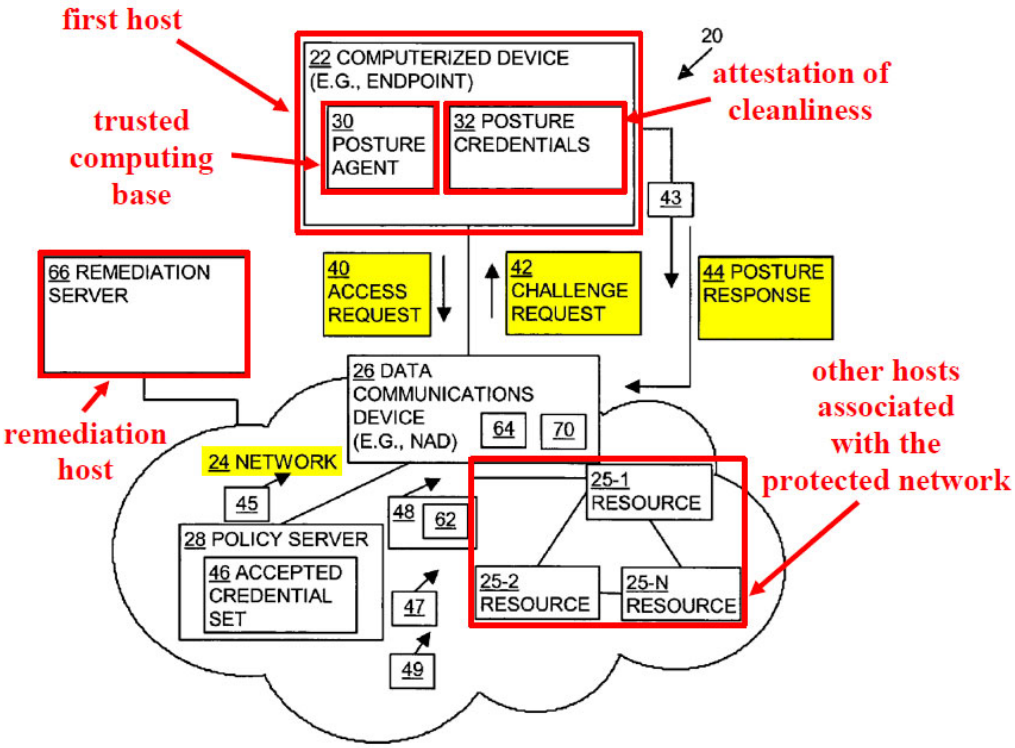
[5] Although Figure 4 shows a quarantine server as QS 204, Lewis refers to the quarantine server as QS 201 in the textual description relating to Figure 4. *See* Ex. 1007, 10:61–11:17.

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. Independent Claim 1

Petitioner contends that the combination of Gleichauf, Ovadia, and Lewis teaches each of the recitations of claim 1. Pet. 29–54. In its proposed combination of Gleichauf, Ovadia, and Lewis, Petitioner relies on Gleichauf to teach most of the recitations of claim 1, except for (1) the limitations reciting "trusted platform module," for which Petitioner further relies on Ovadia, and (2) the limitations relating to the operation of the recited "quarantine server," for which Petitioner further relies on Lewis. *See id.* at 29–54. 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. *Id.* at 21–29.

Figure 1 of Gleichauf, as annotated by Petitioner, is reproduced below.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶ 142.

Pet. 50. Annotated Figure 1 above shows Petitioner's identification of the recited "first host," "trusted computing base," "remediation host," "protected network," and "one or more other hosts associated with the protected network" allegedly present in Gleichauf.

As indicated in Annotated Figure 1 above, in addressing the recitations of claim 1, Petitioner draws a correspondence between (1) the recited "first host" and Gleichauf's computerized device 22; (2) the recited "trusted computing base" and Gleichauf's posture agent 30; (3) the recited "remediation host" and Gleichauf's remediation server 66; (4) the recited "protected network" and Gleichauf's network 24 (*see* Pet. 30 (Petitioner identifies highlighted access request 40 and network 24 in Figure 1 as the

recited "attempt[] to connect to a protected network")); and (5) the recited "one or more other hosts associated with the protected network" and Gleichauf's network resources 25. In making these correspondences or mappings, Petitioner relies generally on Gleichauf's described functionality of detecting an access request by a computer device, initiating a challenge-response sequence by sending a challenge request to the computer device, the computer device's posture agent retrieving its posture credentials and transmitting a challenge response back, quarantining the computer device if the posture credentials do not indicate network policy compliance, and remediating the quarantined computer via communication with a remediation server. *Id.* at 29–33, 38–47, 50, 54.

