Trials@uspto.gov
571-272-7822

Paper 9
Date: September 24, 2021

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CISCO SYSTEMS, INC.,
Petitioner,

v.

K.MIZRA LLC,
Patent Owner.

IPR2021-00593
Patent 8,234,705 B1

Before MINN CHUNG, STACY B. MARGOLIES, and IFTIKHAR AHMED, *Administrative Patent Judges*.

CHUNG, *Administrative Patent Judge*.

DECISION
Granting Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

Cisco Systems, Inc. ("Petitioner") filed a Petition (Paper 2, "Pet.") requesting an *inter partes* review 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"). K.Mizra LLC ("Patent Owner") filed a Preliminary Response. Paper 8 ("Prelim. Resp.").

Institution of an *inter partes* review is authorized by statute when "the information presented in the petition . . . and any response . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." 35 U.S.C. § 314(a); *see* 37 C.F.R. § 42.4. For the reasons described below, we determine that the information presented in the Petition establishes that there is a reasonable likelihood that Petitioner would prevail in showing the unpatentability of all the challenged claims. Accordingly, we institute an *inter partes* review of all challenged claims of the '705 patent, based on the ground raised in the Petition.

II. BACKGROUND

A. 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.) ("the underlying litigation"). Pet. 7–8; Paper 3, 1.

B. 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.

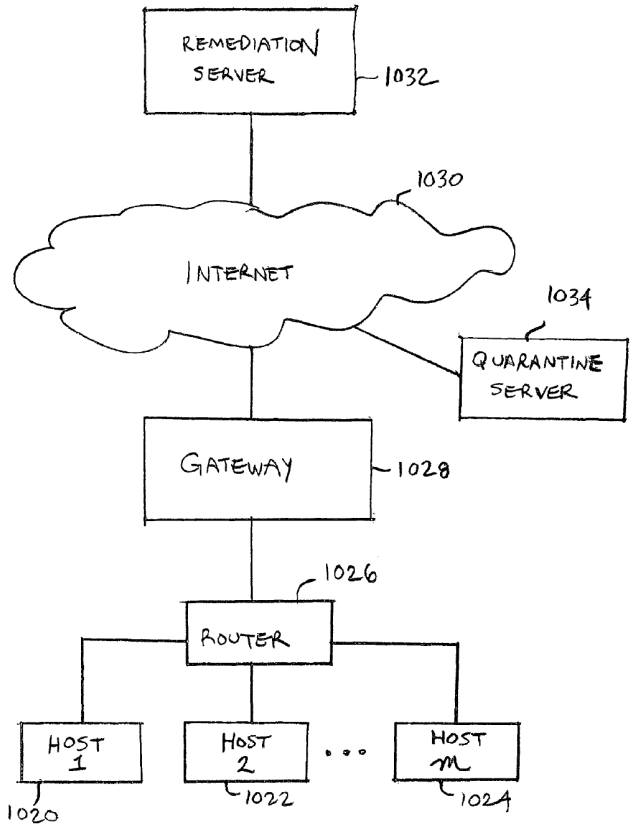


FIG. 10B

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.

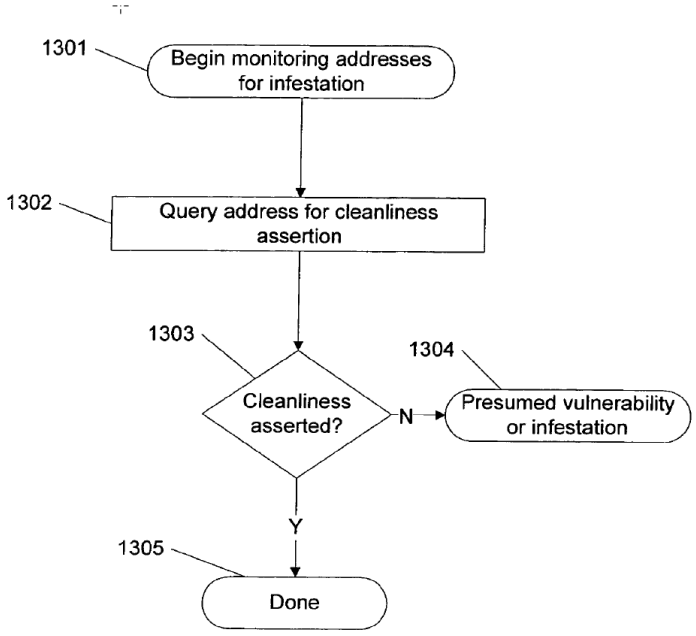


Figure 13

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.

C. 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.

D. Asserted 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)[1]	Gleichauf,[2] Ovadia,[3] Lewis[4]

Petitioner supports its challenge with a declaration from A. L. Narasimha Reddy, Ph.D. (Ex. 1003, "Reddy Declaration").

III. ANALYSIS

A. Discretion Under 35 U.S.C. § 314(a)

In the Preliminary Response, Patent Owner contends that we should exercise our discretion to deny institution under 35 U.S.C. § 314(a) "because the issues presented will long be decided before the Board has an opportunity to provide a final written decision." Prelim. Resp. 4–5 (citing *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, 2–3 (PTAB Mar. 20, 2020) (precedential) ("*Fintiv*"); *Cisco Sys., Inc. v. Oyster Optics, LLC*, IPR2021-00238, Paper 10, 10–17 (PTAB June 1, 2021)); *see id.* at 10–15. Petitioner contends the *Fintiv* factors favor institution. *See* Pet. 69–73.

---

[1] 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.

[2] U.S. Patent No. 9,436,820 B1, filed Aug. 2, 2004, issued Sept. 6, 2016 (Ex. 1005, "Gleichauf").

[3] U.S. Patent No. 7,747,862 B2, filed June 28, 2004, issued June 29, 2010 (Ex. 1006, "Ovadia").

[4] U.S. Patent No. 7,533,407 B2, filed Apr. 14, 2004, issued May 12, 2009 (Ex. 1007, "Lewis").

Based on the arguments presented in the Petition, the Preliminary Response, and the evidence of record, we decline to exercise our discretion to deny institution under § 314(a) for the following reasons.

Under 35 U.S.C. § 314(a), the Director has discretion to deny institution. In determining whether to exercise that discretion on behalf of the Director, we are guided by the Board's precedential decision in *NHK Spring Co. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 (PTAB Sept. 12, 2018) (precedential) ("*NHK*").

In *NHK*, the Board found that the "advanced state of the district court proceeding" was a "factor that weighs in favor of denying" the petition under § 314(a). *NHK*, Paper 8 at 20. The Board determined that "[i]nstitution of an *inter partes* review under these circumstances would not be consistent with 'an objective of the AIA . . . to provide an effective and efficient alternative to district court litigation.'" *Id.* (citing *Gen. Plastic Indus. Co. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 16–17 (PTAB Sept. 6, 2017) (precedential as to § II.B.4.i)).

"[T]he Board's cases addressing earlier trial dates as a basis for denial under *NHK* have sought to balance considerations such as system efficiency, fairness, and patent quality." *Fintiv*, Paper 11 at 5 (collecting cases). *Fintiv* sets forth six non-exclusive factors for determining "whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding." *Id.* at 6. These factors consider:

> 1. whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted;
>
> 2. proximity of the court's trial date to the Board's projected statutory deadline for a final written decision;

> 3. investment in the parallel proceeding by the court and the parties;
>
> 4. overlap between issues raised in the petition and in the parallel proceeding;
>
> 5. whether the petitioner and the defendant in the parallel proceeding are the same party; and
>
> 6. other circumstances that impact the Board's exercise of discretion, including the merits.

Fintiv, Paper 11 at 5–6.

We discuss the parties' arguments in the context of considering the above factors. In evaluating the factors, we take a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review. *Id.*

1. Factor 1: Whether the Court Granted a Stay or Evidence Exists That One May Be Granted If a Proceeding Is Instituted

Petitioner contends this factor is neutral, given that a motion to stay has not yet been filed in district court. Pet. 69 (citing *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24, 7 (PTAB June 16, 2020) (informative)). Patent Owner agrees this factor is neutral as the district court has not considered a motion to stay. Prelim. Resp. 6. We agree with the parties that this factor is neutral.

