UNITED STATES PATENT AND TRADEMARK OFFICE

_____

BEFORE THE PATENT TRIAL AND APPEAL BOARD

_____

CISCO SYSTEMS, INC.,
Petitioner

_____

IPR2021-00593
U.S. Patent No. 8,234,705

PETITION FOR *INTER PARTES* REVIEW UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104

TABLE OF CONTENTS

PETITIONER'S EXHIBIT LIST

Ex.1001	U.S. 8,234,705
Ex.1002	Prosecution History of U.S. 8,234,705
Ex.1003	Declaration of A.L. Narasimha Reddy, Ph.D., Under 37 C.F.R. § 1.68 in Support of Petition for *Inter Partes* Review
Ex.1004	*Curriculum Vitae* of Narasimha Reddy, Ph.D.
Ex.1005	U.S. Patent No. 9,436,820 to Gleichauf et al.
Ex.1006	U.S. Patent No. 7,747,862 to Ovadia
Ex.1007	U.S. Patent No. 7,533,407 to Lewis et al.
Ex.1008	U.S. Patent No. 7,568,107 to Rathi et al.
Ex.1009	U.S. Patent Pub. No. 2004/0177276 to MacKinnon et al.
Ex.1010	U.S. Patent Pub. No. 2006/0005009 to Ball et al.
Ex.1011	U.S. Patent No. 6,829,654 to Jungck
Ex.1012	TCG Specification Architecture Overview (Rev. 1.2 Apr. 28, 2004), *available at*: https://web.archive.org/web/20061003162035if_/https://www.trustedcomputinggroup.org/groups/TCG_1_0_Architecture_Overview.pdf
Ex.1013	TPM Main – Part 1 Design Principles, Specification Version 1.2 (Rev. 62 Oct. 2, 2003), *available at*: https://trustedcomputinggroup.org/wp-content/uploads/tpmwg-mainrev62_Part1_Design_Principles.pdf
Ex.1014	U.S. Patent Pub. No. 2003/0061494 to Girard et al.
Ex.1015	U.S. Patent Pub. No. 2005/0078668 to Wittenberg et al.
Ex.1016	U.S. Patent No. 7,571,460 to Danforth et al.

Ex.1017	U.S. Patent Pub. No. 2005/0097199 to Woodard et al.
Ex.1018	Complaint, *K.Mizra LLC v. Cisco Systems, Inc.*, No. 6-20-cv-01031 (W.D. Tex. Nov. 6, 2020).
Ex.1019	Plaintiff's Preliminary Infringement Contentions, *K.Mizra LLC v. Cisco Systems, Inc.*, No. 6-20-cv-01031 (W.D. Tex. Feb. 5, 2021) (without exhibits).
Ex.1020	Lex Machina court statistics for the Federal District Court for the Western District of Texas
Ex.1021	U.S. Patent Pub. No. 2005/0033987 to Yan et al.
Ex.1022	[Proposed] Agreed Scheduling Order, *K.Mizra LLC v. Cisco Systems, Inc.*, No. 6-20-cv-01031 (W.D. Tex. Feb. 5, 2021)
Ex.1023	U.S. Patent No. 7,330,977 to Cromer et al.

I. INTRODUCTION

Pursuant to 35 U.S.C. §§ 311, 314(a), and 37 C.F.R. § 42.100, Cisco Systems, Inc. ("Petitioner") respectfully requests that the Board review and cancel as unpatentable under (pre-AIA) 35 U.S.C. §103(a) claims 1-3, 5-13, and 15-19 (hereinafter, the "Challenged Claims") of U.S. 8,234,705 (the "'705 patent," Ex.1001).

The '705 patent describes evaluating a host requesting access to a protected network and restricting the host's access if its security measures are inadequate. Ex.1001, Abstract. As shown below and confirmed in the Declaration of Narasimha Reddy, Ph.D. (Ex.1003) these concepts were well known before the priority date of the '705 patent. The references presented in this Petition demonstrate the obviousness of the Challenged Claims. *See generally*, Ex.1003.

II. MANDATORY NOTICES

A. Real Party-in-Interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is Cisco Systems, Inc.

B. Related Matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner, the '705 patent is or was involved in the following cases:

Case Heading	Number	Court	Filed
K. Mizra LLC v. Cisco Systems, Inc.	6-20-cv-01031	WDTX	November 6, 2020
Network Security Technologies, LLC v. Bradford Networks, Inc.	1-17-cv-01487	DDE	October 24, 2017
Network Security Technologies, LLC v. ForeScout Technologies, Inc.	1-17-cv-01488	DDE	October 24, 2017
Network Security Technologies, LLC v. McAfee, Inc.	1-17-cv-01489	DDE	October 24, 2017
Network Security Technologies, LLC v. Pulse Secure, LLC	1-17-cv-01490	DDE	October 24, 2017

C. Lead and Back-up Counsel and Service Information

Lead Counsel
Theodore M. Foster
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (972) 739-8649
Fax: (214) 200-0853
ipr.theo.foster@haynesboone.com
USPTO Reg. No. 57,456

Back-up Counsel
David L. McCombs
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (214) 651-5533
Fax: (214) 200-0853
david.mccombs.ipr@haynesboone.com
USPTO Reg. No. 32,271

Eugene Goryunov
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219
Phone: (312) 216-1630
Fax: (214) 200-0853
eugene.goryunov.ipr@haynesboone.com
USPTO Reg. No. 61,579

Gregory P. Huh
HAYNES AND BOONE, LLP
2323 Victory Ave. Suite 700
Dallas, TX 75219

Phone: (972) 739-6939
Fax: (214) 200-0853
gregory.huh.ipr@haynesboone.com
USPTO Reg. No. 70,480

Please address all correspondence in this proceeding to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above.

III. GROUNDS FOR STANDING

Petitioner certifies that the '705 patent is eligible for IPR and that Petitioner is not barred or estopped from requesting IPR of the Challenged Claims. 37 C.F.R. § 42.104(a).

IV. NOTE

Petitioner cites to exhibits' original page numbers. **Emphasis** in quoted material has been added. Claim terms are presented in *italics*.

V. SUMMARY OF THE '705 PATENT

The '705 patent describes attempting to defend a computer network against threats by analyzing the security state of a device that seeks network access. The device is quarantined if its security state is determined to be inadequate. Ex.1001, Abstract. A device in quarantine "is provided only limited access to the protected network." Ex.1001, 3:9-13. A quarantine notification page, i.e., a webpage, is displayed to the device and "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." Ex.1001, 15:66-16:7. The device is "permitted to access the protected network only as required to remedy a condition that caused the quarantine to be imposed." Ex.1001, 3:14-17.

These concepts were well known before the priority date of the '705 patent.

VI. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in The Art ("POSITA") in September 2004 would have had a working knowledge of the network communication art that is pertinent to the '705 patent, including network security methodologies. Ex.1003, ¶ 18. A POSITA 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. Ex.1003, ¶ 18. Lack of professional experience can be remedied by additional education, and vice versa. Ex.1003, ¶ 18.

VII. CLAIM CONSTRUCTION

Claim terms in IPR are construed according to their "ordinary and customary meaning" to those of skill in the art. 37 C.F.R. § 42.100(b). For the purposes of this proceeding and the ground presented herein, Petitioner proposes construing the

terms below. Constructions are proposed "only to the extent necessary." *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017).

A. "*trusted computing base*"

Claims 1, 12, and 19 recite in part a "*trusted computing base*." For example, claim 1 recites "*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.*"

The '705 patent describes examples of trusted computing bases, which it distinguishes from other components that could respond to a cleanliness query, such as anti-contagion software or an operating system:

> A computer associated with an address identified in a list is queried for a cleanliness assertion (1302), for example by contacting a **trusted computing base** within a computer, and requesting an authenticated infestation scan by trusted software. An example of a **trusted computing base** within a computer is the Paladium security initiative under development by Microsoft and supported by Intel and American Micro Devices. Another example of a **trusted computing base** is described in various TCG specifications, such as the TCG Architecture Overview, published by the Trusted Computing Group. Trusted code bases may for example execute antivirus scans of the remainder of the computer, including untrusted portions of the disk and/or operating system. In some embodiments, trusted code bases

> may digitally sign assertions about the cleanliness (e.g. infestation status) and/or state of their computers. In some embodiments, the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus software, with assertions about the currency of a scan, such as the last time a scan was performed, or a version associated with a current anti-contagion software or definition file in use, wherein a sufficiently updated software and/or scan may act as a cleanliness assertion. In some embodiments, an operating system may respond with information associated with its patch level, wherein a sufficiently recent patch level may be interpreted as an assertion of cleanliness.

Ex.1001, 13:64-14:22.

During prosecution of the '705 patent, the applicants argued that *trusted computing base* is a term of art whose definition was provided on Wikipedia:

> Applicant notes that "trusted computing base" and "trusted platform module["] are terms of art with specific meanings that are in no way discussed in Liang.… As for the term of art "trusted computing base," the final paragraph of the "Definition and characterization" section of the Wikipedia entry on "Trusted Computing Base" (http://en.wikipedia.org/wiki/Trusted_computing_base; retrieved January 10, 2010) states that "A given piece of hardware or software is a part of the TCB if and only if it has been designed to be a part of the mechanism that provides its security to the computer system."

Ex.1002, pp. 183-184.

The term "*trusted computing base*" should be construed according to the express definition provided by the applicants during prosecution. Ex.1003, ¶¶ 32-35. Thus, "*trusted computing base*" should be construed as *a piece of hardware or software that has been designed to be part of a mechanism that provides security to a computer system*. Ex.1003, ¶ 35.

B. "*trusted platform module*"

Claims 1, 12, and 19 recite in part a "*trusted platform module*." For example, claim 1 recites "*contacting a trusted computing base associated with a* ***trusted platform module*** *within the first host*."

The specification does not use the term *trusted platform module*. During prosecution of the '705 patent, the applicants argued that *trusted platform module* is a term of art that specifically refers to a secure cryptoprocessor that, among other things, implements a standard of the same name promulgated by the Trusted Computing Group:

> Applicant notes that "trusted computing base" and "trusted platform module[”] are terms of art with specific meanings that are in no way discussed in Liang. The Wikipedia entry for "Trusted Platform Module (http://en.wikipedia.org/wiki/Trusted platform module; retrieved January 10, 2010) begins, "In computing, Trusted Platform Module (TPM) is both the name of a published specification detailing a secure cryptoprocessor that can store cryptographic keys that protect information, as well as the general name of implementations of that

> specification, often called the "TPM chip" or "TPM Security Device" (as designated in certain Dell BIOS settings[1]). The TPM specification is the work of the Trusted Computing Group. The current version of the TPM specification is 1.2 Revision 103, published on July 9, 2007." Reinforcing the industry adoption of this technology and standardization around the term of art used in the claims, this specification has also been adopted as ISO/IEC standard 11889.

Ex.1002, pp. 183-184.