Petitioner relies on Ovadia for its disclosure of "trusted platform module" described in the Trusted Computing Group's Trusted Platform Module Main Specification to teach the limitations reciting "trusted platform module." Pet. 33–35. Petitioner further relies on Lewis for its teachings regarding a quarantine server and the operation of the quarantine server to quarantine web requests and web traffic from the quarantined computer device. *Id.* at 47–53.

Claim 1 recites [1.1] "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," [1.2] "contacting a trusted computing base associated with a trusted platform module within the first host," [1.3] "receiving a response," and [1.4] "determining whether the response includes a valid digitally signed attestation of cleanliness." Ex. 1001, 19:58–65. Petitioner labels these recitations as limitations [1.1], [1.2], [1.3], and [1.4], as indicated in brackets above. Pet. 29, 32, 38, 39.

As discussed above, Petitioner maps the recited "first host" to Gleichauf's computerized device 22 and the recited "protected network" to Gleichauf's network 24. Pet. 30 (citing Ex. 1005, Fig. 1). Petitioner contends that Gleichauf teaches these limitations because Gleichauf describes a challenge-response sequence initiated by data communications device 26 when computerized device 22 (the claimed "first host") transmits an access request to the data communications device in an attempt to access the network resources within network 24 (i.e., "attempting to connect to a protected network," as claimed). *Id.* at 30–31 (citing Ex. 1005, 3:36–45, 3:50–56, 8:1–4; 11:29–32; 14:16–34; Ex. 1003 ¶ 77). Petitioner further asserts that Gleichauf teaches "detecting an insecure condition on a first host," as recited in claim 1, because in the challenge-response sequence the computerized device responds with its posture credentials, which the policy server analyzes to determine compliance with network admission policy. *Id.* at 31–32 (citing Ex. 1005, 1:10–14, 1:65–2:3, 3:36–45, 8:52–56, 8:65–9:1, 11:58–12:13, 14:16–34; 22:38–59, 31:1–7; Ex. 1003 ¶¶ 78–79, 81).

Claim 1 further recites

> [1.6] 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
>
> > [1.7] receiving a service request sent by the first host, [1.8] serving a quarantine notification page to the first host when the service request comprises a web server request, [1.9] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page

> if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition.

Ex. 1001, 20:5–22. Petitioner labels these recitations as limitations [1.6], [1.7], [1.8], and [1.9], as indicated in brackets above. Pet. 44, 46, 47, 49. Petitioner contends that Gleichauf teaches limitations [1.6] and [1.7] and that the combination of Gleichauf and Lewis teaches limitations [1.8] and [1.9]. *Id.* at 44–54.

Regarding limitation [1.6], "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," Petitioner contends that Gleichauf teaches this limitation because Gleichauf's policy server reviews and validates the digitally signed posture credentials from a device and if the device is found to be out of compliance with a network admission policy, places the device in quarantine. Pet. 44–45 (citing Ex. 1005, 4:24–27, 4:50–56, 7:3–8, 10:30–33, 11:45–60, 22:38–42; Ex. 1003 ¶¶ 119–122). Petitioner further argues that, in Gleichauf, placement 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." *Id.* at 45 (citing Ex. 1005, 11:58–67; Ex. 1003 ¶ 123).

Addressing limitation [1.7], Petitioner asserts that Gleichauf teaches "receiving a service request sent by the first host," as recited in claim 1, because Gleichauf describes how the computerized device transmits an "access request" or "signaling request" in an "attempt to access the network

resources within the network." Pet. 46 (citing Ex. 1005, 3:50–56, 8:1–4; Ex. 1003 ¶¶ 126–127). Petitioner argues that such a request to access network resources, which can occur even after the device has been placed in quarantine, is the recited "service request." *Id.* at 46–47 (citing Ex. 1005, 3:60–65, 13:52–65; Ex. 1003 ¶¶ 128–130).