2. Factor 2: Proximity of the Court's Trial Date to the Board's Projected Statutory Deadline for a Final Written Decision

Petitioner asserts the Agreed Scheduling Order in the district court proceeding "proposes July 27, 2021 as the date for the *Markman* hearing and June 6, 2022, as the trial date." Pet. 70 (citing Ex. 1022, 3–4). Petitioner contends however that "the current average time-to-trial for the district court

hearing the co-pending litigation is over two years," and therefore, this factor weighs against discretionary denial. *Id.*

Patent Owner contends that the underlying litigation is "currently scheduled for jury selection more than three months before the statutory deadline for a final written decision in this proceeding." Prelim. Resp. 6. According to Patent Owner, "Petitioner's analysis regarding the scheduled trial date for the co-pending litigation is filled with speculation about what might happen in that case." *Id.* at 6–7. Patent Owner asserts the jury selection for the district court proceeding is scheduled to begin June 6, 2022 and "this date would need to slip over three months before it approaches the Board's statutory deadline for a final written decision." *Id.* at 7. Patent Owner further asserts that "recent trial proceedings before the district court indicate that it is unlikely that the trial date will be significantly delayed, much less by the three months that would be required to shift the Board's analysis of this *Fintiv* factor." *Id.* Thus, according to Patent Owner, this factor weighs in favor of denial. *Id.* at 9.

The Agreed Scheduling Order proposes a trial date of June 6, 2022. Ex. 1022, 4. We note that the claim construction hearing was rescheduled twice and on August 3, 2021, was cancelled until further order of the court. *See K.Mizra LLC v. Cisco Sys. Inc.*, No. 6:20-cv-1031, Dkts. 26, 32, 37 (W.D. Tex. Aug. 3, 2021) (Ex. 3001). Although it is possible that this rescheduling may also impact the trial date, we do not speculate on the possible delay. In fact, the district court's recent Agreed Scheduling Order maintains the same trial date. *See K.Mizra LLC v. Cisco Sys. Inc.*, No. 6:20-cv-1031, Dkt. 43 (W.D. Tex. Sept. 20, 2021) (Ex. 3002, 3). The projected statutory deadline for a final written decision, however, is reasonably close

to the trial date (about three months after the trial date), and this factor weighs slightly in favor of exercising our discretion to deny institution.[5]

3. Factor 3: Investment in the Parallel Proceeding by the Court and the Parties

Petitioner contends "[t]he co-pending litigation is in its early stages, and the investment in it has been minimal." Pet. 71. According to Petitioner, this is evidenced by the following: "[t]he deadline to serve final infringement and invalidity contentions is not until September 23, 2021, fact discovery is not set to close until January 6, 2022, and expert discovery is not set to close until March 2, 2022." *Id.* (citing Ex. 1022, 3). Petitioner further contends it has "worked expeditiously to prepare and file this petition approximately one month after receiving Patent Owner's infringement contentions on February 5, 2021." *Id.* at 70.

Patent Owner contends this factor weighs in favor of denial because "by the time the Board may issue an Institution Decision in this proceeding, the parties and district court will have completed claim construction . . ., fact discovery will have been open for a month, and the parties will have served final infringement and invalidity contentions." Prelim. Resp. 9.

[5] Patent Owner argues that "the *inter partes* review process now includes . . . the additional step of discretionary review by the Director" which "will likely increase the gap between the district court trial date and a final determination, weighting this factor even more heavily in favor of discretionary denial." Prelim. Resp. 8–9. This factor, however, considers "proximity of the court's trial date to the Board's projected *statutory deadline for a final written decision*," not the time required to complete any subsequent rehearing requested by a party. *Fintiv*, Paper 11 at 5–6 (emphasis added).

The "investment factor is related to the trial date factor, in that more work completed by the parties and court in the parallel proceeding tends to support the arguments that the parallel proceeding is more advanced, a stay may be less likely, and instituting would lead to duplicative costs." *Fintiv*, Paper 11 at 10. Here, the related litigation is at an early stage. The deadline to serve final invalidity contentions is October 21, 2021. Ex. 3002, 2. Discovery is ongoing with a deadline for fact discovery of January 6, 2022, and expert discovery of March 2, 2022. *See* Ex. 1022, 3. As discussed above, the claim construction hearing has been rescheduled twice and has now been cancelled until further order by the court. On these facts, we find that the related litigation is at an early stage and the investment by the court and the parties therein is relatively minimal.

Additionally, Petitioner acted without much delay in filing the Petition on March 15, 2021 (*see* Paper 6, 1), which is only about a month after being served with Patent Owner's preliminary infringement contentions in the district court litigation. *See* Ex. 1019; *see also* Pet. 70.

Thus, this factor weighs against exercising our discretion to deny institution.

4. Factor 4: Overlap Between Issues Raised in the Petition and in the Parallel Proceeding

Petitioner contends this factor weighs against discretionary denial because "[t]here is no overlap of prior art issues at this time." Pet. 71. Further, Petitioner contends "there will be no overlap of prior art issues" because "[i]f the Board institutes trial, Petitioner will cease asserting in the co-pending litigation the combination of references on which trial is

instituted for the claims on which trial is instituted, to the extent Petitioner even asserts the same combination in the district court." *Id.*

Patent Owner contends this factor favors denial. Prelim. Resp. 10. Patent Owner acknowledges that "the Petition challenges claims not at issue in the district court litigation," but argues that "that mere fact is not enough to favor institution without some explanation as to why the additional claims are impactful." *Id.* (citing *Cisco*, IPR2021-00238, Paper 10 at 16). Patent Owner asserts that "Petitioner's offer to reduce its invalidity assertions based on the outcome of the Board's institution" does not change the analysis because "Petitioner [is seeking] two bites at the invalidity apple and is offering to discard one of its attempts only where the other shows particular promise." *Id.*

Petitioner's stipulation is not as encompassing as the one addressed in *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 18–19 (PTAB Dec. 1, 2020) (precedential as to § II.A) (noting that the petitioner broadly stipulated not to pursue "any ground raised or that could have been reasonably raised") (emphasis omitted). We are however persuaded that Petitioner's stipulation here mitigates some concern regarding duplicative efforts and potentially conflicting results.

Moreover, the Petition challenges claim 8, which is not at issue in the district court litigation and recites subject matter not found in the claims asserted in the district court. *See* Ex. 2002, 1; Pet. 17.

Thus, this factor weighs slightly against exercising our discretion to deny institution.

5. Factor 5: Whether the Petitioner and the Defendant in the Parallel Proceeding Are the Same Party

Petitioner acknowledges it is a defendant in the district court proceeding, but contends "[t]hat is true of most Petitioners in IPR proceedings" and further contends this factor is neutral and should not be a basis for denying institution. Pet. 72. Patent Owner contends this factor weighs in favor of denial in light of the fact that Petitioner is a defendant in the district court proceeding. Prelim. Resp. 11 (citing *Cisco*, IPR2021-00238, Paper 10 at 16–17). We agree with Patent Owner that this factor weighs in favor of exercising our discretion to deny institution.

6. Factor 6: Other Circumstances that Impact the Board's Exercise of Discretion, Including the Merits

Petitioner argues this factor weighs against discretionary denial because the merits of its arguments are strong. Pet. 72. Patent Owner argues this factor weighs in favor of denial because, in its Preliminary Response, Patent Owner raises substantive reasons why the Petition should be denied on its merits. Prelim. Resp. 11.

For the reasons discussed below regarding Petitioner's obviousness challenges, on the record before us, we find Petitioner's asserted ground to be relatively strong. For example, it is undisputed, on the current record, that the asserted references disclose each limitation of the challenged claims in the asserted ground. As discussed below, we are not persuaded at this stage of the proceeding by Patent Owner's arguments, including that Petitioner has failed to show a reason to combine the asserted references or that reasonable expectation of success for the proposed combination. Thus, we find that this factor weighs against exercising our discretion to deny institution.

7. Weighing the Factors

After weighing all of the factors and taking a holistic view of the relevant circumstances of this proceeding, we determine that, on balance, the factors favor not exercising discretion to deny institution under 35 U.S.C. § 314(a).

B. Level of Ordinary Skill in the Art

Supported by the testimony of Dr. Reddy, Petitioner proposes that a 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).

At this stage of the proceeding, Patent Owner does not oppose Petitioner's articulation of the level of ordinary skill in the art, although Patent Owner states that it "reserves the right to dispute Petitioner's definition if an IPR is instituted." Prelim. Resp. 16.