Consistent with the applicants' arguments, the Trusted Platform Module specification describes a trusted platform module that includes various components for performing cryptographic operations and storing cryptographic information. Major components are depicted in figures reproduced below:

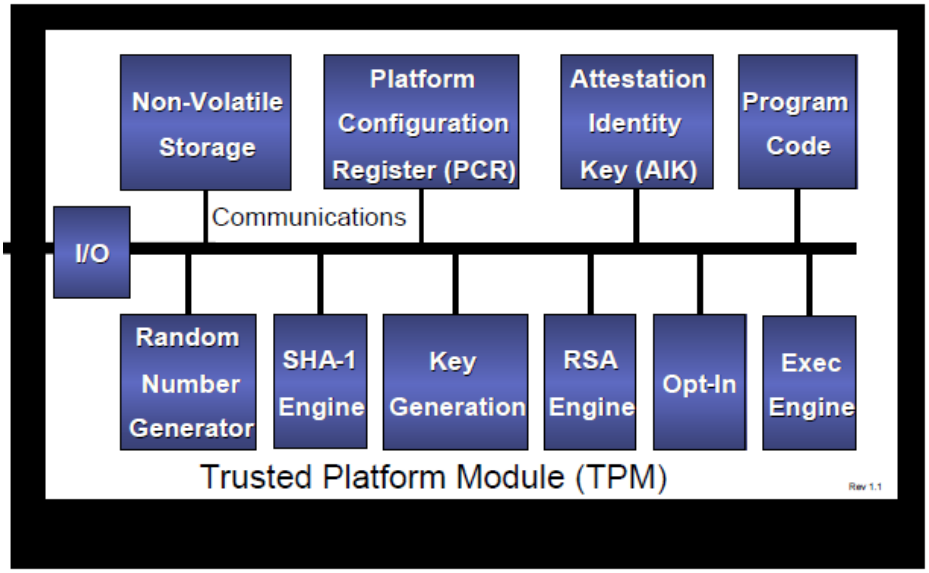
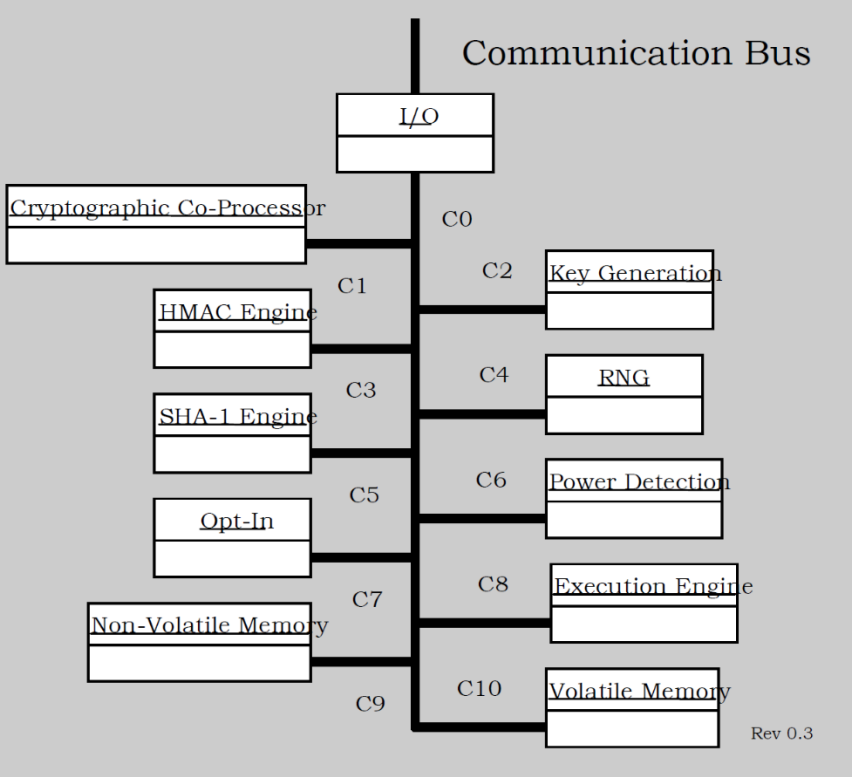


Figure 4:g – TPM Component Architecture

Ex.1012, 19.



Ex.1013, 11.

According to the Trusted Platform Module specification, the components of a trusted platform module include an input/output (I/O) component, a key generation component, a random number generator (RNG), a SHA-1 engine, an opt-in component, an execution engine, and memory (volatile and non-volatile). Ex.1013, 11-22; Ex.1012, 19-20. Consistent with the applicants' statement—that a trusted platform module "store[s] cryptographic keys that protect information"—the Trusted Platform Module specification provides that a compliant trusted platform module stores cryptographic keys in memory. *See* Ex.1012, 19 ("Non-volatile storage is used to store Endorsement Key (EK), Storage Root Key (SRK),

owner authorization data and persistent flags."); *see also* Ex.1013, 19 ("Non-volatile memory component … is used to store persistent identity and state associated with the TPM.")

The term "*trusted platform module*" should be construed according to the express definition provided by the applicants during prosecution. Ex.1003, ¶¶ 36-40. Thus, "*trusted platform module*" should be construed as *a secure cryptoprocessor that implements the Trusted Platform Module specification from the Trusted Computing Group*. Ex.1003, ¶ 40.

VIII. RELIEF REQUESTED AND THE REASONS FOR THE REQUESTED RELIEF

Petitioner asks that the Board institute a trial for *inter partes* review and cancel the Challenged Claims in view of the analysis below.

IX. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Challenged Claims

The Challenged Claims (1-3, 5-13, and 15-19) include (1) claims that Patent Owner has asserted in the co-pending litigation and (2) other claims that are also rendered unpatentable by the same prior art. A finding that the Challenged Claims are unpatentable in this proceeding will resolve the parties' dispute and obviate the need for a trial regarding the '705 patent in the co-pending litigation, substantially reducing the time and expense of that litigation for all parties.

B. Statutory Grounds for Challenges

Ground	Claims	Basis
#1	1-3, 5-13, 15-19	35 U.S.C. § 103 (Pre-AIA) over Gleichauf in view of Ovadia and Lewis

U.S. Patent No. 9,436,820 to **Gleichauf** et al. (Ex.1005, "Gleichauf") was filed on August 2, 2004.

U.S. Patent No. 7,747,862 to **Ovadia** (Ex.1006, "Ovadia") was filed on June 28, 2004.

U.S. Patent No. 7,533,407 to **Lewis** et al. (Ex.1007, "Lewis") was filed on April 14, 2004.

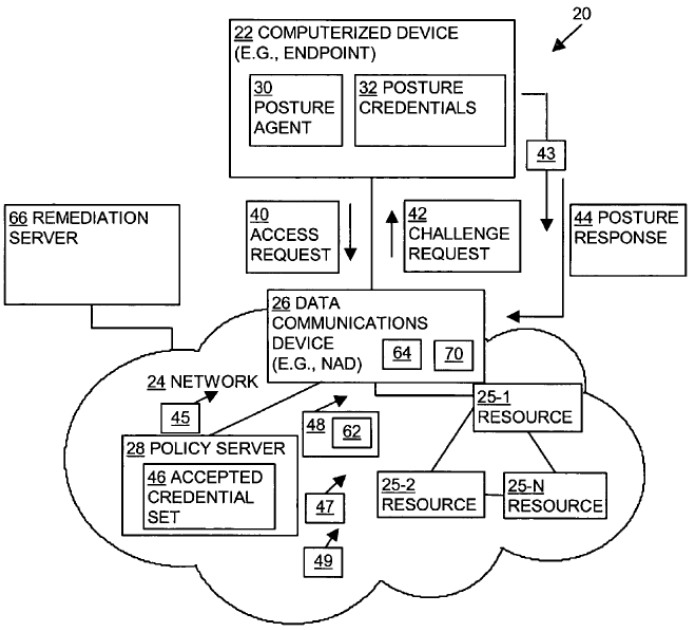
Gleichauf, Ovadia, and Lewis are prior art under 35 U.S.C. § 102(e).

Petitioner's analysis also cites additional prior art to demonstrate the knowledge of a POSITA and to provide contemporaneous context to support Petitioner's assertions regarding what a POSITA would have understood from the asserted prior art. *See Yeda Research v. Mylan Pharm. Inc.*, 906 F.3d 1031, 1041-1042 (Fed. Cir. 2018) (affirming the use of "supporting evidence relied upon to support the challenge"); 37 C.F.R. § 42.104(b); *see also K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1365-66 (Fed. Cir. 2014); *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1363 (Fed. Cir. 2016).

C. Ground 1

1. Gleichauf

Gleichauf generally relates to the field of network security. Ex.1005, 7:55-61; Ex.1003, ¶ 45. Gleichauf teaches controlling a computerized device's access to network resources based on the security posture of the device. Ex.1005, 3:4-9; Ex.1003 ¶ 45. Gleichauf illustrates a data communications system in Figure 1 that includes a device that is attempting to access a network resource on the network:



Ex.1005, Fig. 1.

Gleichauf's policy server controls the device's access to the network. Ex.1005, 7:4-8, 10:20-23; Ex.1003, ¶ 46. When the policy server detects a security issue with a device, e.g., an out-of-date anti-virus application, the device is quarantined. Ex.1005, 15:55-61; Ex.1003, ¶ 47. While in quarantine, the device has

limited network access but is still permitted to access a remediation server with security updates suitable to bring the device into compliance with network access security protocols. Ex.1005, 16:13-21; Ex.1003, ¶ 47. Normal access is generally granted after the device is updated. Ex.1005, 16:40-43; Ex.1003, ¶ 47.

Gleichauf was not before the Examiner during prosecution of the '705 patent.

2. Ovadia

Like Gleichauf, Ovadia discloses network security measures and describes steps to ensure that a device seeking to access a network has an authorized configuration. Ex.1006, 1:8-11, Abstract; Ex.1003, ¶ 49. Ovadia's security scheme generates security keys, including attestation identity keys ("AIKs"), using a trusted platform module. Ex.1006, Abstract; Ex.1003, ¶ 49. The trusted platform module is used "to verify [that] a current configuration of a subscriber station platform is an authorized configuration." Ex.1006, Abstract; Ex.1003, ¶ 49. A subscriber station seeking network access "sends authentication information including a manifest signed with the SS's [subscriber station's] private AIK key." Ex.1006, Abstract; Ex.1003, ¶ 49. An authentication server receives the information and authenticates the subscriber station via the subscriber station's public AIK key. Ex.1006, Abstract; Ex.1003, ¶ 49.

Ovadia was not before the Examiner during prosecution of the '705 patent.

3. Lewis

Like Gleichauf, Lewis describes network security measures, including verifying the configuration state of a device that seeks to access a network. Ex.1007, 4:7-9; Ex.1003, ¶ 51. Lewis provides "a system for ensuring that machines having invalid or corrupt states are restricted from accessing network resources." Ex.1007, 4:7-9; Ex.1003, ¶ 51. Lewis describes how the device must provide a "bill of health" to a quarantine server before gaining access to the network. Ex.1007, 4:13-15; Ex.1003, ¶ 51. The quarantine server determines if the bill of health is valid or invalid. Ex.1007, 4:16-23; Ex.1003, ¶ 51. A valid bill of health indicates that the device has up-to-date security software, and the device is granted access to the network. Ex.1007, 4:18-21; Ex.1003, ¶ 51. An invalid bill of health indicates that the device lacks security measures sufficient for access to the network, and the device's network configuration is put in a lock-down configuration. Ex.1007, 13:44-52; Ex.1003, ¶ 51.

The lock-down configuration puts the device in quarantine. Ex.1007, 13:63-65; Ex.1003, ¶ 52. A quarantined device's communications are restricted, but it is permitted to access the quarantine server that provides a webpage to inform the "user that the client [device] is in quarantine and corrective action must be taken." Ex.1007, 10:61-66; Ex.1003, ¶ 52. If the user performs the corrective action and submits an updated bill of health that is valid, the device is permitted access to the

network. Ex.1007, 13:12-15; Ex.1003, ¶ 52.