Turning next to limitation [1.8], "serving a quarantine notification page to the first host when the service request comprises a web server request," Petitioner contends that Gleichauf teaches that "the service request comprises a web server request" because Gleichauf discloses "URL Redirect" and redirecting HTTP traffic from the user device to a remediation server. Pet. 47 (citing Ex. 1005, 15:45, 15:55–67). Citing the testimony of Dr. Reddy, Petitioner asserts that a person of ordinary skill in the art would have known that "HTTP traffic includes a *web server request* because hyper-text transfer protocol (HTTP) is the protocol used for communications between web browsers and web servers." *Id.* (citing Ex. 1003 ¶ 133). Petitioner further argues that a person of ordinary skill in the art would have been familiar with URL redirection as "a common technique used to forcibly provide an alternative response to a client's request for a webpage." *Id.* at 47–48 (citing Ex. 1015 ¶ 3; Ex. 1003 ¶ 134). Petitioner and Dr. Reddy cite a published U.S. patent application—U.S. Patent Application Publication 2005/0078668 A1 (Ex. 1015)—as evidence of how a person of ordinary skill in the art would have known URL redirection involves a request for a webpage. *Id.*; Ex. 1003 ¶ 134.

To teach "serving a quarantine notification page," Petitioner relies on the combination of Gleichauf's teaching of "notification messages" displayed to the user indicating that the device has been quarantined and

Lewis's teaching of a quarantine server providing a default webpage when a user opens a web browser from a client device that has been quarantined. Pet. 48 (citing Ex. 1005, 4:56–63, 21:1–12; Ex. 1007, 4:24–31, 13:7–12; Ex. 1003 ¶¶ 135–136). In the proposed combination, Petitioner further relies on Gleichauf's teaching of redirecting HTTP traffic from a quarantined device to a remediation server. *Id.* at 50 (explaining that in Gleichauf, "HTTP traffic from the [quarantined] device directed to the remediation server is permitted while HTTP traffic directed to other destinations is redirected [to the remediation server]" (citing Ex. 1005, 14:62–66, 15:55–67)). Petitioner asserts that "[i]n the combination, HTTP traffic from a quarantined device would be redirected to a quarantine server as taught by Lewis" and that "[t]he quarantine server would then serve a webpage to the user, as taught by Lewis." *Id.* at 49 (citing Ex. 1003 ¶ 137). In other words, in the proposed combination of Gleichauf and Lewis, Gleichauf would be modified such that HTTP traffic from a quarantined device would not be redirected to a remediation server but instead would be redirected to a quarantine server, which serves an informational webpage to the user of the device, as taught by Lewis. *Id.* at 48–49; Pet. Reply 14 (citing Ex. 1005, 4:56–63, 21:1–12; Ex. 1007, 4:24–31, 13:7–15; Pet. 48).

Addressing next limitation [1.9], "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition," Petitioner asserts that the combination of Gleichauf and Lewis teaches this limitation. Pet. 49–54.

In the proposed combination, Petitioner relies on Gleichauf's disclosure discussed above that "HTTP traffic from the [quarantined] device directed to the remediation server is permitted while HTTP traffic directed to other destinations is redirected [to the remediation server]" as teaching "serv[ing] the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host." Pet. 50 (citing Ex. 1005, 14:62–66, 15:55–67; Ex. 1003 ¶¶ 143–144). Petitioner further contends that Lewis teaches "providing in response an IP address of a quarantine server configured to serve the quarantine notification page" because Lewis describes the operation of "hijack DNS component 421 for intercepting DNS queries from quarantined clients" such that "[w]henever the client performs name resolution on any address, it will receive the IP [address] of QS [quarantine server]." *Id.* at 51 (citing Ex. 1007, 11:15–17, 14:22–23; Ex. 1003 ¶ 146). Petitioner argues that because Gleichauf describes that HTTP traffic from the [quarantined] device directed to the remediation server is permitted while HTTP traffic directed to other destinations, i.e., when the DNS query is not associated with a remediation host, is redirected (*id.* at 50), the combination of Gleichauf and Lewis teaches or suggests "responding to a DNS query with the IP address of a quarantine server if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition." *Id.* at 52–53 (emphasis omitted) (citing Ex. 1003 ¶ 148).

Addressing the motivation to combine, Petitioner presents several reasons why a person of ordinary skill in the art would have combined

Gleichauf and Lewis as proposed.[6] Pet. 26–29. Patent Owner asserts that a person of ordinary skill in the art would not have been motivated to modify Gleichauf to redirect traffic away from Gleichauf's remediation server to Lewis's quarantine server. PO Resp. 15–17. Patent Owner further argues that, although Petitioner discusses the benefits of a quarantine notification page generally, "Petitioner never explained why a quarantine notification page *hosted on a separate 'quarantine server'* . . . should be used to notify users of the need for remediation" when Gleichauf itself already provides the alleged benefits of the proposed combination. PO Sur-reply 9; *see also* Tr. 29:21–31:16 (Patent Owner argues Petitioner fails to explain why a person of ordinary skill in the art would have looked to Lewis to modify Gleichauf to implement a separate quarantine server). We agree with Patent Owner's argument. For the reasons explained below, we find that Petitioner does not explain sufficiently why a person of ordinary skill in the art would have looked to Lewis to modify Gleichauf, as proposed, when Gleichauf provides all of the Petitioner-identified benefits or advantages of the proposed combination of Gleichauf and Lewis.