Based on the current record, we find Petitioner's proposal 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); *In re GPAC Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995). Therefore, 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.

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) (2019). 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; Prelim. Resp. 17. 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. Prelim. Resp. 17.

The parties dispute construction of "trusted platform module" (Pet. 13–16; Prelim. Resp. 17) but do not identify any issue that would turn on the construction of this term, at least for purposes of deciding whether to institute a review. *See generally* Pet.; Prelim. Resp.

Based on the current 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. For the reasons discussed below, we determine that, on the present record, the information presented shows a reasonable likelihood that Petitioner would prevail on this ground with respect to all challenged claims.

1. Relevant Principles of Law

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. *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.[6] *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of "whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring "articulated reasoning with some rational underpinning to support the legal conclusion of obviousness")); *see Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1366–67 (Fed. Cir. 2012) (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]")). Petitioner cannot satisfy its burden of proving obviousness by employing "mere conclusory statements." *In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1380 (Fed. Cir. 2016).

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

2. Overview of Gleichauf (Ex. 1005)

Gleichauf describes a system for controlling access to a network when a device attempts to connect to the network. Ex. 1005, 3:7–9.

[6] The parties do not present arguments or evidence related to such secondary considerations. Therefore, secondary considerations do not constitute part of our analysis in this Decision.

Figure 1 of *Gleichauf* is reproduced below.

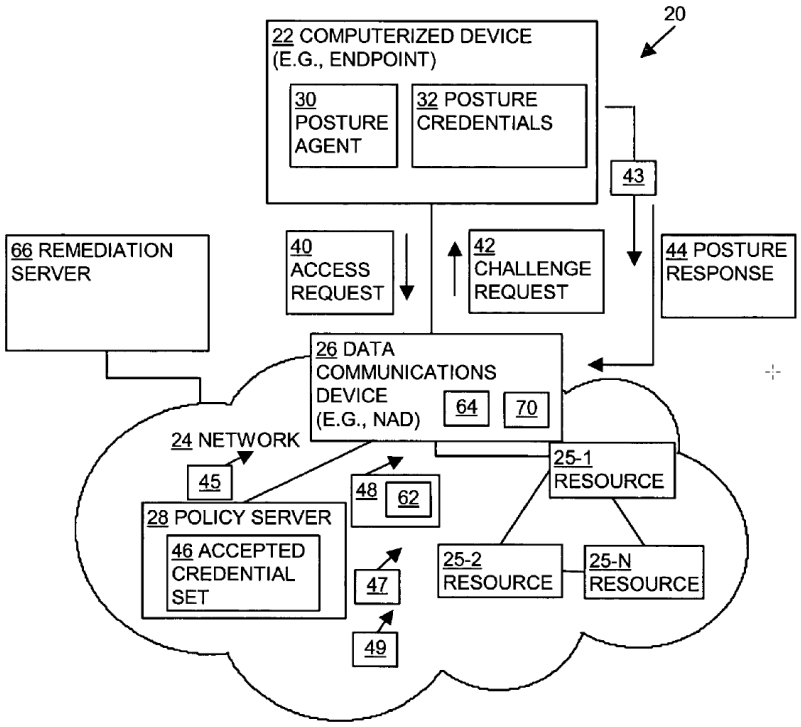


Figure 1 illustrates an exemplary data communication system. *Id.* at 8:32–33.

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., firewall) 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.

In an embodiment, the policy server can send notification messages to the posture agent running on the computing device placed on a quarantine network, automatically connecting or prompting the user to manually connect the computing device to a remediation server on the quarantine network. *Id.* at 4:57–5:8. 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.

3. 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.

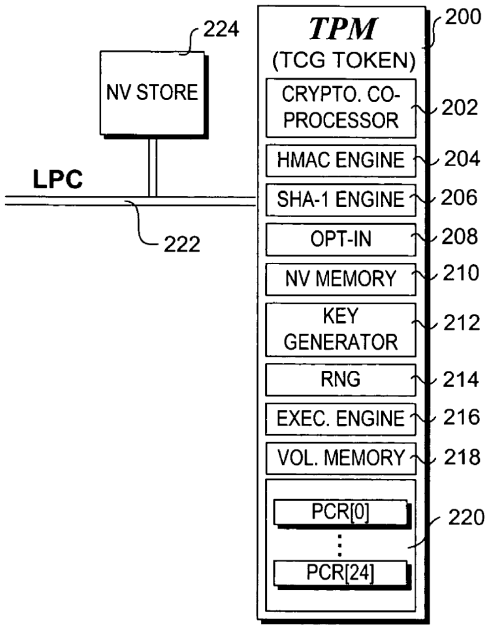


Figure 2 is a schematic diagram of a trusted platform module. *Id.* at 3:7–8.

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.

4. 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.

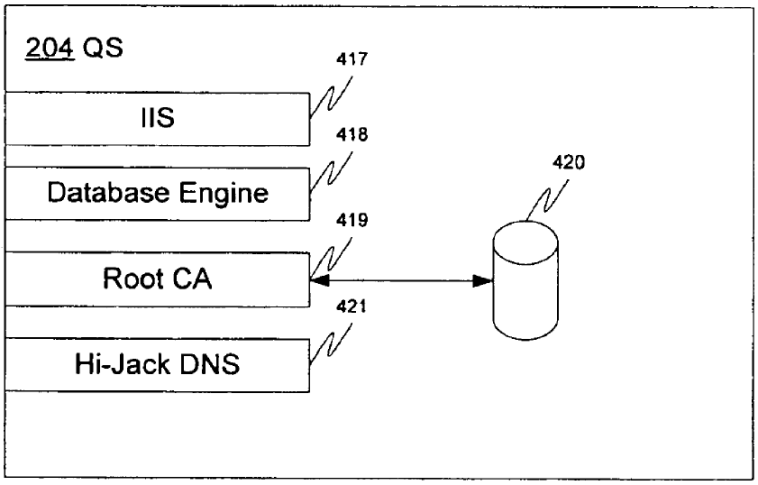


Figure 4 illustrates a quarantine server of Lewis. *Id.* at 4:52–53.

As shown in Figure 4, quarantine server (QS) 201[7] 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 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.

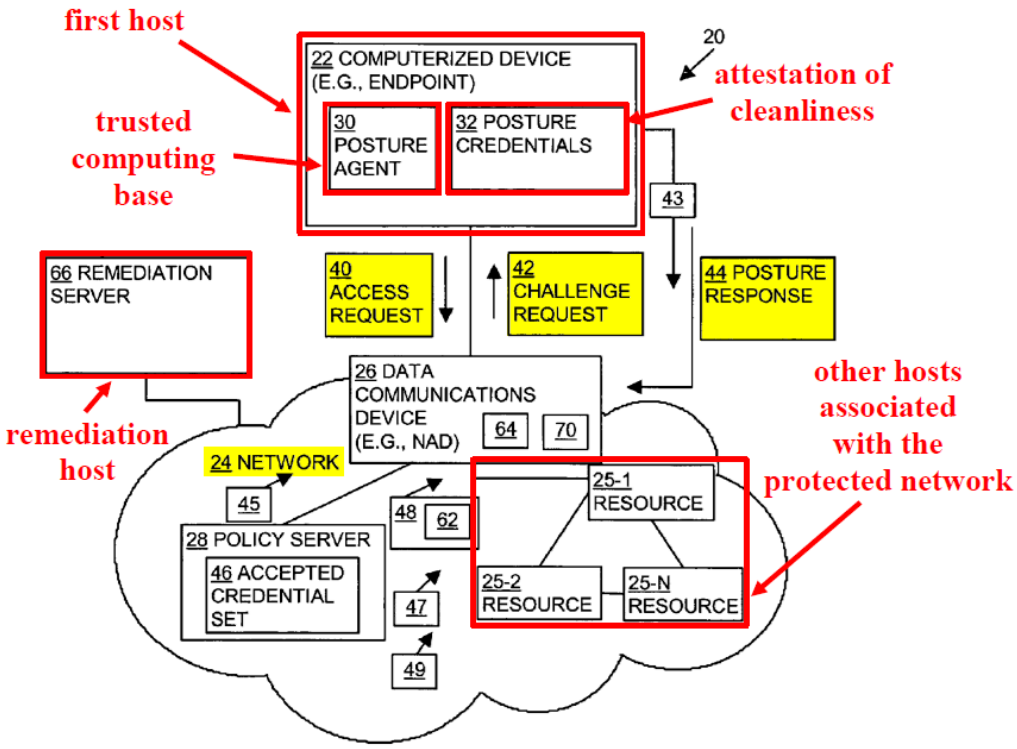
5. Proposed Combination of Gleichauf, Ovadia, and Lewis

In its proposed combination of Gleichauf, Ovadia, and Lewis, Petitioner relies on Gleichauf to teach most of the limitations of the challenged independent claims, except for (1) the limitations reciting

[7] 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.