During prosecution of the '705 patent, Lewis's corresponding application publication, U.S. Patent Pub. No. 2005/0131997, was cited by the Examiner for its teaching of a quarantine server providing a quarantine notification page. Ex.1002, 98-99. The applicants did not dispute this, arguing instead that the Examiner's cited art (including Lewis) failed to render obvious other features recited in then-pending claim 1. Ex.1002 at 73-74; Ex.1003, ¶ 53. Petitioner is relying on Lewis for the same point asserted by the Examiner and conceded by the applicants. As such, Lewis is cited for a point of agreement that was not overcome during prosecution. There is no basis for the Board to exercise its 35 U.S.C. § 325(d) discretion on these facts.

4. Reasons to Combine Gleichauf and Ovadia

A POSITA when considering the teachings of Gleichauf would have also considered the teachings of Ovadia, as both relate to providing secure access when an individual computerized device connects to a network. Ex.1005, 3:4-9; Ex.1006, 1:8-11; Ex.1003, ¶ 54. A POSITA would have been motivated to combine the teachings of Gleichauf and Ovadia for multiple reasons and doing so would have been within the POSITA's skillset. Ex.1003, ¶ 55. The combination would have been obvious because it merely uses known techniques (e.g., Ovadia's trusted platform module security infrastructure and digital signatures) to improve a similar

method (e.g., Gleichauf's authentication and authorization of devices seeking network access) in the same way. Ex.1003, ¶ 55.

A POSITA would have been motivated to take advantage of Ovadia's use of a trusted platform module—as described in the Trusted Computing Group "platform-independent industry specification"—because it would standardize Gleichauf's posture credentials. Ex.1006, 4:32-35; Ex.1003, ¶ 56; *see also* Ex.1012, 2 (TCG was formed as an "industry-standards organization with the aim of enhancing the security of the computing environment in disparate computer platforms."). A TCG-defined TPM can advantageously be used to provide asset tracking functionalities, collect and report (in a trusted manner) platform configuration information, and secure client-server communications. Ex.1012, 2-4; *see also* Ex.1014, [0011] ("The TCPA architecture includes an isolated computing engine, or trusted platform module (TPM) (not shown), whose processes can be trusted because they cannot be altered. … Additionally, the TPM may encrypt or wrap data, such as a key, and may bind or seal an internally generated asymmetric key pair to a particular TPM and/or a particular platform configuration."); Ex.1023, 2:8-11 (TCPA is the former name of TCG); Ex.1021, [0003]-[0004] (same). Put differently, 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. Ex.1003, ¶ 56. This would also allow Gleichauf's policy server to process posture credentials that were received, in a trusted manner, more efficiently and in substantially the same way regardless of the device returning the credentials. Ex.1003, ¶ 56. Following the industry standard would also promote the interoperability of devices from diverse manufacturers. Ex.1003, ¶ 57. Ensuring the interoperability of devices is a common and important goal in the computer networking arts. Ex.1003, ¶ 57.

Ovadia describes applying technology from the "Trusted Computing Group (TCG)" which addresses "network security" and "covers trust in computing platforms in general." Ex.1006, 4:16-35. A POSITA would thus have understood that the trusted computing and authentication technologies described in Ovadia are not limited to the wireless networks Ovadia describes but instead are generally applicable to networks—like Gleichauf's—that condition network access on authentication and authorization of client devices. Ex.1003, ¶ 58.

The combination also would have been obvious because it applies the known technique of digitally signing an attestation about the state of a device to make its authentication more secure (as in Ovadia) with the known network authorization process of analyzing a device's security posture credentials, including its authentication (as in Gleichauf) to yield predictable results. Ex.1003, ¶ 59. A POSITA would have been familiar with the use of digital signatures to prove the

integrity and authenticity of network communications and would have recognized that Ovadia's digital signature technique would improve Gleichauf's process by increasing resistance to forged or tampered-with posture credentials. Ex.1010, [0033]; Ex.1003, ¶ 59. A POSITA also would have recognized that use of a digital signature would improve Gleichauf's process by allowing the policy server to confirm that the posture credentials originated with the device attempting to access the network. Ex.1003, ¶ 59.

A POSITA also would have been motivated to combine the teachings of Gleichauf and Ovadia because Ovadia provides additional details regarding implementation of Gleichauf's techniques. Ex.1003, ¶ 60. Gleichauf provides that "policy server 28 authenticates an identity of the computerized device 22 to generate an authentication result." Ex.1005, 22:3-5. Ovadia explains that one way to authenticate a device is to check that device's digital signature. Ex.1006, 16:30-32. It would have been obvious to a POSITA to use Ovadia's digital signatures as a way of performing Gleichauf's device authentication. Ex.1003, ¶ 60.

A POSITA would have had a reasonable expectation of success in combining Gleichauf and Ovadia. Ex.1003, ¶ 61. Notably, components of Ovadia's trusted computing architecture have corresponding components in Gleichauf's architecture, and a POSITA would have recognized how details provided for components in Ovadia would be applicable to the corresponding components in

Gleichauf. Ex.1003, ¶ 61.

Similar to the posture agent in Gleichauf, which gathers information about the device's "configuration state," Ovadia uses "an authentication agent to determine the state of a platform environment" and generate an "integrity measurement." Ex.1005, 3:8, 12:21-31; Ex.1006, 4:40-43, 14:1-6; Fig. 8. Ovadia's integrity measurement is stored in the trusted platform module. Ex.1006, 13:61-63, Fig. 8. The integrity measurement is then provided to an authentication server as part of authentication data in response to an authentication challenge, which is analogous to Gleichauf's sending the posture credentials of a device to a policy server in response to requests to authenticate the device. Ex.1006, 4:43-45, 13:61-63, Fig. 8; Ex.1005, 10:63-11:3; Ex.1003, ¶ 62. Ovadia's integrity measurement is "digitally signed with appropriate keys" before it is sent to the authentication server. Ex.1006, 13:63-64, Fig. 8; Ex.1003, ¶ 62. A POSITA would have understood that Ovadia's trusted platform module generates and sends the integrity measurement because the integrity measurements are digitally signed with an Attestation Integrity Key (AIK) and "AIKs are only permitted to sign data generated by a TPM." Ex.1006, 14:9, 5:35-36; Ex.1003, ¶ 63. It would have been obvious to a POSITA to implement Gleichauf's posture agent with trusted platform module functionality, e.g., the ability to store, provide, and digitally sign integrity measurements, as taught in Ovadia, to provide the greater security assurances

available with digital signatures and limited-use integrity keys. Ex.1003, ¶ 63.

Both references also describe providing a message with an explanation to the user of the device if the posture credentials or integrity measurement is not accepted. Ex.1005, 4:50-67; Ex.1006, 16:62-65; Ex.1003, ¶ 64. The analogous architectures of Gleichauf's and Ovadia's respective systems—together with the fact that they both solve similar problems within the same field of network access authentication—would have provided a POSITA with a reasonable expectation of success in combining their disclosures. Ex.1003, ¶ 64. The predictability of their combination is also consistent with, and supported by, Gleichauf's and Ovadia's mutual acknowledgements that a POSITA would have had the skills to make "various changes in form and details" to their described embodiments. Ex.1005, 27:24-29; Ex.1006, 18:64-19:4; Ex.1003, ¶ 64.

Petitioner's proposed combinations permit but do not require physical incorporation of elements from Ovadia into Gleichauf. *See In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012); *In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985); Ex.1003, ¶ 65.

5. Reasons to Combine Gleichauf, Ovadia, and Lewis

A POSITA 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. Ex.1005, 3:4-9; Ex.1006, 1:8-11; Ex.1007, 4:7-9; Ex.1003, ¶ 66. A POSITA would have been motivated to combine the teachings of Gleichauf, Ovadia, and Lewis for multiple reasons and doing so would have been within the POSITA's skillset. Ex.1003, ¶ 67. The combination would have been obvious because it uses the known technique of redirection of device traffic to a quarantine server that serves a webpage to the device, as in Lewis, to improve a similar method of traffic redirection, as in Gleichauf, in the same way. Ex.1003, ¶ 67.

The combination would also 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, yielding predictable results. Ex.1003, ¶ 68. A POSITA would have known that serving a webpage with remediation instructions to a quarantined device from a quarantine server would beneficially provide information to the user while simultaneously preventing the device from accessing protected network resources. Ex.1007, 10:61-66, 13:63-14:1; Ex.1003, ¶ 68. Lewis's quarantine webpage would also be advantageous to Gleichauf's or Ovadia's notification message. Ex.1003, ¶ 68. Redirection to Lewis's quarantine server would be triggered by the user opening a browser and attempting to access network resources. Ex.1007, 10:63-66; Ex.1003, ¶ 68. The webpage served by the

quarantine server would be displayed in the browser that the user already has opened, which would advantageously avoid necessitating additional software components running on the device to receive and display the notification message to the user. Ex.1005, 4:56-60; Ex.1006, 16:62-65; Ex.1003, ¶ 68.

Serving 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. Ex.1003, ¶ 69. A user attempting to access the network from a fixed location (e.g., an office) may have time to proceed with remediation. Ex.1003, ¶ 69. In this instance, the webpage would direct the user to a remediation server that can resolve the security issues per Gleichauf. Ex.1005, 5:4-11; Ex.1003, ¶ 69. A user that does not have the time to remediate security issues (e.g., a user attempting access from an airport terminal) may opt to terminate the connection attempt. Ex.1003, ¶ 69. A POSITA would have understood the benefits of giving the user the option to choose their desired course of action. Ex.1003, ¶ 69.

A POSITA would have had a reasonable expectation of success in combining the teachings of Gleichauf and Ovadia with Lewis. Ex.1003, ¶ 70. As explained, Gleichauf's policy server sends a notification message to a quarantined device with information and remediation instructions. Ex.1005, 5:4-11. Put differently, the policy server identifies whether a device is to be quarantined and what actions should be taken to remediate the security issue before the device is

allowed access to the network. Ex.1005, 7:3-8, 4:60-63. A POSITA 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. Ex.1003, ¶ 70.

Petitioner's proposed combinations permit but do not require physical incorporation of elements from Lewis and Ovadia into Gleichauf. *See In re Mouttet*, 686 F.3d at 1332; *In re Etter*, 756 F.2d at 859; Ex.1003, ¶ 71.

6. Claim 1

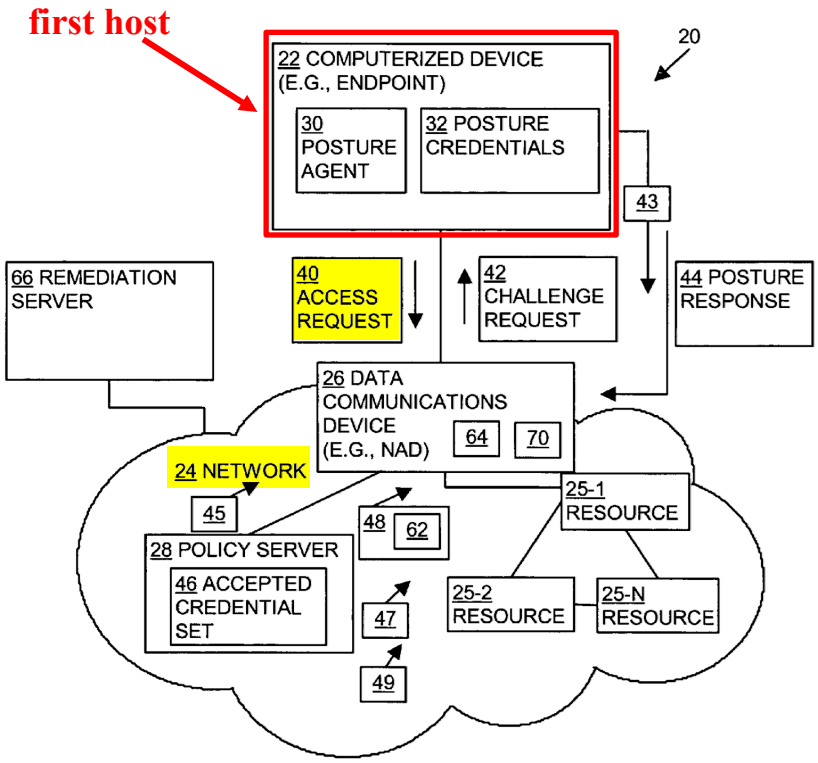
[1.0] ***A method for protecting a network, comprising:***

Gleichauf discloses a "computer-implemented **method** to control access to resources in a network." Ex.1005, 27:61-62; Ex.1003, ¶¶ 72-74. 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. Ex.1005, 5:55-60, 7:56-61, 8:16-31, 12:57-67; Ex.1003, ¶ 73. As explained below, the combination of Gleichauf, Ovadia, and Lewis renders obvious a method "*comprising*" the claimed steps.