---

[6] As discussed above, Petitioner relies on the combination of Gleichauf and Ovadia as teaching the limitations reciting "trusted platform module," whereas Petitioner relies on the combination of Gleichauf and Lewis as teaching the limitations relating to the operation of the recited "quarantine server." *See* Pet. 29–54. Because the subject matter of these two groups of limitations are relatively disjoint, Petitioner's proffered reasons to combine Gleichauf and Ovadia are largely unrelated to the reasons to combine Gleichauf and Lewis. *Compare* Pet. 21–26, *with id.* at 26–29. Thus, for limitations [1.8] and [1.9], for which Petitioner relies on the combination of Gleichauf and Lewis, we focus on Petitioner's proffered reasons to combine Gleichauf and Lewis.

First, Petitioner asserts that "[a person of ordinary skill in the art] 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. 27 (emphasis added) (citing Ex. 1007, 10:61–66, 13:63–14:1; Ex. 1003 ¶ 68).

As Petitioner acknowledges, however, Gleichauf itself already provides this benefit without the need for Lewis's quarantine server. For example, when addressing limitation [1.8], Petitioner acknowledges that Gleichauf discloses "notification messages" displayed to the user indicating that the device has been quarantined. Pet. 48 ("Gleichauf describes providing 'one or more *notification messages*' for display to a user 'indicating that the device has been quarantined.'" (emphasis added) (citing Ex. 1005, 4:56–63, 21:1–12)). In the cited portion of Gleichauf, Gleichauf describes that

> [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*). For 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 (emphases added). Petitioner also concedes, when addressing limitation [1.6], Gleichauf discloses that 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. 45 (citing Ex. 1005, 11:58–67; Ex. 1003

¶ 123). Thus, Petitioner admits that Gleichauf alone, without the need for 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." *See id.* at 27, 45, 48.

Next, Petitioner asserts, citing the testimony of its declarant, Dr. Reddy, 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. 27–28 (emphasis added) (citing Ex. 1005, 4:56–60; Ex. 1006, 16:62–65; Ex. 1003 ¶ 68); *see also id.* at 48 (citing Ex. 1005, 4:56–63, 21:1–12).

Gleichauf's notification messages, however, provide the same benefit without the need for Lewis's quarantine webpage 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). Thus, Gleichauf indicates that the notification messages may be displayed on a browser using XML pages, without the need for additional software running on the device to receive and display the notification message to the user. *See also* Tr. 43:7–15 (Patent Owner argues that even if Gleichauf only teaches "messages," a person of ordinary skill in the art could implement a webpage as part of the notification). Neither Petitioner nor Dr. Reddy addresses this disclosure in

Gleichauf or explains 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.

Petitioner next asserts 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 that does not have the time to remediate security issues (e.g., a user attempting access from an airport terminal)," the user "may opt to terminate the connection attempt." Pet. 28 (citing Ex. 1003 ¶ 69). Petitioner contends that "[a person of ordinary skill in the art] would have understood the benefits of giving the user the option to choose their desired course of action." *Id.* (citing Ex. 1003 ¶ 69). During the oral hearing, Petitioner elaborated on this rationale in a question and answer exchange with the panel as follows.

> JUDGE AHMED: Counsel, let me follow up on that. I know you said the patent owner raised this argument in the surreply, but I'm still having a little bit of difficulty following the need for a separate quarantine server when the remediation server itself could have hosted the quarantine webpage, right?
>
> Can you point me to what petitioner's basis is for that, why a person of skill in the art would be motivated to separate this functionality out on a separate server?
>
> MR. GORYUNOV:
>
> . . .
>
> The combination of Gleichauf with Lewis would then redirect the HTTP request from the web server to this quarantine webpage hosted by a quarantine server, which would provide all this information to the user, remind them that the device is in quarantine, remind them of what remedial actions must be taken,

> and provide *a link to the remediation server* that *they can click on* and remediate.
>
> This goes to one of the reasons, Your Honor, for the -- *reason for the combination*, *to give the user a choice*. If I may, K. Mizra says if you're at the remediation server, you expect your device to be remediated every single time. Well, if a user is in the airport and, you know, I have ten minutes before I'm boarding my flight, I may not have time to download the latest Windows patch which can be multiple hundreds of megabytes and you need time to install that.
>
> So I have the option at that point of terminating the connection and resuming it at a later time.