"trusted platform module," for which Petitioner relies on Ovadia, and (2) the limitations relating to the operation of the recited "quarantine server," for which Petitioner relies on Lewis. *See* Pet. 29–54 (claim 1), 65–67 (claims 12 and 19).

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 recited limitations of the challenged independent claims, 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. Pet. 29–33, 38–47, 50, 54.

As discussed above, 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. In the proposed combination, according to Petitioner, "Gleichauf's posture agent would be implemented with trusted platform module functionality, i.e., a trusted platform module, per Ovadia." *Id.* at 36. Petitioner also relies on Ovadia for its disclosure of the details the TPM's security functions, including TPM's use of Attestation Identity Keys (AIKs) to digitally sign attestation of the integrity measurements, to teach the limitations reciting "digitally signed attestation." *Id.* at 40. 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 33–35, 47–53.

6. Independent Claim 1

Petitioner contends that the combination of Gleichauf, Ovadia, and Lewis teaches each of the recitations of claim 1. Pet. 29–54. At this stage of the proceeding, Patent Owner does not dispute that the combination teaches the claimed subject matter. *See generally* Prelim. Resp.

a. Differences Between the Claimed Subject Matter and the Prior Art

(i) Preamble

The preamble of claim 1 recites "[a] method for protecting a network." Ex. 1001, 19:57. Petitioner contends that Gleichauf teaches the preamble of claim 1 because Gleichauf describes a "computer-implemented method to control access to resources in a network." Pet. 29 (citing Ex. 1005, 27:61–62; Ex. 1003 ¶¶ 72–74). Petitioner further asserts that Gleichauf's method protects the network by decreasing the likelihood of malware or virus infection and ensuring that the device attempting to access the network is authorized and is the device it claims to be. *Id.* (citing Ex. 1005, 5:55–60, 7:56–61, 8:16–31, 12:57–67).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently that Gleichauf teaches the preamble of claim 1.[8]

[8] At this stage of the proceeding, we do not determine whether the preamble is limiting. *See Vivid Techs.*, 200 F.3d at 803.

(ii) Limitation [1.1]

Next, addressing the limitations recited in the body of the claim, Petitioner contends that Gleichauf teaches "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network," as recited in claim 1. Pet. 29–32. Petitioner identifies this recitation as limitation [1.1]. *Id.* at 29.

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. *Id.* at 30 (citing Ex. 1005, Fig. 1). Petitioner contends that Gleichauf teaches limitation [1.1] 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).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently that Gleichauf teaches limitation [1.1].

(iii) Limitations [1.2], [1.3], and [1.4]

Claim 1 recites "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." Petitioner labels these recitations as limitations [1.2], [1.3], and [1.4], as indicated in brackets above. Pet. 32, 38, 39. Petitioner contends that the combination of Gleichauf and Ovadia teaches each of these limitations. *Id.* at 32–42.

Addressing first limitation [1.2], Petitioner asserts that Gleichauf's "posture agent" and "posture plug-ins" teach the recited "trusted computing base" because the posture agent collects information about the device's security posture from the "posture plug-ins" installed on the device and prepares posture credentials that it transmits to the policy server for analysis and access control. Pet. 32 (citing Ex. 1005, 3:9–16, 9:24–39; Ex. 1003 ¶¶ 82–85). Petitioner further argues that "[s]ince the posture credentials are used to secure the restricted resources, a [person of ordinary skill in the art] would have understood that the combined functionality of the posture agent and plug-ins is part of the mechanism that provides such security." *Id.* (citing Ex. 1003 ¶ 86). Petitioner asserts, therefore, the combined functionality of the posture agent and plug-ins is a "trusted computing base" recited in claim 1. *Id.* at 32–33 (citing Ex. 1003 ¶ 86).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently that Gleichauf teaches a "trusted computing base" recited in claim 1.

As discussed above, 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. 33–34 (citing Ex. 1006, 4:16–55, Fig. 2; Ex. 1003 ¶¶ 87–89). Petitioner contends that in the proposed combination "Gleichauf's posture agent would be implemented with trusted platform module functionality, i.e., a trusted platform module, per Ovadia." *Id.* at 36 (citing Ex. 1003 ¶ 93). Relying on the testimony of Dr. Reddy, Petitioner asserts that "[t]he posture agent implemented with trusted platform module functionality would interface with Gleichauf's posture plug-ins in the same way disclosed in Gleichauf by using the 'posture plug-in API [application programming interface]' to collect information requested by Gleichauf's policy server." *Id.* (citing Ex. 1005, 9:24–28; Ex. 1003 ¶ 94). Petitioner further argues that "[w]ith the posture agent (part of the trusted computing base) . . . integrated with the TPM software," the functionality of the posture agent and posture plug-ins would be "associated with a trusted platform module," as recited in the claim. *Id.* at 36–37 (citing Ex. 1003 ¶ 94).

Next, Petitioner asserts that Gleichauf's policy server "contacts" the computerized device's posture agent (the claimed "trusted computing base"), which prompts the posture agent to collect the device's posture credentials from the posture plug-ins. Pet. 37 (citing Ex. 1005, 4:7–11, 3:28–36; Ex. 1003 ¶ 90).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently that the combination of Gleichauf and Ovadia teaches "contacting a trusted computing base

associated with a trusted platform module within the first host," as recited in claim 1 (limitation [1.2]).

Next, Petitioner contends that Gleichauf teaches "receiving a response," as recited in the claim, because Gleichauf describes Gleichauf's posture agent responding to the policy server's request with its policy credentials and the policy server receiving a response to its request for policy credentials. Pet. 38 (citing Ex. 1005, 3:28–36, 4:11–15, Fig. 1; Ex. 1003 ¶¶ 96–99).

Based on the record presented, for purposes of this Decision, Petitioner has shown sufficiently that Gleichauf teaches "receiving a response," as recited in claim 1 (limitation [1.3]).

Next, Petitioner asserts that the combination of Gleichauf and Ovadia teaches "determining whether the response includes a valid digitally signed attestation of cleanliness," as recited in the claim (limitation [1.4]). Pet. 39–42. First, Petitioner contends that Gleichauf teaches the recited "attestation of cleanliness" because the posture credentials received by the policy server contain information such as "what particular virus software and virus definition versions are installed," "when was the last time a local antivirus scan was executed," "what operating system patches are installed," and "types and versions of software applications" on the device. *Id.* at 39 (citing Ex. 1005, 3:36–49; Ex. 1003 ¶ 101). Petitioner further asserts that Gleichauf teaches "determining whether the response includes a valid . . . attestation of cleanliness," as recited in the claim, because Gleichauf's policy server analyzes and "validate[s] the posture credentials." *Id.* (citing Ex. 1005, 10:30–33; Ex. 1003 ¶ 102).

As discussed above, in the proposed combination of Gleichauf and Ovadia, Petitioner relies on Ovadia as teaching the recited "digitally signed attestation." Pet. 40. Specifically, Petitioner relies on Ovadia's disclosure of TPM's use of Attestation Identity Key (AIK) to digitally sign attestation of the integrity measurements stored in the trusted platform module. *Id.* (citing Ex. 1006, 5:35–36, 13:61–64, 14:1–10, 14:13–23, 16:66–17:6, Fig. 8; Ex. 1003 ¶ 106). Petitioner asserts that "[i]n the combination, Gleichauf's posture credentials, prepared by the posture agent implemented with trusted platform module functionality, would be digitally signed, as taught by Ovadia." *Id.* at 42 (citing Ex. 1003 ¶¶ 107–109).

Based on the record presented, for purposes of this Decision, Petitioner has shown sufficiently that the combination of Gleichauf and Ovadia teaches "determining whether the response includes a valid digitally signed attestation of cleanliness," as recited in claim 1 (limitation [1.4]).