[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***

First, Gleichauf describes a "computerized device, such as a personal computer attempting to communicate with restricted resources in the network."

Ex.1005, 3:50-56; Ex.1005, 8:1-4; Ex.1003, ¶¶ 75-76. Figure 1 of Gleichauf illustrates the computerized device sending an access request to the network ("*attempting to connect to a protected network*"):



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶ 80.

Gleichauf's computerized device is a *first host*, and, since they are protected by access control measures, the restricted network resources are part of a *protected network*. Ex.1003, ¶ 77. The access request, packet transmission, and attempt to access the restricted network resources show that the device has *connected* or *is attempting to connect* to the network. Ex.1003, ¶ 77.

Second, Gleichauf's policy server *detects an insecure condition* in the

computerized device. Ex.1003, ¶ 78. The device's communication attempt triggers a "posture based challenge-response" exchange where the device transmits its posture credentials to the network. Ex.1005, 11:29-32. The posture credentials contain "critical security information" including information about the "particular virus software and virus definition versions" installed on the device. Ex.1005, 3:36-45. The policy server analyzes these posture credentials and *detects* the absence "of an anti-virus application (e.g., or an up-to-date anti-virus application or virus definition file)." Ex.1005, 14:16-34; Ex.1003, ¶ 78. Devices that "are not configured with anti-virus or up-to-date anti-virus applications" are considered "vulnerable" because "network resources [may] become 'infected' with malware carried by the 'vulnerable' [computerized] user device 22." Ex.1005, 22:38-59, 11:58-12:13. A device would also be vulnerable to any malware that might be transmitted by network resources. Ex.1005, 1:10-14, 8:52-56. Thus, absence of an anti-virus application or up-to-date anti-virus application is an example of an *insecure condition*. Ex.1003, ¶ 78. Gleichauf also describes other examples of a potential *insecure condition*, such as "the version of operating systems used by the user device 22 or the presence of updated 'patches' associated with the operating systems" and "when was the last time a local antivirus scan was executed." Ex.1005, 1:65-2:3, 8:65-9:1, 3:36-45, 31:1-7; Ex.1003, ¶ 79. Gleichauf explains that there may be "known vulnerabilities in the device operating system, resident

applications, associated security programs, and their respective configurations." Ex.1005, 1:65-2:3. Additional examples of a potential *insecure condition* are discussed *infra* at [1.4] in relation to the *attestation of cleanliness*.

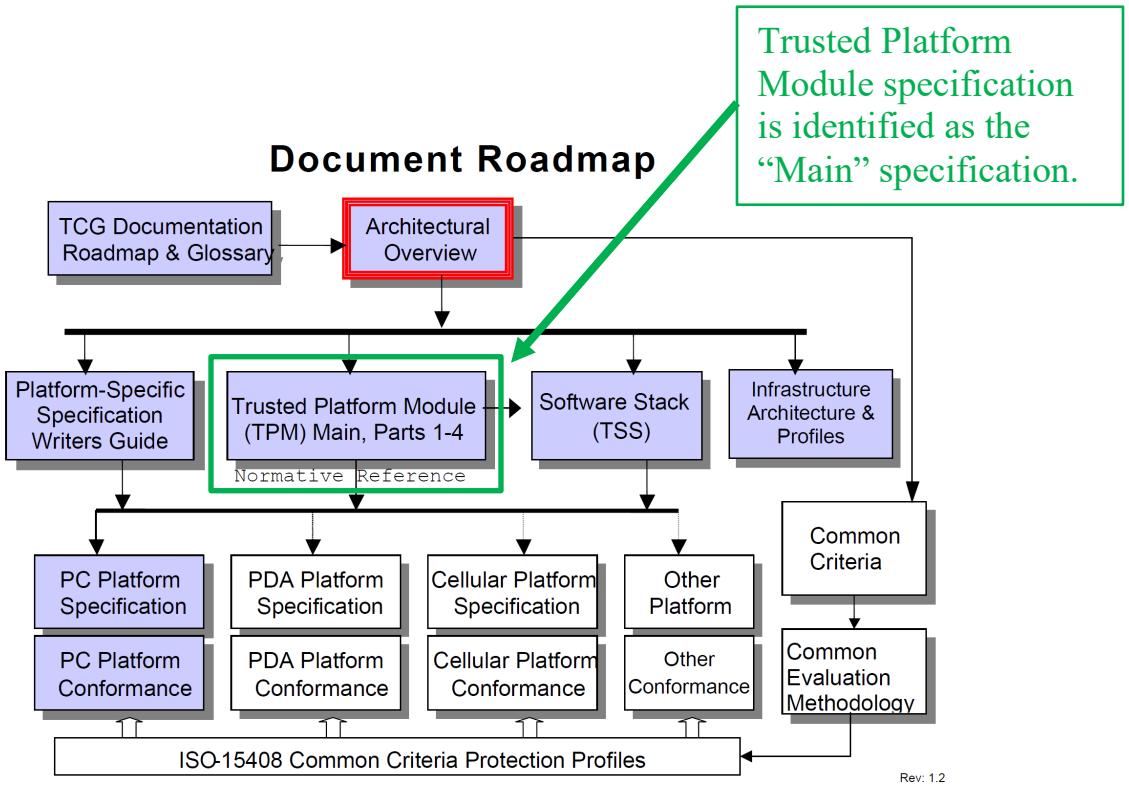
By gathering information relating to a computerized device's vulnerabilities—such as the presence of up-to-date anti-virus application and operating system patches or when an anti-virus scan was last run—Gleichauf renders obvious *detecting an insecure condition*. Ex.1003, ¶¶ 78, 81.

[1.2] ***contacting a trusted computing base associated with a trusted platform module within the first host,***

First, Gleichauf's computerized device includes a "posture agent" and one or more "posture plug-ins" installed on the device that collect information about the device's security posture. Ex.1005, 3:9-16; Ex.1003, ¶¶ 82-83. The posture agent accesses information collected by each plug-in using an API implemented by each plug-in manufacturer and prepares posture credentials that it transmits to the policy server for analysis and access control. Ex.1005, 9:24-39; Ex.1003, ¶¶ 84-85. Gleichauf's posture agent is "embodied as a software or hardware application." Ex.1005, 9:29-39. Since the posture credentials are used to secure the restricted resources, a POSITA would have understood that the combined functionality of the posture agent and plug-ins is part of the mechanism that provides such security. Ex.1003, ¶ 86. Thus, the combined functionality of the posture agent and plug-ins

is a *trusted computing base*. Ex.1003, ¶ 86; *see also supra* § VII.A.

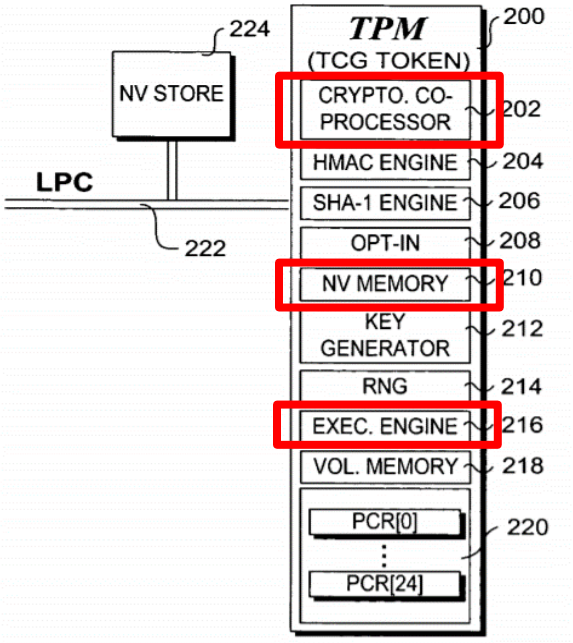
Second, Ovadia discloses a security apparatus that employs a trusted platform module implementing the Trusted Computing Group "main specification (Version 1.2, October 2003…)." Ex.1006, 4:16-47. The main specification from TCG is the Trusted Platform Module Main Specification (Ex.1003, ¶ 87):



Ex.1012, iv (annotated); Ex.1013; Ex.1003, ¶ 87.

Ovadia's trusted platform module implements the Trusted Platform Module main specification from the TCG and includes a "cryptographic co-processor," "non-volatile (NV) memory," and an "execution engine." Ex.1006, 4:46-55, Fig. 2; Ex.1003, ¶ 88. Since Ovadia's trusted platform module implements the Trusted

Platform Module main specification, it would have been obvious to a POSITA that the non-volatile memory stores cryptographic keys because that is how it is described in the main specification. Ex.1013, 19; Ex.1012, 19; Ex.1003, ¶ 88.



Ex.1006, Fig. 2 (annotated); Ex.1003, ¶ 88.

Therefore, Ovadia's trusted platform module is a *trusted platform module* as claimed. Ex.1003, ¶ 89; *see supra* § VII.B. Ovadia's trusted platform module "may be embodied as a hardware device (most common) or via software." Ex.1006, 4:24-26. Like Gleichauf's posture agent, Ovadia's trusted platform module is used "to verify [that] a current configuration of a subscriber station platform is an authorized configuration." Ex.1006, Abstract; Ex.1003, ¶ 89. The configuration (called the integrity measurement) including information about the subscriber station, including the "current measurement of the firmware and/or software" of

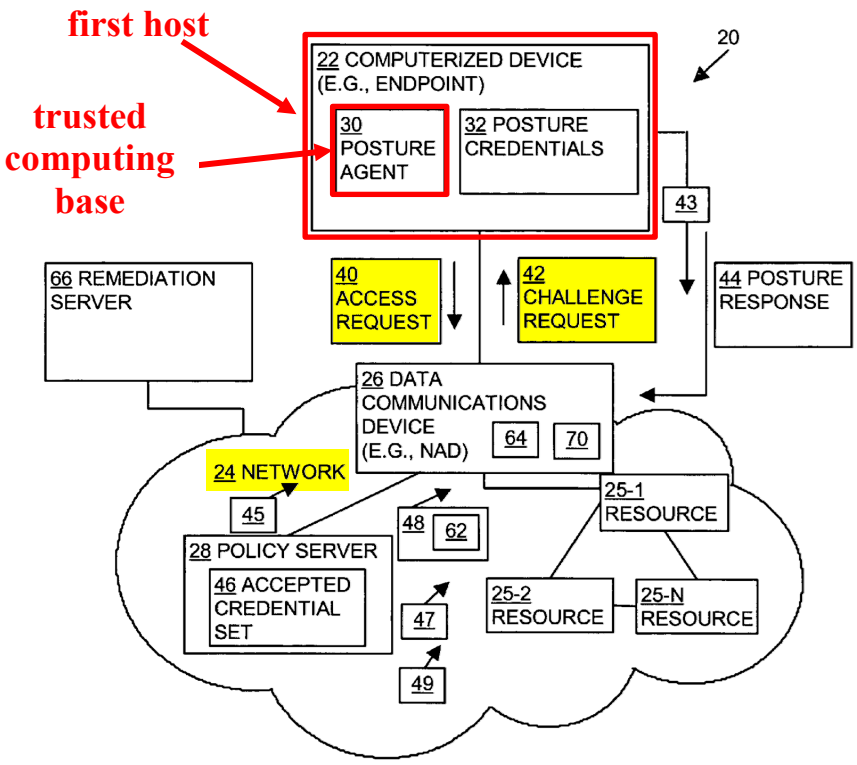
the station. Ex.1006, 13:57-14:12; Ex.1003, ¶ 89.