Tr. 17:1–18:11 (emphases added). In other words, according to Petitioner, one of the benefits of the proposed combination of Gleichauf and Lewis is giving the user a choice or option of remediating now or later.

Petitioner, however, concedes that Gleichauf alone provides the same benefit because Petitioner acknowledges that Gleichauf "gives the user a choice: remediate now or later." Pet. Reply 15 (citing Ex. 1005, 23:65–24:2 as disclosing "a user 'may' click on a link to a remediation server"). In the cited portion, 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, without the need for Lewis's quarantine server, 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.

Therefore, we find that Gleichauf alone provides all of the alleged benefits or advantages of the proposed combination of Gleichauf and Lewis identified by Petitioner.

As discussed above, in the proposed combination of Gleichauf and Lewis, Gleichauf would be modified such that HTTP traffic from a quarantined device would not be redirected to a remediation server but instead would be redirected to a quarantine server, which serves an informational webpage to the user of the device, as taught by Lewis. Pet. 48–49; Pet. Reply 14 (citing Ex. 1005, 4:56–63, 21:1–12; Ex. 1007, 4:24–31, 13:7–15; Pet. 48). Thus, Petitioner's proposed combination contemplates (1) modifying Gleichauf's network by adding a separate quarantine server, (2) modifying Gleichauf's policy server to not redirect HTTP traffic from a quarantined device to a remediation server and to instead redirect the HTTP traffic to the quarantine server, and (3) providing a quarantine notice webpage to the user from the quarantine server, including a link to the remediation server, which the user can click on to access the remediation server. In addition, Gleichauf's policy server would also need to be modified to not provide the notification messages to the user for HTTP traffic to avoid having both the policy server and the quarantine server provide the same or similar information displays to the user.

Neither Petitioner nor Dr. Reddy explains adequately why a person of ordinary skill in the art would have been motivated to look to Lewis to introduce such significant changes to the architecture or design of Gleichauf's network when Gleichauf alone already provides all of the alleged benefits or advantages of the proposed combination identified by Petitioner. *See* Pet. 26–29; Pet. Reply 14–16; Ex. 1003 ¶¶ 66–71. Thus, based on the complete record, we find that the alleged benefits or advantages of the proposed combination identified by Petitioner do not provide sufficient basis for establishing why a person of ordinary skill in the art

would have been motivated to combine Gleichauf and Lewis in the manner proposed by Petitioner. *See In re Anova Hearing Labs, Inc.*, 809 F. App'x 840, 843 (Fed. Cir. 2020) (finding that the Board's 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 when the Board does not explain why a person of ordinary skill in the art would have been "motivated to modify Brown, which already includes vents, to address occlusion effect") (non-precedential); *cf. Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1369 (Fed. Cir. 2012) ("Because each device independently operates effectively, a person having ordinary skill in the art, who was merely seeking to create a better device to drain fluids from a wound, would have no reason to combine the features of both devices into a single device.").

Dr. Reddy additionally testifies that "URL redirection is a well-known concept in HTTP traffic" (Ex. 1003 ¶ 24) and that "[a person of ordinary skill in the art] would have been familiar with URL redirection, which was a common technique used to forcibly provide an alternative response to a client's request for a web page" (*id.* at ¶ 134). During the oral hearing, Petitioner also stated, citing the Reddy Declaration, that "it was well known to redirect traffic to a separate server." Tr. 17:8–12 (citing Ex. 1003 ¶ 134).

This, however, does not provide a sufficient explanation why a person of ordinary skill in the art would have been motivated to combine Gleichauf and Lewis. This rationale and all of the other reasons for the proposed combination proffered by Petitioner establish, at most, that Gleichauf and Lewis *could* have been combined to meet limitations [1.8] and [1.9], rather than a person of ordinary skill in the art *would have been* motivated to make

the proposed combination. This is insufficient. *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)). We find, therefore, that Petitioner does not provide a sufficient reasoning to support obviousness of claim 1 based on the proposed combination.[7] *See Kinetic Concepts*, 688 F.3d at 1366–67 (holding that "some kind of motivation must be shown from some source, so that the [trier of fact] can understand why a person of ordinary skill would have thought of either combining two or more references or modifying one to achieve the patented [invention]")); *InTouch Techs.*, 751 F.3d at 1348–49 (Fed. Cir. 2014) ("[The expert witness's] testimony was nothing more than impermissible hindsight; she opined that all of the elements of the claims disparately existed in the prior art, but failed to provide the glue to combine these references.").