Thus, Petitioner has shown sufficiently that the combination of Gleichauf and Ovadia teaches "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," as recited in claim 1.

(iv) Limitation [1.5]

Claim 1 recites "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." Petitioner identifies this recitation as limitation [1.5]. Pet. 42.

Petitioner contends the combination of Gleichauf and Ovadia teaches "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," as recited in the claim, because Gleichauf's posture credentials transmitted to the policy server (the claimed "attestation of cleanliness") contain information about "the last time a local antivirus scan was executed." Pet. 42 (citing Ex. 1005, 3:41; Ex. 1003 ¶¶ 110–111). Citing the testimony of Dr. Reddy, Petitioner argues that if a posture credential shows timely execution of the anti-virus scan, a person of ordinary skill in the art would have understood it as showing "an attestation that the trusted computing base has ascertained that the first host is not infested." *Id.* (citing Ex. 1003 ¶ 111).

Petitioner further asserts that Gleichauf teaches "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," as recited in the claim, because Gleichauf's posture credentials also contain information about "what particular virus software and virus definition versions are installed," "what operating system patches are installed," and "types and versions of software applications" on the device. Pet. 42–43 (citing Ex. 1005, 3:36–49; Ex. 1003 ¶ 112).

Based on the record presented, for purposes of this Decision, we determine that Petitioner has shown sufficiently that the combination of Gleichauf and Ovadia teaches "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," as recited in claim 1 (limitation [1.5]).

(v) Limitation [1.6]

Claim 1 recites "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 identifies this recitation as limitation [1.6]. Pet. 44.

As discussed above with respect to limitation [1.4], Petitioner asserts that "[i]n the combination, Gleichauf's posture credentials, prepared by the posture agent implemented with trusted platform module functionality, would be digitally signed, as taught by Ovadia." Pet. 42 (citing Ex. 1003 ¶¶ 107–109). Petitioner contends the combination of Gleichauf and Ovadia teaches limitation [1.6] because in the combination, 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. *Id.* at 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).

Based on the record presented, for purposes of this Decision, we determine that Petitioner has shown sufficiently that the combination of Gleichauf and Ovadia teaches limitation [1.6] of claim 1.

(vi) Limitations [1.7], [1.8], and [1.9]

Claim 1 recites "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.

Petitioner labels these recitations as limitations [1.7], [1.8], and [1.9], as indicated in brackets above. Pet. 46, 47, 49. Petitioner contends that Gleichauf teaches limitation [1.7] and that the combination of Gleichauf and Lewis teaches limitations [1.8] and [1.9]. *Id.* at 46–54.

First, 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).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently that Gleichauf teaches "receiving a service request sent by the first host," as recited in claim 1 (limitation [1.7]).

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. 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.* at 47–48; 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. *Id.* 48 (citing Ex. 1005, 4:56–63, 21:1–12; Ex. 1007, 4:24–31, 13:7–12; Ex. 1003 ¶¶ 135–136). 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).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently that the combination of Gleichauf and Lewis teaches "serving a quarantine notification page to the first host when the service request comprises a web server request," as recited in claim 1 (limitation [1.8]).

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.

First, as discussed above in Section III.D.5, Petitioner maps the recited "remediation host" to Gleichauf's remediation server 66. Pet. 50 (citing Ex. 1005, 5:4–11; Ex. 1003 ¶ 141). Petitioner asserts that Gleichauf teaches the recited "remediation host configured to provide data usable to remedy the insecure condition" because Gleichauf's 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.* (citing Ex. 1005, 5:4–11; Ex. 1003 ¶ 141).

Citing the testimony of Dr. Reddy, Petitioner further contends that a person of ordinary skill in the art would have known that "HTTP traffic, such as that from Gleichauf's device, is usually preceded by a DNS query." Pet. 51 (citing Ex. 1003 ¶ 145). Petitioner and Dr. Reddy cite U.S. Patent No. 7,568,107 B1 (Ex. 1008), as supporting evidence of their contention. *Id.* (citing Ex. 1008, 5:49–63; Ex. 1003 ¶ 145). Thus, Petitioner argues that a person of ordinary skill in the art would have understood that Gleichauf teaches or suggests "in the event the service request comprises a DNS query," as recited in claim 1. *Id.* (citing Ex. 1003 ¶ 145).

Petitioner further asserts that the combination of Gleichauf and Lewis teaches "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" because Gleichauf describes that "HTTP traffic from the [quarantined] device directed to the remediation server is permitted while HTTP traffic directed to other destinations is redirected." Pet. 50 (citing Ex. 1005, 14:62–66, 15:55–67; Ex. 1003 ¶¶ 143–144). As discussed above with respect to limitation [1.8], Petitioner argues 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).

Lastly, Petitioner 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]." Pet. 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 (citing Ex. 1003 ¶ 148).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently that the combination of Gleichauf and Lewis teaches "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," as recited in claim 1 (limitation [1.9]).

(vii) Limitation [1.10]

Claim 1 recites "permitting the first host to communicate with the remediation host." Petitioner identifies this recitation as limitation [1.10]. Pet. 54.

Petitioner contends Gleichauf teaches this limitation because Gleichauf discloses that a computerized device out of compliance with network admission policy is quarantined and communications from the device to network resources are restricted or rejected except that HTTP traffic from the quarantined device to a remediation server is permitted.

Pet. 54 (citing Ex. 1005, 4:50–56, 11:58–67, 14:62–66; Ex. 1003 ¶¶ 151–154).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently that Gleichauf teaches "permitting the first host to communicate with the remediation host," recited in claim 1 (limitation [1.10]).

b. Motivation to Combine

(i) Motivation to Combine Gleichauf and Ovadia

Citing the testimony of its declarant, Dr. Reddy, Petitioner contends that a person of ordinary skill in the art would have been motivated to combine the teachings of Gleichauf and Ovadia as proposed by Petitioner because the trusted platform module described in Ovadia was well-known in the field as being part of a platform-independent industry standard from the Trusted Computing Group. Pet. 21–22 (citing Ex. 1003 ¶¶ 55–56). Petitioner further asserts that "following the industry standard, as described in Ovadia, would benefit Gleichauf's system by formatting a device's posture credentials consistently and with substantially the same information, regardless of the device's manufacturer or components." *Id.* at 22–23 (citing Ex. 1003 ¶¶ 56–57). Petitioner argues that "[f]ollowing the industry standard would also promote the interoperability of devices from diverse manufacturers" and that "[e]nsuring the interoperability of devices is a common and important goal in the computer networking arts." *Id.* at 23 (citing Ex. 1003 ¶ 57).

Citing the testimony of Dr. Reddy, Petitioner further asserts that a person of ordinary skill in the art would have been motivated to combine the

teachings of Gleichauf and Ovadia because Ovadia provides additional details regarding implementation of Gleichauf's techniques, such as authenticating a device with digital signature and using AIKs to digitally sign attestations. Pet. 24–25 (citing Ex. 1003 ¶¶ 60–63).

In addition, Dr. Reddy testifies that Gleichauf's and Ovadia's systems have "analogous architectures" and "both solve similar problems within the same field of network access authentication." Ex. 1003 ¶ 64; Pet. 26 (citing Ex. 1003 ¶ 64). Dr. Reddy explains as follows:

> Like the posture agent in Gleichauf, which is used to gather information about the device's "configuration state," Ovadia describes using "an authentication agent to determine the state of a platform environment" and generate an "integrity measurement." Gleichauf at 3:8, 12:21–31; Ovadia at 4:40–43, 14:1–6, Fig. 8. Ovadia's integrity measurement is stored in the TPM and then provided to an authentication server as part of authentication data in response to an authentication challenge. Ovadia at 4:43–45, 13:61–63, Fig. 8. This is *analogous to Gleichauf's description* of sending the configuration state of a device (or "posture credentials") to a policy server in response to "one or more requests 49 to authenticate the computerized device" seeking network access. Gleichauf at 10:63–11:3.