As described in more detail in Section IX.C.4, a POSITA would have been motivated to combine the teachings of Gleichauf and Ovadia and doing so would have been within the POSITA's skillset. Ex.1003, ¶ 93. A POSITA would have appreciated the value in implementing Gleichauf's posture agent with trusted platform module functionality. Ex.1003, ¶ 93. The TCG, which prepares the TCG specification discussed above, is "an **industry consortium** concerned with platform and network security." Ex.1006, 4:31-32. The TCG specification is a "**platform-independent industry specification** that covers trust in computing platforms" as well as how to implement and use trusted platform modules. Ex.1006, 4:32-35, 4:22-24. Implementing Gleichauf's posture agent with trusted platform module functionality would provide consistency among posture credentials generated by such posture agents operating on various computerized devices. Ex.1003, ¶ 93. On the device side, a posture agent implemented with trusted platform module functionality would operate consistent with the TCG specification, regardless of the device it is running on, and operation of such trusted platform modules would be consistent throughout the adopting industry. Ex.1003, ¶ 93. On the network side, a policy server receiving Gleichauf's posture credentials would process them more quickly and with more confidence that adequate information is provided. Ex.1003, ¶ 93. Indeed, the policy server would

be able to process all received posture credentials in substantially the same way because such credentials would have been gathered in substantially the same way. Ex.1003, ¶ 93. In the combination, Gleichauf's posture agent would be implemented with trusted platform module functionality, i.e., a *trusted platform module,* per Ovadia. Ex.1003, ¶ 93. For example, one obvious way to implement Gleichauf's posture agent with trusted platform module functionality would be for the posture agent software to be executed by the execution engine in Ovadia's trusted platform module. Ex.1003, ¶ 94; Ex.1006, Fig. 2. The 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. Ex.1005, 9:24-28; Ex.1003, ¶ 94. With the posture agent executing in the trusted platform module execution engine, the information collected by the posture agent would be "data generated by a TPM" and thus eligible for digital signature under the Trusted Platform Module main specification. Ex.1006, 5:36; Ex.1003, ¶ 94. As another example implementation of Gleichauf's posture agent with trusted platform module functionality, the posture agent software would simply be integrated with a software-implemented trusted platform module. Ex.1003, ¶ 94; *see* Ex.1006, 4:24-26 ("TPM functionality may be embodied… via software."). With the posture agent (part of the *trusted*

computing base) executing on the TPM hardware or integrated with the TPM software, the functionality of the posture agent and posture plug-ins would be *associated with a trusted platform module*. Ex.1003, ¶ 94.

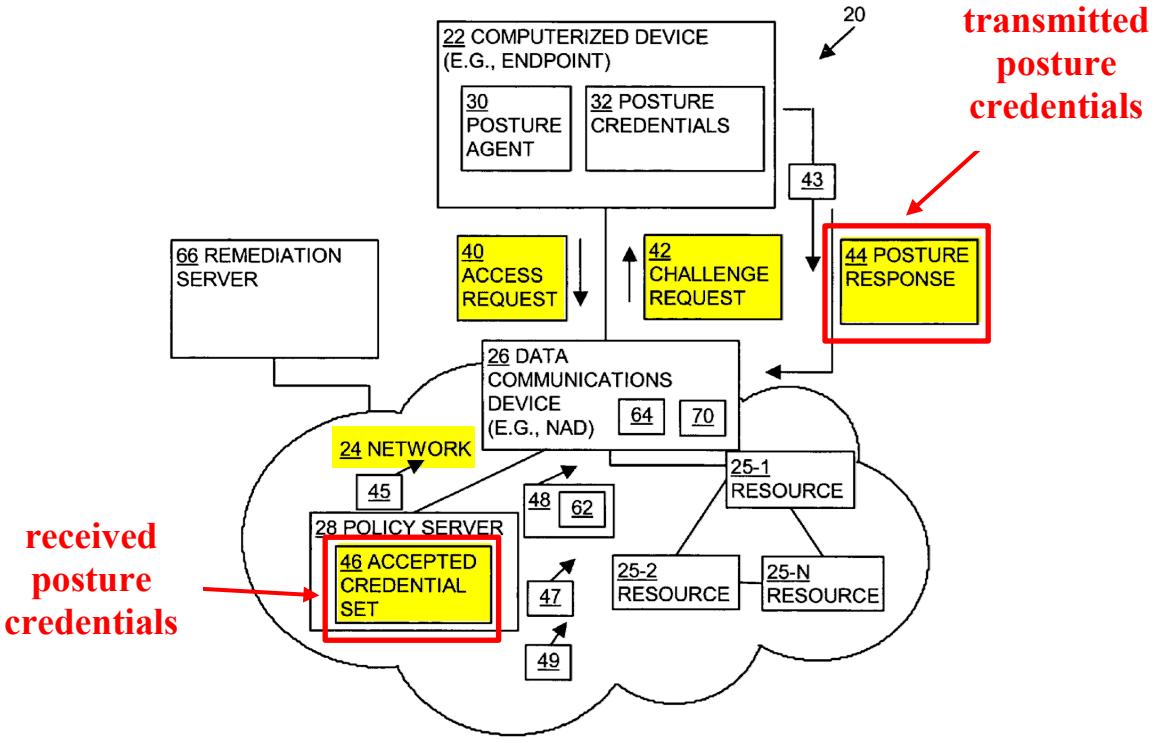
Third, Gleichauf's policy server *contacts* the computerized device's posture agent, which prompts the posture agent to collect the device's posture credentials from the posture plug-ins. Ex.1005, 4:7-11, 3:28-36; Ex.1003, ¶ 90. Gleichauf's Figure 1, below, shows the posture agent *within* the device. Ex.1003, ¶ 91. It would have been obvious to a POSITA that the *trusted platform module* would likewise be *within* the device. Ex.1003, ¶¶ 92, 95.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶ 91.

[1.3] ***receiving a response, and***

Gleichauf's posture agent responds to the policy server's request by collecting the computerized device's posture credentials from the one or more posture plug-ins and transmitting the credentials in a posture response to the policy server. Ex.1005, 3:28-36, 4:11-15; Ex.1003, ¶¶ 96-97. Gleichauf's Figure 1 illustrates the transmission and reception of posture credentials:



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶ 98.

Thus, the policy server "*receiv[es] a response*" to its request for the posture credentials. Ex.1003, ¶¶ 98-99.

[1.4] ***determining whether the response includes a valid digitally signed attestation of cleanliness,***

First, as discussed at [1.3], Gleichauf's posture response includes posture credentials. Ex.1003, ¶¶ 100-101. 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, each individually and collectively providing an *attestation of cleanliness*. Ex.1005, 3:36-49; Ex.1003, ¶ 101.

Second, the policy server analyzes and "validate[s] the posture credentials" (i.e., "*determining whether the response includes a valid … attestation of cleanliness*"). Ex.1005, 10:30-33; Ex.1003, ¶ 102. For example, the policy server checks for (i.e., "*determin[es]*") the presence of an anti-virus application. Ex.1005, 10:30-33; Ex.1003, ¶ 102. If a current anti-virus is present, the computerized device will be allowed to access the network resources, which demonstrates that the policy server deemed the response to include "*a valid … attestation of cleanliness*." Ex.1005, 11:45-58; Ex.1003, ¶¶ 103-104. If a current anti-virus is absent, the device's access to the network will be restricted, which demonstrates that the policy server deemed the response to lack "*a valid … attestation of cleanliness*." Ex.1005, 11:58-67; Ex.1003, ¶ 104.

Third, the posture agent "securely transmit[s]" posture credentials to the policy server. Ex.1005, 11:3-12; Ex.1003, ¶ 105.

Fourth, Ovadia provides further details about secure transmission of a device's configuration information for the purpose of requesting access to a network. Ex.1003, ¶ 106. Like the device in Gleichauf, Ovadia's subscriber station seeking network access uses its trusted platform module to respond to an authentication request by taking a "current measurement of the firmware and/or software configuration" and uses this as a "current integrity measurement." Ex.1006, 14:1-6; Ex.1003, ¶ 106. The integrity measurement is stored in the trusted platform module. Ex.1006, 13:61-63, Fig. 8; Ex.1003, ¶ 106. The integrity measurement is then used to produce a value that is "**digitally signed** with the SS's [subscriber station's] AIK [Attestation Integrity Key] private key, and sent to the AS [Authentication Server]." Ex.1006, 14:6-10; Ex.1003, ¶ 106. The subscriber station "is authenticated" and allowed access to the network if the integrity measurement is acceptable and "the digital signature is authentic." Ex.1006, 14:13-23, 16:66-17:6; Ex.1003, ¶ 106.

As described in more detail in Section IX.C.4., a POSITA would have been motivated to combine the teachings of Gleichauf and Ovadia and would have had the skills to do so. Ex.1003, ¶ 107. A POSITA would have understood that Ovadia's digital signature decreases the risk of accepting credentials that have been

altered by a malicious actor. Ex.1003, ¶ 107. As discussed at [1.2], in the combination, Gleichauf's posture credentials would be prepared by a posture agent implemented with trusted platform module functionality (as taught by Ovadia). Ex.1003, ¶ 107. A POSITA would have recognized that digitally signing Gleichauf's posture credentials (as taught by Ovadia) would provide a mechanism for Gleichauf's policy server (which evaluates those credentials) to be assured that the posture credentials have not been forged or tampered with. Ex.1003, ¶ 107. Ovadia explains that a device's integrity measurements (*e.g.*, posture credentials) are digitally signed with an Attestation Integrity Key (AIK), and that "AIKs are only permitted to sign data generated by a TPM." Ex.1006, 14:9, 5:35-36. Since only the trusted platform module (Gleichauf's posture agent implemented with trusted platform module functionality as discussed at [1.2]) could produce a valid digital signature and the trusted platform module would only sign posture credentials that it prepares itself, Gleichauf's policy server would have an assurance that posture credentials with a valid digital signature were authentic and correct. Ex.1003, ¶ 107. Put differently, the policy server would be assured that a virus or other malware on the computing device had not tampered with or forged the posture credentials to hide their presence on the computing device. Ex.1003, ¶ 107. It would have been obvious to a POSITA to apply Ovadia's teaching of digitally signing an integrity measurement of a device's configuration information

to Gleichauf's transmission of a device's posture credentials. Ex.1003, ¶ 107. In 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. Ex.1003, ¶¶ 107-109.

[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;***

First, the computerized device's posture credentials transmitted to the policy server (the "*attestation of cleanliness*" in [1.4]), contain information about "the last time a local antivirus scan was executed." Ex.1005, 3:41; Ex.1003, ¶¶ 110-111. Gleichauf expressly contemplates that failure to show "timely execution of the anti-virus application" is a failure to show cleanliness and results in restrictions on network access. Ex.1005, 22:38-47; Ex.1003, ¶ 111. It would have been obvious to a POSITA that the opposite showing would have the opposite effect. Ex.1003, ¶ 111. It would have been obvious for a posture credential that <u>does show</u> timely execution of the anti-virus to be treated as "*an attestation that the trusted computing base has ascertained that the first host is not infested*." Ex.1003, ¶ 111.