Accordingly, based on the complete record, we determine that Petitioner does not demonstrate, by a preponderance of the evidence, that the

[7] We note that Gleichauf alone or the combination of Gleichauf and Ovadia does not render claim 1 obvious because Gleichauf alone or the combination of Gleichauf and Ovadia does not satisfy the limitation "providing . . . an IP address of a quarantine server configured to serve the quarantine notification page," as recited in limitation [1.9]. Thus, to show obviousness of claim 1 over the combination of Gleichauf, Ovadia, and Lewis, Petitioner must identify "some articulated reasoning with some rational underpinning" why a person of ordinary skill in the art would have combined Gleichauf and Lewis to arrive at the subject matter recited in limitations [1.8] and [1.9]. *See KSR*, 550 U.S. at 418.

subject matter of claim 1 would have been obvious over the combination of Gleichauf, Ovadia, and Lewis.

5. Independent Claims 12 and 19

For independent claims 12 and 19, Petitioner asserts that all of the steps or functions recited in the claims are "substantively identical to the steps of claim 1 and are rendered obvious for the same reasons." Pet. 65, 67. For claims 12 and 19, Petitioner does not provide any additional reasons why a person of ordinary skill in the art would have been motivated to combine Gleichauf and Lewis beyond those discussed above with respect to claim 1. *See* Pet. 65–67. Therefore, for the same reasons discussed above with respect to claim 1, we find Petitioner does not provide a sufficient reasoning to support obviousness of claims 12 and 19 based on the proposed combination of Gleichauf, Ovadia, and Lewis.

Accordingly, based on the complete record, we determine that Petitioner does not demonstrate, by a preponderance of the evidence, that the subject matter of claims 12 and 19 would have been obvious over the combination of Gleichauf, Ovadia, and Lewis.

6. Dependent Claims 2, 3, 5–11, 13, and 15–18

Claims 2, 3, 5–11, 13, and 15–18 depend directly or indirectly from claims 1 or 12. Petitioner's arguments and evidence presented with respect to these dependent claims do not remedy the deficiencies in Petitioner's analysis of independent claim 1 discussed above. Therefore, for the same reasons discussed above with respect to claim 1, Petitioner has not shown by a preponderance of the evidence that claims 2, 3, 5–11, 13, and 15–18 are

unpatentable under 35 U.S.C. § 103(a) over the combination of Gleichauf, Ovadia, and Lewis.

IV. CONCLUSION

The table below summarizes our conclusions as to the challenged claims.

Claims	35 U.S.C. §	References/Basis	Claims Shown Unpatentable	Claims Not Shown Unpatentable
1–3, 5–13, 15–19	103(a)	Gleichauf, Ovadia, Lewis		1–3, 5–13, 15–19

V. ORDER

In consideration of the foregoing, it is

ORDERED that claims 1–3, 5–13, and 15–19 of U.S. Patent No. 8,234,705 B1 have not been shown, by a preponderance of the evidence, to be unpatentable; and

FURTHER ORDERED that, because this is a Final Written Decision, a party to the proceeding seeking judicial review of the Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

For PETITIONER:

Theodore M. Foster
David L. McCombs
Eugene Goryunov
Gregory P. Huh
HAYNES AND BOONE LLP
ipr.theo.foster@haynesboone.com
david.mccombs.ipr@haynesboone.com
eugene.goryunov.ipr@haynesboone.com
gregory.huh.ipr@haynesboone.com

Louis Campbell
Matthew McCullough
Kimball Anderson
WINSTON & STRAWN LLP
llcampbell@winston.com
mrmccullough@winston.com
kanderson@winston.com

Manish Mehta
Davis Chin
Kal K. Shah
Samuel Ruggio
BENESCH FRIEDLANDER COPLAN & ARONOFF LLP
mmehta@beneschlaw.com
dchin@beneschlaw.com
kshah@beneschlaw.com
sruggio@beneschlaw.com

For PATENT OWNER:

Sang Hui Kim
David Schumann
Palani Rathinasamy
Moses Xie
Cliff Win
FOLIO LAW GROUP PLLC
michael.kim@foliolaw.com
david.schumann@foliolaw.com
palani@foliolaw.com
moses.xie@foliolaw.com
cliff.win@foliolaw.com