Ex. 1003 ¶ 62 (emphasis added); Pet. 25 (citing Ex. 1005, 3:8, 10:63–11:3, 12:21–31; Ex. 1006, 4:40–43, 4:43–45, 13:61–63, 14:1–6, Fig. 8; Ex. 1003 ¶ 62). Dr. Reddy further states that "Gleichauf and Ovadia also both describe providing an explanatory message if the posture credentials or integrity measurement, respectively, are not accepted." Ex. 1003 ¶ 64 (citing Ex. 1005, 4:50–67; Ex. 1006, 16:62–65); Pet. 26 (citing Ex. 1005, 4:50–67; Ex. 1006, 16:62–65; Ex. 1003 ¶ 64). Dr. Reddy testifies, therefore, a person of ordinary skill in the art would have had a reasonable expectation

of success in combining the teachings of Gleichauf and Ovadia. Ex. 1003 ¶ 64.

In the Preliminary Response, Patent Owner presents several arguments disputing Petitioner's contentions regarding the motivation to combine Gleichauf and Ovadia with a reasonable expectation of success. *See* Prelim. Resp. 21–37. We address each of Patent Owner's arguments in turn.

First, Patent Owner argues that Petitioner does not identify the claim limitations that are missing in Gleichauf in the proposed combination of Gleichauf and Ovadia. Prelim. Resp. 21.

We disagree that Petitioner has failed to identify the claim limitations that are missing in Gleichauf. As explained above in our discussion of Petitioner's contentions regarding the proposed combination of the teachings of the asserted references (Section III.D.5) and the differences between the claimed subject matter and the prior art (Section III.D.6.a), Petitioner specifically identifies the prior art reference that Petitioner alleges teaches each claim limitation. *See, e.g.*, Pet. 29–54.

Next, Patent Owner asserts that a person of ordinary skill in the art would not have been motivated to combine Ovadia's teachings of the TCG/TPM industry standard with Gleichauf to achieve interoperability because interoperability is already provided by the features disclosed in Gleichauf. Prelim. Resp. 23–25. Patent Owner argues that Gleichauf already discloses interoperability by using "well defined, application independent forms for representing information or data," such as the Type-Length Value (TLV) format or an extensible markup language (XML) format, as well as "using protocols such as the Extensible Authentication

Protocol (EAP), Protected Extensible Authentication Protocol (PEAP) and Flexible EAP Authentication using Secure Tunnel Protocol (EAP-FAST)" to "securely transmit posture and/or identity." *Id.* (citing Ex. 1005, 9:6–19, 10:14–19, 11:3–12, 12:60–67, 20:54–64, 22:11–23) (emphases omitted). Patent Owner asserts that there is no motivation to combine Gleichauf with Ovadia because "[a person of ordinary skill in the art] would not be motivated to modify a prior art reference to address a given problem *if the reference already addresses it*." *Id.* at 25 (emphasis added) (citing *Henny Penny Corp. v. Frymaster LLC*, 938 F.3d 1324, 1332 (Fed. Cir. 2019)).

At this stage of the proceeding, based on the current record, Patent Owner's argument and evidence does not undermine Petitioner's showing of motivation to combine. As explained by Petitioner's declarant, Dr. Reddy, the TCG/TPM Specification was promoted as industry standard to specifically address "network security" and "trust in computing platforms." Ex. 1003 ¶ 58; Pet. 23 (citing Ex. 1006, 4:16–35; Ex. 1003 ¶ 58). Dr. Reddy's explanation of the benefits of combining the teachings of Gleichauf with the teachings of the TCG "platform-independent industry specification," as described in Ovadia, is premised on the ordinary artisan's understanding of the features of the TCG/TPM standard to "enhanc[e] the security of the computing environment in disparate computer platforms," including the feature of TCG/TPM that "[i]nformation provided by the TPM is 'trusted' because this information cannot be altered, and it is commonly encrypted or otherwise protected from manipulation by others." Ex. 1003 ¶ 56 (citing TCG Specification Architecture Overview (Ex. 1012); U.S. Patent Pub. No. 2003/0061494 (Ex. 1014) ¶ 11); Pet. 22 (citing Ex. 1003 ¶ 56; Ex. 1012, 2; Ex. 1014 ¶ 11). In other words, according to Dr. Reddy

and Petitioner, the interoperability resulting from adopting the TCG/TPM standard is not merely a generic compatibility—such as using the same file formats—but, rather, interoperability specific to the network security and platform trust functions.

Patent Owner does not explain adequately why the TLV and XML file formats or the EAP / PEAP/ EAP-FAST authentication protocols described in Gleichauf address "trust in computing platforms" or provide the same or similar security and trust functions described in the TCG/TPM Specification. Nor does Patent Owner explain sufficiently whether the TLV and XML file formats or the EAP etc. protocols have been widely adopted as industry standards to provide interoperability for the "network security" and "trust in computing platforms" functions in computer systems similar to the TCG/TPM Specification. Thus, at this stage of the proceeding, Patent Owner does not establish sufficiently that Gleichauf "already addresses" the same or similar interoperability provided by the TCG/TPM standard.

In addition, the fact that the TLV and XML file formats or the EAP / PEAP/ EAP-FAST authentication protocols provide interoperability in some aspects, e.g., file compatibility, does not necessarily take away from the motivation to adopt the TCG/TPM standard to obtain interoperability with respect to the network security and platform trust functions. Thus, at this stage of the proceeding, Patent Owner's reliance on *Henny Penny* does not undermine Petitioner's showing of motivation to combine.

Next, Patent Owner disputes Petitioner's contentions on reasonable expectation of success in combining Gleichauf and Ovadia because "the two references are fundamentally different and directed towards opposite goals." Prelim. Resp. 29, 38. Patent Owner provides a technical discussion of

Gleichauf and Ovadia to conclude that a person of ordinary skill in the art would not have found it reasonable to combine these references because "Gleichauf would deny access based on a ***lack*** of a change, and Ovadia would deny access based on the ***presence*** of a change." *Id.* at 29–34.

As discussed above, however, Petitioner argues, citing the testimony of Dr. Reddy, "[t]he analogous architectures of Gleichauf's and Ovadia's respective systems . . . would have provided a [person of ordinary skill in the art] with a reasonable expectation of success in combining their disclosures." Pet. 26 (citing Ex. 1003 ¶ 64). In the cited paragraph of his Declaration, Dr. Reddy testifies that Gleichauf's and Ovadia's systems have "analogous architectures" and "both solve similar problems within the same field of network access authentication." Ex. 1003 ¶ 64. Dr. Reddy also explains how Ovadia/TPM's authentication challenge-response process is analogous to Gleichauf's posture credentials challenge-response process. *Id.* ¶ 62.

Although Patent Owner and Petitioner argue opposite positions regarding the similarities or differences between Gleichauf and Ovadia, Patent Owner's argument at this stage is not supported by declaration evidence of how a person of ordinary skill in the art would have understood Gleichauf and Ovadia, whereas Petitioner's contentions are supported by the Reddy Declaration and the cited evidence of record. "What a prior art reference discloses or teaches is determined from the perspective of one of ordinary skill in the art." *Sundance, Inc. v. DeMonte Fabricating Ltd.*, 550 F.3d 1356, 1361 n.3 (Fed. Cir. 2008). At this stage of the proceeding, we credit Dr. Reddy's testimony and determine, based on the current record, Patent Owner's argument that Gleichauf and Ovadia "are fundamentally different and directed towards opposite goals" is insufficient to undercut

Petitioner's showing of motivation to combine or a reasonable expectation of success.

Next, Patent Owner argues that "the TPM execution engine is a special purpose processor with a limited instruction set that is highly secure and is not open for various external software to be implemented within the engine" and that Petitioner provides no evidence "(1) how a TPM chip manufacturer would develop within the TPM execution engine, software typically developed by third parties; or (2) why the TPM manufacturer would open up the chip to external software integration in that way." Prelim. Resp. 28–29 (citing Ex. 1013, 19).

Dr. Reddy testifies, however, "[t]he [proposed] combination permits but does not require physical incorporation of elements from Ovadia into Gleichauf." Ex. 1003 ¶ 65. To the extent Patent Owner's argument is premised on physical incorporation of the TPM execution engine or a TMP chip into Gleichauf's device, we disagree with Patent Owner because "[t]he test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference . . . . Rather, the test is what the combined teachings of the references would have suggested to those of ordinary skill in the art." *MCM Portfolio LLC v. Hewlett-Packard Co.*, 812 F.3d 1284, 1294 (Fed. Cir. 2015) (*quoting In re Keller*, 642 F.2d 413, 425 (CCPA 1981)).