Second, the 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. Ex.1005, 3:36-49; Ex.1003, ¶ 112. Such information on software and patches is "*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*." Ex.1003, ¶ 113.

Gleichauf's posture agent prepares posture credentials from information it collects from posture plug-ins. Ex.1005, 3:9-16, 9:24-39; Ex.1003, ¶ 114. The posture agent "is also responsible for determining whether the posture of the computer device 22 has changed by learning of any changes from the posture plug-ins 32 through the posture plug-in API." Ex.1005, 9:50-53. The combined functionality of the posture agent and plug-ins, i.e., *trusted computing base*, thus "*ascertains*" the security posture of the device. Ex.1003, ¶ 114.

Third, Gleichauf's disclosures regarding the claimed *attestation* are substantially the same as those of the '705 patent specification. Ex.1003, ¶ 115. The '705 patent states:

> In some embodiments, the query for cleanliness (1302) may be responded to by anti-contagion software, such as antivirus software, with **assertions about the currency of a scan**, **such as the last time a scan was performed, or a version associated with a current anti-contagion software or definition file in use**, **wherein a sufficiently updated software and/or scan may act as a cleanliness assertion**.

Ex.1001, 14:12-19.

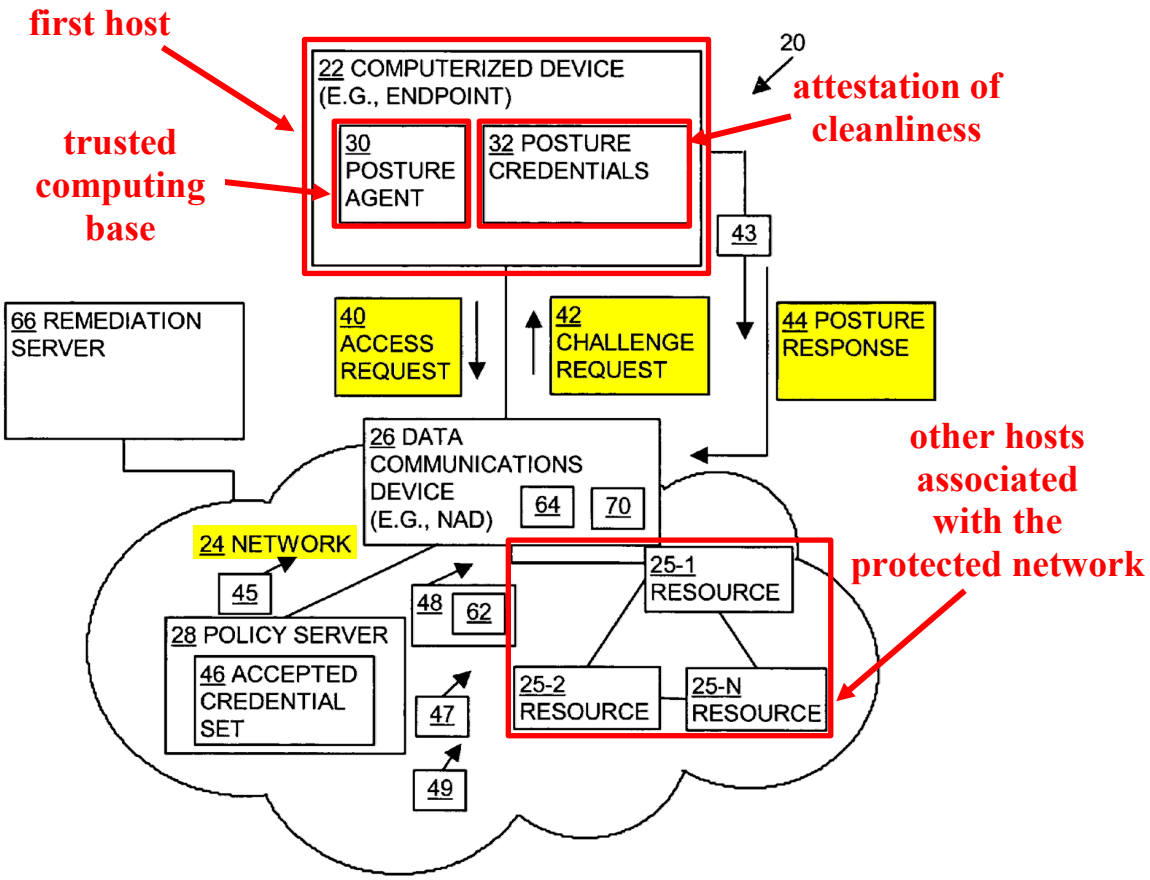
A POSITA would have understood Gleichauf's disclosure that posture credentials contain information about "the last time a local antivirus scan was executed," Ex.1005, 3:36-49, to equate to the '705 patent's note about the currency of a virus scan. Ex.1003, ¶¶ 116-118.

[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***

First, as explained in [1.4], Gleichauf's policy server reviews and validates posture credentials. Ex.1005, 10:30-33, 11:45-58; Ex.1003, ¶¶ 119-120. The policy server reviews the credentials for compliance with network admission policy, e.g., for the presence of an anti-virus application and/or the timeliness of the last virus scan. Ex.1005, 11:45-58, 22:38-42; Ex.1003, ¶ 120.

Second, Gleichauf describes using the posture credentials to determine whether to place the device in quarantine ("*quarantining the first host*"). Ex.1005, 4:24-27, 7:3-8; Ex.1003, ¶ 121. There are many reasons why a device might be placed into quarantine, including if it is found to be out of compliance with a network admission policy, Ex.1005, 4:50-56, if its behavior is found to be anomalous, suggesting that it may have been compromised, *see* Ex.1017, [0039], or if it is found to be infected with a virus or has been hijacked by an unauthorized entity. *See, e.g.*, Ex.1016, 4:8-14; Ex.1003, ¶ 122.

If the policy server "fails to detect the presence of, or a listing of, the anti-virus" application or definition in the device's posture credentials, the device is out of compliance with network admission policy (i.e., "*when it is determined that the response does not include a valid digitally signed attestation of cleanliness*"). Ex.1005, 11:59-60; Ex.1003, ¶ 123. Gleichauf provides that "devices that are out of compliance with admission requirements [are assigned] to a quarantine." Ex.1005, 4:50-56. 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." Ex.1005, 11:58-67; Ex.1003, ¶ 123.



Ex.1005, Fig. 1 (annotated); Ex.1003, ¶ 124.

Restricting or completely rejecting communications from the computerized device to network resources, e.g., resources 25-1 through 25-N, renders obvious *preventing the first host from sending data to one or more other hosts associated with the protected network.* Ex.1003, ¶¶ 124-125.

[1.7] ***receiving a service request sent by the first host,***

Gleichauf describes how the computerized device transmits an "access request" or "signaling request" in an "attempt to access the network resources within the network." Ex.1005, 3:50-56, 8:1-4; Ex.1003, ¶¶ 126-127. Such access

attempts can occur even after the device has been placed in quarantine. Ex.1005, 13:52-65; Ex.1003, ¶ 128. A request to access network resources is a "*service request*." Ex.1003, ¶ 129. The request is received and acted upon by a data communications device. Ex.1005, 3:60-65; Ex.1003, ¶ 129. Therefore, Gleichauf discloses "*receiving a service request sent by the first host*." Ex.1003, ¶ 130.

[1.8] ***serving a quarantine notification page to the first host when the service request comprises a web server request,***

First, as explained in [1.6], Gleichauf discloses that a computerized device that is out of compliance with network admission policy is quarantined. Ex.1005, 4:50-56; Ex.1003, ¶¶ 131-132. Communications from a quarantined device are restricted or rejected. Ex.1005, 11:58-67; Ex.1003, ¶ 132. Limited communications to certain destinations, such as a remediation server, may be permitted. Ex.1005, 14:62-66; Ex.1003, ¶ 132. For example, Gleichauf provides that "a redirect access instruction" is applied to "HTTP traffic." Ex.1005, 15:55-67; Ex.1003, ¶ 133. A POSITA 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. Ex.1003, ¶ 133. This is evidenced by the fact that Gleichauf refers to the redirection as a "URL Redirect." Ex.1005, 15:45, Ex.1003, ¶ 134. A POSITA would have been familiar with URL redirection, which was a common technique used to forcibly provide an alternative

response to a client's request for a webpage. Ex.1015, [0003]; Ex.1003, ¶ 134. This technique is commonly used to redirect a user's web browser to a login page at a hotel or airport. Ex.1008, 4:56-57; Ex.1009, [0044]; Ex.1003, ¶ 134.

Second, Gleichauf describes providing "one or more notification messages" for display to a user "indicating that the device has been quarantined." Ex.1005, 4:56-63, 21:1-12. The message may include "a link to a remediation server or the IP address of the remediation server." Ex.1005, 21:1-12; Ex.1003, ¶ 135.

Similar to Gleichauf, Lewis also discloses the use of redirection with a client device that is quarantined. Ex.1007, 4:24-31; Ex.1003, ¶ 136. When a user of the device opens a web browser (which would generate a "*service request compris[ing] a web server request*"), an initial domain name service (DNS) request from the device is redirected to a quarantine server. Ex.1007, 13:7-12; Ex.1003, ¶ 136. The quarantine server receives the DNS request and supplies a default webpage on the quarantine server to the device ("*serving a quarantine notification page to the first host*"). Ex.1007, 13:12-15; Ex.1003, ¶ 136. The webpage informs the user that the device "is in quarantine and corrective action must be taken." Ex.1007, 10:61-66; Ex.1003, ¶ 136.

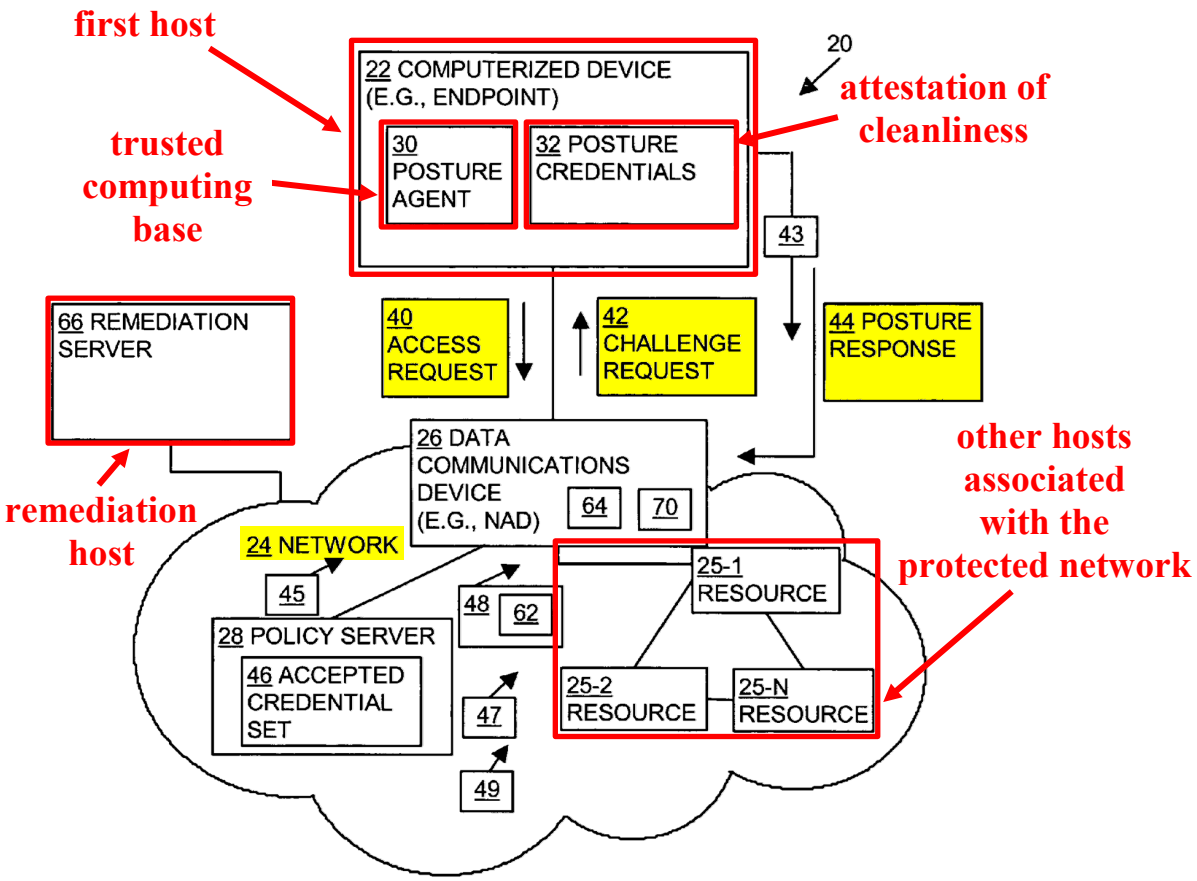
As described in more detail in Section IX.C.5, a POSITA would have been motivated to combine the teachings of Gleichauf, Ovadia, and Lewis and would have had the skill to do so. Ex.1003, ¶ 137. A POSITA would have appreciated the

security benefits of redirecting HTTP traffic from Gleichauf's device to a quarantine server (per Lewis), rather than a remediation server. Ex.1003, ¶ 137. The user of the quarantined device would receive information about the quarantine reasons via a webpage served by the quarantine server. Ex.1003, ¶ 137. The user would then have the option to either proceed with remediation or terminate the connection attempt. Ex.1003, ¶ 137. A user may elect to terminate the connection attempt, for example, if the user does not desire to have their device configuration changed or if the user is in a hurry and does not have time to remediate the identified issues. Ex.1003, ¶ 137. In the combination, HTTP traffic from a quarantined device would be redirected to a quarantine server as taught by Lewis. Ex.1003, ¶ 137. The quarantine server would then serve a webpage to the user, as taught by Lewis. Ex.1003, ¶ 137. The webpage would inform the user that the device is in quarantine (a "*quarantine notification page*"). Ex.1003, ¶¶ 137-138.

[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***

First, as discussed in [1.6], Gleichauf discloses that a computerized device that is out of compliance with network admission policy is quarantined and that communications from a quarantined device to protected resources in the network are restricted or rejected. Ex.1005, 4:50-56, 11:58-67; Ex.1003, ¶¶ 139-140.

Second, Gleichauf discloses a remediation server, shown in Fig. 1:



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

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" (a "*remediation host configured to provide data usable to remedy the insecure condition*"). Ex.1005, 5:4-11; Ex.1003, ¶ 141. HTTP traffic from the device directed to the remediation server is permitted while HTTP traffic directed to other destinations is redirected. Ex.1005, 14:62-66, 15:55-67; Ex.1003, ¶¶ 143-144.

It would have been obvious to a POSITA that HTTP traffic, such as that from Gleichauf's device, is usually preceded by a DNS query (i.e., "*and in the event the service request comprises a DNS query*"). Ex.1003, ¶ 145. The DNS query is used to obtain the internet protocol (IP) address of a named server, which would be a web server in the case of HTTP traffic. Ex.1003, ¶ 145. The device accesses a webpage by sending an HTTP request to the DNS-resolved IP address. Ex.1003, ¶ 145. These steps were commonly known and ubiquitously employed by web browsers in the prior art. Ex.1008, 5:49-63; Ex.1003, ¶ 145.

Third, Lewis describes a "hijack DNS component 421 for intercepting DNS queries from quarantined clients." Ex.1007, 11:15-17. The operation of the hijack DNS component is such that "[w]henever the client performs name resolution on any address, it will receive the IP [address] of QS [quarantine server]." Ex.1007, 14:22-23. As discussed at [1.8], Lewis's quarantine server (QS) provides a default webpage including a *quarantine notification*. Ex.1003, ¶ 146. The default webpage informs the user that the device is in quarantine and what corrective action must be taken for the device to be released from quarantine. Ex.1007, 10:61-66, 13:12-15. Thus, the IP address of Lewis's quarantine server is *an IP address of a quarantine server configured to serve the quarantine notification*. Ex.1003, ¶ 146.

Fourth, both Gleichauf and Lewis describe allowing a device placed in quarantine to communicate with one or more servers to fix the issues that led to it

being quarantined. Ex.1005, 5:4-13; Ex.1007, 13:12-17, 14:17-31; Ex.1003, ¶ 147. It would have been obvious to a POSITA that communications with such a remediation server would be preceded by a DNS request to resolve the remediation server's name into its IP address. Ex.1003, ¶ 147. This is because servers are frequently known and referred to by their domain name; however, the domain name cannot directly be used to address an IP packet to the server. Ex.1003, ¶ 147. The domain name must first be resolved, using DNS, into the server's IP address. Ex.1003, ¶ 147. The IP address is then specified as the destination for the IP packet. Ex.1003, ¶ 147. A POSITA would have been familiar with the use and operation of DNS. Ex.1003, ¶ 147.

Gleichauf describes allowing a device in quarantine to communicate with a remediation server "to upgrade or provide up-to-date patches to applications, such as anti-virus applications." Ex.1005, 16:14-16. Hence, it would have been obvious to a POSITA for a DNS server (responding to a request to resolve the IP address of the remediation server) to provide the correct IP address of the remediation server. Ex.1003, ¶ 148. It would have been obvious to a POSITA to adapt the functionality of a hijack DNS component, e.g., that of Lewis, to provide the correct IP address resolution to DNS queries relating to servers involved with device remediation. Ex.1003, ¶ 148. For all other queries, the hijack DNS component would function as described in Lewis by answering such DNS queries with the IP address of a

quarantine server. Ex.1003, ¶ 148. Thus, the combined teachings of Gleichauf and Lewis render obvious 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*. Ex.1003, ¶ 148.

As described in more detail in Section IX.C.5, a POSITA would have been motivated to combine the teachings of Gleichauf, Ovadia, and Lewis and would have had the skills to do so. Ex.1003, ¶ 149. A POSITA would have appreciated the need to ensure that a device placed into quarantine would be able to access the server necessary to remediate its security problem and thereafter gain full access to the network. Ex.1003, ¶ 149. Gleichauf contemplates identifying the remediation server by name since it provides "a link to a remediation server," which Gleichauf distinguishes from providing "the IP address of the remediation server." Ex.1005, 21:8-12; Ex.1003, ¶ 149. Gleichauf further explains that the "link" to the remediation server would be provided as a Universal Resource Link (URL). Ex.1005, 21:3-4; Ex.1003, ¶ 149. It was well known that a "URL typically includes the domain name of the provider of the identified resource." Ex.1011, 9:12-14; Ex.1003, ¶ 149. Thus, a POSITA would have found it obvious from Gleichauf's statement—that the remediation server is identified via URL—for the server to be identified to a quarantined device by its domain name. Ex.1003, ¶ 149. It would

have been obvious to a POSITA that the device needing to communicate with the remediation server would send a DNS query to obtain the IP address corresponding to the domain name of the server. Ex.1003, ¶ 149. In the combination, the DNS response provided to the device would include the correct IP address of the remediation server so that the device could resolve its security problems and exit quarantine (e.g., obtain update virus definitions). Ex.1003, ¶¶ 149-150.

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

As explained in [1.6], 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. Ex.1005, 4:50-56, 11:58-67; Ex.1003, ¶¶ 151-152. HTTP traffic from the device to a remediation server is permitted, however (i.e., "*permitting the first host to communicate with the remediation host*"). Ex.1005, 14:62-66; Ex.1003, ¶¶ 153-154.

7. Claim 2

[2.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 155.

[2.1] ***wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.***

First, as explained in [1.1], Gleichauf teaches that a policy server *detects an*

insecure condition in the computerized device by reviewing the device's posture credentials. Ex.1005, 3:36-45, 11:29-32, 11:58-12:3, 14:16-34, 22:39-59; Ex.1003, ¶¶ 156-157.

Second, the posture credentials include information about "the last time a local antivirus scan was executed," and a device that is "not configured with anti-virus or up-to-date anti-virus applications" is "vulnerable." Ex.1005, 3:36-49, 22:54-56; Ex.1003, ¶ 158. The failure to show "timely execution of the anti-virus application" is another indication that the device is "vulnerable" and in an *insecure condition*. Ex.1005, 22:38-59; Ex.1003, ¶ 158. A POSITA would have understood that checking for an anti-virus application and the recency of an anti-virus scan each constitute "*scanning for a vulnerability*." Ex.1003, ¶ 158.

The posture credentials also contain information about whether the device can "resist reception or transmission of… content (spam and/or data theft)." Ex.1005, 8:52-56; Ex.1003, ¶ 159. A POSITA would have understood that spam is a type of "*malicious data*" because it is unsolicited. Ex.1003, ¶ 159. A POSITA would also have understood that the device would be "*scanned*" to determine whether the device can resist reception or transmission of spam. Ex.1003, ¶ 159.

The posture credentials further include information about the presence or absence of an anti-virus software, recentness of an anti-virus definition, and the status of a firewall application. Ex.1005, 3:36-49, 8:62-65; Ex.1003, ¶ 160. A

POSITA would have understood that an anti-virus and intrusion prevent software (e.g., a firewall) are types of "*security software*" because they can detect and prevent virus and other security infestations. Ex.1003, ¶ 160. Reviewing the posture credentials for information about the presence or absence of anti-virus software or firewall application involves "*determining whether a security software is installed*." Ex.1003, ¶¶ 160-162.

8. Claim 3

[3.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 163.

[3.1] ***wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.***

First, as explained in [1.1], Gleichauf teaches that a policy server *detects an insecure condition* in the computerized device by reviewing posture credentials. Ex.1005, 3:36-45, 11:29-32, 11:58-12:3, 14:16-34, 22:39-59; Ex.1003, ¶¶ 164-165.

Second, the posture credentials contain information about "operating system patches [that] are installed within the computing system" (i.e., "*updates to an operating system*"). Ex.1005, 3:36-49; Ex.1003, ¶ 166. Gleichauf explains, and a POSITA would have known, that an outdated operating system may make the device "vulnerable" to network threats. Ex.1005, 1:65-2:3, 4:50-56; Ex.1003, ¶¶ 167-168. When the device is quarantined, the policy server can transmit a

notification message to the device that may "include a link to a remediation server" where the remediation server "is configured to upgrade or provide up-to-date patches to the operating system." Ex.1005, 21:8-12, 5:8-11; Ex.1003, ¶ 169. Once remediated, the device "should be admitted" into the network. Ex.1005, 5:11-13; Ex.1003, ¶ 169. A POSITA would have found it obvious from Gleichauf's description of quarantining devices with outdated operating systems and of providing operating system updates, to quarantine a device "*until an update to an operating system has been installed*." Ex.1003, ¶¶ 169-170.

9. Claim 5

[5.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 171.

[5.1] ***wherein permitting the first host to communicate with the remediation host includes:***

See analysis at [1.10]. Ex.1003, ¶ 172.