Lastly, Patent Owner contends, based on its technical discussion of Gleichauf and Ovadia, that Petitioner has not shown sufficiently how a person of ordinary skill in the art would have combined Gleichauf with Ovadia to arrive at the claimed invention of the '705 patent. Prelim. Resp. 26–29.

As discussed above in Section III.D.6.a, Petitioner relies on the combination of Gleichauf and Ovadia to teach limitations [1.2] and [1.4]. Pet. 32–37, 39–42. With respect to limitation [1.2], Petitioner contends that in the proposed combination of Gleichauf and Ovadia, "Gleichauf's posture agent would be implemented with trusted platform module functionality, i.e., a trusted platform module, per Ovadia." *Id.* at 36 (citing Ex. 1003 ¶ 93). Relying on the testimony of Dr. Reddy, Petitioner asserts that "[t]he posture agent implemented with trusted platform module functionality would interface with Gleichauf's posture plug-ins in the same way disclosed in Gleichauf by using the 'posture plug-in API [application programming interface]' to collect information requested by Gleichauf's policy server." *Id.* (citing Ex. 1005, 9:24–28; Ex. 1003 ¶ 94). In the cited paragraph of his Declaration, Dr. Reddy testifies that "[a person of ordinary skill in the art] would have appreciated that one obvious way to implement Gleichauf's posture agent with TPM functionality would be for the posture agent software to be executed by the execution engine in Ovadia's TPM." Ex. 1003 ¶ 94 (citing Ex. 1006, Fig. 2). Dr. Reddy also opines that "[a person of ordinary skill in the art] would have appreciated that another obvious way to implement Gleichauf's posture agent with TPM functionality would be to simply integrate the posture agent software with a software-implemented TPM, as taught by Ovadia." *Id.* (citing Ex. 1006, 4:24–26).

In addition, as discussed above with respect to limitation [1.4], Petitioner relies on Ovadia's disclosure of TPM's use of Attestation Identity Key (AIK) to digitally sign attestation of the integrity measurements stored in the trusted platform module. Pet. 40 (citing Ex. 1006, 5:35–36, 13:61–64, 14:1–10, 14:13–23, 16:66–17:6, Fig. 8; Ex. 1003 ¶ 106). Citing the Reddy

Declaration, Petitioner asserts that "[i]n the combination, Gleichauf's posture credentials, prepared by the posture agent implemented with trusted platform module functionality, would be digitally signed, as taught by Ovadia." *Id.* at 42 (citing Ex. 1003 ¶¶ 107–109). In the cited paragraph of his Declaration, Dr. Reddy explains that because "Ovadia explains that . . . 'AIKs are only permitted to sign data generated by a TPM,'" a person of ordinary skill in the art would have understood that "the TPM (embodied in Gleichauf's posture agent implemented with TPM functionality . . .) . . . would only sign posture credentials that it prepares itself." Ex. 1003 ¶ 107 (citing Ex. 1006, 5:35–36, 14:9).

Based on the record presented, we determine, for purposes of this Decision, Petitioner has shown sufficiently how a person of ordinary skill in the art would have combined Gleichauf with Ovadia to obtain the subject matter recited in limitations [1.2] and [1.4]. We also determine, for purposes of this Decision, Petitioner sufficiently articulates a reason why a person of ordinary skill in the art would have been motivated to combine Gleichauf and Ovadia with a reasonable expectation of success.

(ii) Motivation to Combine Gleichauf, Ovadia, and Lewis

Addressing the motivation to combine Gleichauf, Ovadia, and Lewis, Petitioner contends that a person of ordinary skill in the art "when considering the teachings of Gleichauf and Ovadia would have also considered the teachings of Lewis, as all of the references relate to providing secure access when an individual computerized device connects to a network." Pet. 26–27 (citing Ex. 1005, 3:4–9; Ex. 1006, 1:8–11; Ex. 1007, 4:7–9; Ex. 1003 ¶ 66). Citing the testimony of Dr. Reddy, Petitioner asserts that the combination of Gleichauf, Ovadia, and Lewis would have been

obvious because "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." *Id.* at 27 (citing Ex. 1003 ¶ 68).

Petitioner further argues that the proposed combination would have been beneficial because "[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." Pet. 28 (citing Ex. 1003 ¶ 69). Citing the testimony of Dr. Reddy, Petitioner asserts 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).

In addition, Petitioner contends that a person of ordinary skill in the art would have had a reasonable expectation of success in combining the teachings of Gleichauf and Ovadia with Lewis because an ordinary artisan "would have found it straight-forward to provide the contents of Gleichauf's notification message in a webpage since doing so would display the contents of the message to the user in the browser the user is already using." Pet. 29 (citing Ex. 1003 ¶ 70).

Addressing the motivation to combine Gleichauf and Ovadia with Lewis, Patent Owner asserts that Petitioner does not provide sufficient motivation to "substitute Gleichauf's notification message with Lewis's quarantine webpage" because Petitioner does not show that "Gleichauf's notification message was *insufficient* for meeting its objectives." Prelim. Resp. 39 (emphasis added).

To the extent Patent Owner argues that a showing of a shortcoming in a reference is required to demonstrate a motivation to combine with another reference, we disagree with Patent Owner's argument. On the contrary, the Supreme Court in *KSR* has set forth an "expansive and flexible approach" to obviousness determination. *KSR*, 550 U.S. at 415. Under *KSR*, "[t]he required 'expansive and flexible approach' . . . may look at a variety of facts, including prior-art teachings and marketplace demands and *artisans'* background knowledge, 'in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.'" *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 992 (Fed. Cir. 2017) (quoting *KSR*, 550 U.S. at 415, 418).

As discussed above, Dr. Reddy testifies that the proposed combination would have been beneficial because "[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" and 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." Ex. 1003 ¶ 69; Pet. 28 (citing Ex. 1003 ¶ 69).

At this juncture, for purposes of this Decision, we credit Dr. Reddy's testimony and conclude that Petitioner sufficiently articulates a reason 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 with a reasonable expectation of success in doing so.

The record would benefit from further development of the issue of motivation to combine, and Patent Owner will have an opportunity to do so

during the trial through introduction of its own evidence and through cross-examination of Dr. Reddy.

c. Patent Owner's Remaining Arguments

As discussed above, at this stage of the proceeding, Patent Owner does not dispute that the combination of Gleichauf, Ovadia, and Lewis teaches each of the recitations of claim 1. *See generally* Prelim. Resp. In Section III.D.6.b above, we address Patent Owner's arguments regarding the motivation to combine. We address Patent Owner's remaining arguments here.

(i) Dr. Reddy's Declaration

Patent Owner argues that Dr. Reddy's declaration should be given no weight. Prelim. Resp. 19–20. Patent Owner contends that Petitioner's argument on motivation to combine Gleichauf and Ovadia is mostly identical to the Dr. Reddy's declaration testimony on that issue. *Id.* at 20 (citing Pet. 21–26; Ex. 1003 ¶¶ 54–65). Patent Owner further contends that "[m]ost of the arguments copied from the petition in Dr. Reddy's declaration amount to nothing more than conclusory statements without any objective evidentiary support." *Id.* at 20 (citing Pet. 25; Ex. 1003 ¶ 63). Patent Owner therefore asks us to afford no weight to Dr. Reddy's declaration testimony. *Id.* at 19, 20.

The extent to which a party chooses to copy language from a declaration in a brief is that party's choice. A declaration is not less persuasive simply because a party repeats the language in its brief. Rather, a critical inquiry is the helpfulness of the declaration. *See* Fed. R. Evid. 702(a) ("A witness who is qualified as an expert . . . may testify . . . if: (a) the expert's . . . knowledge will help the trier of fact to understand the

evidence or to determine a fact in issue . . . .”). The helpfulness of a declaration is judged based on the specific issues presented in a given case.

Here, Petitioner relies upon Dr. Reddy’s declaration to the extent noted in our discussion above. For the purposes of this Decision, we find Dr. Reddy’s opinions supported by the cited evidence. For example, his testimony that a person of ordinary skill in the art would have been motivated to take advantage of Ovadia’s use of a TPM—as described in the TCG “platform-independent industry specification”—because it would standardize Gleichauf’s posture credentials is supported by citations to Gleichauf, Ovadia, and other evidence of record. *See* Ex. 1003 ¶¶ 54–56 (citing Ex. 1005, 3:4–9; Ex. 1006, 1:8–11, 4:32–35; Ex. 1012 (TCG Specification Architecture Overview), 2–4; Ex. 1014 (U.S. Patent Pub. No. 2003/0061494) ¶ 11; Ex. 1021 (Yan) ¶¶ 3–4; Ex. 1023 (Cromer), 2:8–11)

We therefore decline Patent Owner’s request to disregard Dr. Reddy’s declaration at this stage in the proceeding.

(ii) Identifying Challenged Grounds with Requisite Particularity

Patent Owner also argues that Petitioner fails to identify its challenged grounds with requisite particularity because Petitioner’s grounds rely on several more references than identified by Petitioner. Prelim. Resp. 40–43. Patent Owner contends that Petitioner identified Ground 1 as the combination of Gleichauf, Ovadia, and Lewis, but relies on at least seven more references in its analysis for Ground 1, and according to Patent Owner, these references should have been identified as part of Petitioner’s asserted obviousness combinations. *Id.* at 41 (citing Pet. 33–34, 44, 48, 51, 53;

Exs. 1008, 1009, 1011, 1012, 1013, 1015, 1016). Patent Owner asserts that Petitioner was required to show, among other things, that a person of ordinary skill in the art would have been motivated to combine ten references, not three, to arrive at the challenged claims in order to set forth a *prima facie* case of obviousness for Ground 1. *Id.* at 41–42.

We disagree. Petitioner relies on Gleichauf, Ovadia, and Lewis as teaching each of the limitations of the challenged claims under Ground 1. Petitioner cites to the additional seven references merely to illustrate well-known concepts or explain how a person of ordinary skill would have understood the asserted references. For example, Petitioner cites Exhibit 1015 (U.S. Patent Application Publication 2005/0078668 A1) as evidence of how a person of ordinary skill in the art would have known that URL redirection involves a request for a webpage. *See* Pet. 47–48 (citing Ex. 1015 ¶ 3). Similarly, Petitioner cites to Exhibit 1011 (U.S. Patent No. 6,829,654 B1) to support its contention that it was well-known that a "URL typically includes the domain name of the provider of the identified resource." *Id.* at 53 (citing Ex. 1011, 9:12–14). Likewise, Petitioner relies on Exhibit 1008 (U.S. Patent No. 7,568,107 B1) in support of its assertion that the steps in DNS query to obtain the internet protocol (IP) address of a named server, e.g., a web server in the case of HTTP traffic, were "commonly known and ubiquitously employed by web browsers in the prior art." *Id.* at 51 (citing Ex. 1008, 5:49-63).

We are therefore not persuaded on the record before us that Petitioner fails to identify its challenged grounds with requisite particularity.

d. Conclusion Regarding Claim 1

Based on the record presented, for purposes of this Decision, Petitioner makes a sufficient showing that the combination of Gleichauf, Ovadia, and Lewis teaches each of the recitations of claim 1. We also find that Petitioner articulates sufficient rationale for combining the respective teachings of Gleichauf, Ovadia, and Lewis under the standard applicable at this stage of the proceeding. Accordingly, based on the record presented, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing in its challenge to claim 1 as unpatentable under 35 U.S.C. § 103(a) over the combination of Gleichauf, Ovadia, and Lewis.

7. Independent Claims 12 and 19

Claim 12 recites "[a] system for protecting a network," "a processor configured to," "a memory coupled to the processor and configured to provide instructions to the processor," and also recites other limitations that are substantially similar to those in claim 1. Ex. 1001, 21:1–38.

Petitioner asserts that Gleichauf teaches the recited "system for protecting a network" because Gleichauf describes a "robust network security architecture and system for controlling access to a network." Pet. 65 (citing Ex. 1005, 3:4–9). Petitioner further argues that Gleichauf teaches the recited "processor" and "memory" because Gleichauf's policy server "includes a controller 209 formed of a memory 210 and a processor 212." *Id.* at 65–66 (citing Ex. 1005, 25:41–46). Citing the testimony of Dr. Reddy, Petitioner asserts that a person of ordinary skill in the art would have understood that memory 210 is coupled to processor 212 because they are part of the same controller 209. *Id.* at 66 (citing Ex. 1003 ¶ 224). Petitioner further argues that memory 210 is "configured to provide

instructions to the processor" of the policy server because it is "encoded with logic instructions (e.g., software code) and/or data that form a credential analysis application 246" where "application 246 represents software code, instructions and/or data . . . that reside within memory . . . accessible to the policy server 28." *Id.* (citing Ex. 1005, 26:66–27:8).

For the remaining limitations of claim 12, Petitioner relies on its arguments directed to claim 1. Pet. 65 (arguing that "[e]lements [12.2]–[12.11] are substantively identical to the steps of claim 1 and are rendered obvious for the same reasons.").

Claim 19 recites "[a] computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions," and also recites other limitations that are similar to those in claim 1. Ex. 1001, 22:14–49.

Petitioner contends that Gleichauf teaches the recited computer program product because it describes a "computer program product 200 includes an application or logic instructions that are loaded into the computerized device 22, data communications device 26, and policy server 28 to configure the devices 22, 24, 26 to operate as part of the data communications system 20." Pet. 66–67 (citing Ex. 1005, 25:46–51, 3:4–9).

For the remaining limitations of claim 19, Petitioner relies on its arguments directed to claim 1. Pet. 67 (arguing that "[e]lements [19.1]–[19.10] are substantively identical to the steps of claim 1 and are rendered obvious for the same reasons.").

Patent Owner does not present separate argument for claims 12 and 19. *See* Prelim. Resp. 21–40 (arguing all challenged claims together).

For the reasons discussed above with respect to claim 1, and because Petitioner sufficiently shows that Gleichauf teaches the additional elements recited in claims 12 and 19, we determine, based on the record presented, that Petitioner has demonstrated a reasonable likelihood of prevailing in its challenge to independent claims 12 and 19 as unpatentable under 35 U.S.C. § 103(a) over the combination of Gleichauf, Ovadia, and Lewis.

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

Claims 2, 3, and 5–11 each depend directly from claim 1 and claims 13 and 15–18 depend directly or indirectly from claim 12.

Petitioner contends that Gleichauf teaches or suggests each of the additionally recited limitations of dependent claims 2, 3, 5, 7–11, 13, and 15–18. Pet. 54–59, 60–64, 66. Petitioner also asserts that the combination of Gleichauf and Lewis teaches or suggest the additionally recited limitation of dependent claim 6. *Id.* at 59–60. Petitioner provides explanations and citations to the prior art indicating where in the references the claimed features are disclosed or explaining how the differences between the claimed subject matter and the prior art are such that the subject matter would have been obvious to a person of ordinary skill in the art. *Id.* at 54–64, 66. In addition, Petitioner relies upon the Reddy Declaration to support its positions. *Id.* We have reviewed this evidence and argument.

Patent Owner does not present separate argument for dependent claims 2, 3, 5–11, 13, and 15–18. *See* Prelim. Resp. 21–40 (arguing all challenged claims together).

Based on the record presented, we determine that Petitioner has demonstrated a reasonable likelihood of prevailing in its challenge to

claims 2, 3, 5–11, 13, and 15–18 as unpatentable under 35 U.S.C. § 103(a) over the combination of Gleichauf, Ovadia, and Lewis.

IV. CONCLUSION

For the foregoing reasons, we conclude that the information presented in the Petition establishes a reasonable likelihood that Petitioner would prevail in proving that all challenged claims of the '705 patent are unpatentable under § 103(a). Accordingly, we institute an *inter partes* review of all challenged claims based on the ground asserted in the Petition.

At this stage of the proceeding, we have not made a final determination as to the patentability of any of the challenged claims. Our final determination will be based on the record as fully developed during trial.

V. ORDER

In consideration of the foregoing, it is

ORDERED that, pursuant to 35 U.S.C. § 314(a), *inter partes* review is hereby instituted as to claims 1–3, 5–13, and 15–19 of the '705 patent on the ground set forth in the Petition; and

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

PETITIONER:

Theodore Foster
David McCombs
Eugene Goryunov
Gregory 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

PATENT OWNER:

Sang Hui Kim
Palani Rathinasamy
David Schumann
FOLIO LAW GROUP PLLC
michael.kim@foliolaw.com
palani@foliolaw.com
david.schumann@foliolaw.com