[5.2] ***detecting an outbound communication from the first host; and***

Gleichauf's quarantined device receives a notification message from the policy server "indicating that the device has been quarantined and needs to be remediated" and including "a link to a remediation server." Ex.1005, 21:5-12; Ex.1003, ¶¶ 173-174. The device responds to the message by activating the link and being directed to the remediation server. Ex.1005, 21:20-23; Ex.1003, ¶ 174.

A POSITA would have understood that the device activating the link directing it to the remediation server includes an "*outbound communication from the first host*" to the remediation server. Ex.1003, ¶ 175. Gleichauf explains that data communications device 26 "is configured to **detect attempted connections** to the network 24 by the user device." Ex.1005, 10:6-11, 12:57-67. A POSITA would have understood that directing the device to the remediation server—a server that is not part of the device—would be an "*outbound communication from the first host*." Ex.1003, ¶ 175. A POSITA would also have understood that the data communications device 26 would "*detect[]*" an outbound communication when it is applying access instructions that govern the device's permitted level of network access. Ex.1003, ¶¶ 176-177; Ex.1005, 13:52-65, 14:3-7, 14:20-34, 22:38-47.

[5.3] ***forwarding the outbound communication if it is addressed to the remediation host.***

As discussed in [5.2], Gleichauf discloses that communications from a quarantined device are restricted or rejected. Ex.1005, 22:38-47; Ex.1003, ¶¶ 178-179. A quarantined device is generally permitted to engage in HTTP communication with a remediation server. Ex.1005, 14:62-66; Ex.1003, ¶ 179. A POSITA would have understood that permitting HTTP traffic from a device to a remediation server, per Gleichauf, would entail the data communications device 26 "*forwarding the outbound communication if it is addressed to the remediation*

host." Ex.1003, ¶¶ 179-180.

10. Claim 6

[6.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 181.

[6.1] ***wherein preventing the first host from sending data to the one or more other hosts includes:***

See analysis at [1.6]. Ex.1003, ¶ 182.

[6.2] ***detecting an outbound communication from the first host; and***

See analysis at [5.2]. Ex.1003, ¶ 183.

[6.3] ***redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.***

First, Gleichauf restricts or rejects communications from a quarantined device. Ex.1005, 11:58-67; Ex.1003, ¶¶ 184-185. Gleichauf explains that communications are permitted "only to certain destination addresses, e.g., IP address of remediation server, **and only to certain protocols or ports**, e.g., HTTP traffic." Ex.1005, 14:62-66. A POSITA would have understood Gleichauf to teach that a quarantined device may be limited to communications with a remediation server using only HTTP (an "*approved service*"). Ex.1003, ¶ 185.

Second, as discussed in [1.9], Gleichauf discloses that HTTP traffic (an "*approved service*") from the device to a remediation server is permitted. Ex.1005, 14:62-66; Ex.1003, ¶ 186. However, HTTP traffic from the device to other

destinations ("*not addressed to a remediation host*") will be subject to a "**redirect** access instruction" that will "direct the computerized device 22 (e.g., HTTP traffic from the computerized device 22) to a remediation server." Ex.1005, 15:55-16:6; Ex.1003, ¶ 186. As discussed at [1.8]-[1.9], it would have been obvious to a POSITA, in view of Lewis, to *redirect* unauthorized access requests to a *quarantine server* that would inform the user of their device's quarantine status via a quarantine notification page. Ex.1007, 11:15-17, 14:22-23; Ex.1003, ¶¶ 186-187.

11. Claim 7

[7.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 188.

[7.1] ***wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.***

As explained in [1.6], Gleichauf discloses that a computerized device that is out of compliance with network admission policy is quarantined. Ex.1005, 4:50-56; Ex.1003, ¶¶ 189-190. Outbound communications from a quarantined device are not permitted to destinations that are not the remediation server. Ex.1005, 11:58-67, 14:62-66; Ex.1003, ¶ 190. It would have been obvious to a POSITA that inbound communications would be similarly subject to access restrictions. Ex.1003, ¶ 191. If outbound requests from the quarantined device are not permitted to non-remediation destinations, the quarantined device is effectively prevented

from receiving information that it would have received in response to such requests. Ex.1003, ¶ 191. Since Gleichauf teaches that a device in quarantine may only communicate with remediation-related servers, it would have been obvious to a POSITA that Gleichauf's system prevents the quarantined device from receiving information not related to remediation ("*preventing … from receiving via the protected network data not related to remediation of the insecure condition*"). Ex.1003, ¶ 191.

To the extent that this claim is interpreted as requiring the blocking of all non-remediation-related traffic from reaching the device, this restriction would have been obvious to a POSITA. Ex.1003, ¶ 192. Gleichauf is concerned with limiting or preventing the risk that network resources "receive or transmit malware" **from or to** "vulnerable computerized devices." Ex.1005, Abstract, 8:52-55; Ex.1003, ¶ 192. That is why vulnerable devices are quarantined in an "isolated … network segment" until the vulnerability has been remedied so that the device cannot receive such malware. Ex.1005, 4:25-26; Ex.1003, ¶ 192. It would thus have been obvious to a POSITA that a device in quarantine would be restricted from receiving data not related to remediation in the same way that the device is restricted from transmitting data to non-remediation servers. Ex.1003, ¶ 192. A POSITA would have had a reasonable expectation of success in restricting communications to or from a quarantined device because Gleichauf describes

allowing or preventing communications "between" the device and the network. Ex.1003, ¶¶ 192-193; Ex.1005, 14:3-7, 14:20-25.

12. Claim 8

[8.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 194.

[8.1] ***performed at an Internet service provider.***

Gleichauf's computerized device attempts to communicate using the network, where the network is "a computer network, such an enterprise network or the **Internet,** which includes the network resources 25, the data communications device 26, and the policy server 28." Ex.1005, 3:50-56, 9:57-64; Ex.1003, ¶¶ 195-196. Network resources 25 are "servers that contain content accessible by the . . . device." Ex.1005, 9:65-67; Ex.1003, ¶ 196.

A POSITA would have understood that the combination of the data communications device and policy server is an *Internet service provider* because the combination selectively provides access to the network, which Gleichauf explains is the Internet. Ex.1003, ¶ 197. The policy server determines whether to quarantine the device (by means of instructions to the data communications device) and protect the network. Ex.1005, 4:50-56, 10:30-33, 11:45-67; Ex.1003, ¶ 197. While in quarantine, the device is unable to communicate with network resources. Ex.1005, 11:58-67,14:62-66. A POSITA would have therefore appreciated that the

data communications device and policy server determine whether the device can access resources on the network, e.g., on the Internet. Ex.1003, ¶ 197. Thus, the data communications device and the policy server together operate to provide the device Internet access, which a POSITA would have understood to be the function of an "*Internet service provider*." Ex.1003, ¶¶ 197-198. Moreover, it would have been obvious for the data communications device and policy server to be owned by a company that provides Internet service.

13. Claim 9

[9.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 199.

[9.1] ***wherein the software component on the first host is an operating system.***

See analysis at [3.1]. Ex.1003, ¶ 200.

14. Claim 10

[10.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 201.

[10.1] ***wherein determining that the response does not include a valid digitally signed attestation of cleanliness includes determining that the software component on the first host is not sufficiently updated.***

See analysis at [1.4]. Ex.1003, ¶ 202. Gleichauf's computerized device's posture response includes posture credentials. Ex.1003, ¶ 202. The posture credentials contain information about the "particular **virus software and virus**

definition versions" installed on the device. Ex.1005, 3:36-49, 8:56-9:5. If the current anti-virus definition is not present, the device is quarantined and communications from it to the network will be restricted or completely rejected, showing that the response is deemed not to include "*a valid . . . attestation of cleanliness*." Ex.1005, 11:58-67; Ex.1003, ¶ 202.

15. Claim 11

[11.0] ***A method as recited in claim 1,***

See analysis at [1.0]-[1.10]. Ex.1003, ¶ 203.

[11.1] ***wherein determining that the software component on the first host is not sufficiently updated includes determining that a patch level associated with the software component on the first host is not sufficiently recent.***

The computerized device's posture credentials contain information about the "particular virus software and virus definition versions" installed on the device. Ex.1005, 3:36-49, 8:56-9:5; Ex.1003, ¶¶ 204-205. If a review of the posture credentials "fails to detect the presence of an anti-virus application (e.g., or **an up-to-date anti-virus application or virus definition file**)," the device will be quarantined. Ex.1005, 14:16-34; Ex.1003, ¶ 205. A POSITA would have understood that failure to detect an up-to-date anti-virus application or definition file indicates that the existing anti-virus application or definition file on the device "*is not sufficiently recent*." Ex.1003, ¶¶ 205-206.

16. Claim 12

[12.0] ***A system for protecting a network, comprising:***

Gleichauf teaches a "**robust network security architecture and system for controlling access to a network** depending on the configuration state or 'security posture' of a device when it attempts to connect to that network." Ex.1005, 3:4-9; Ex.1003, ¶¶ 207-208. Gleichauf's system, and specifically its policy server, protects the network by reducing the risk of the network becoming infected with malware or suffering a virus outbreak. Ex.1005, 8:16-31; Ex.1003, ¶ 208. Thus, Gleichauf discloses "*[a] system for protecting a network*." Ex.1003, ¶ 209. As explained below, the combination of Gleichauf, Ovadia, and Lewis renders obvious a system "*comprising*" the claimed steps.

[12.1] ***a processor configured to:***

As discussed in [1.0]-[1.10], Gleichauf's policy server operates to protect the network. Ex.1003, ¶¶ 210-211. The policy server "includes a controller 209 formed of a memory 210 and a **processor 212**." Ex.1005, 25:44-46; Ex.1003, ¶¶ 211-212.

[12.2]-[12.11] (elements recited in claim 12)

Elements [12.2]-[12.11] are substantively identical to the steps of claim 1 and are rendered obvious for the same reasons. Ex.1003, ¶¶ 213-222.

[12.12] ***a memory coupled to the processor and configured to provide instructions to the processor.***

As discussed in [12.1], Gleichauf's policy server operates to protect the

network. Ex.1003, ¶¶ 223-224. Gleichauf's policy server "includes a controller 209 formed of a **memory 210** and a processor 212." Ex.1005, 25:41-46; Ex.1003, ¶ 224. A POSITA would have understood that memory 210 is coupled to processor 212 because they are part of the same controller 209. Ex.1003, ¶ 224.

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." Ex.1005, 26:66-27:8; Ex.1003, ¶¶ 225-226.

17. Claims 13 and 15-18

Claims 13 and 15-18 depend from claim 12 and recite substantively identical limitations as claims 2, 7, and 9-11 that depend from claim 1. Accordingly, claims 13 and 15-18 are rendered obvious for the same reasons. Ex.1003, ¶¶ 227-236.

18. Claim 19

[19.0] ***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 for:***

Gleichauf 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" described throughout the reference. Ex.1005, 25:46-51, 3:4-9; Ex.1003, ¶¶ 237-238. A POSITA would have understood that Gleichauf's computer program product *comprises computer instructions*. Ex.1003, ¶ 238.

As described for claim 12, Gleichauf's policy server operates to protect the network and directs the operation of the data communications device 26. Ex.1003, ¶ 239. The policy server includes "*non-transitory computer readable medium*" in the form of memory 210 that stores "**logic instructions (e.g., software code) and/or data**" for operating the disclosed security architecture. Ex.1005, 26:66-27:8; Ex.1003, ¶ 239. Gleichauf's system protects the network by reducing the risk of the network becoming infected with malware or suffering a virus outbreak. Ex.1005, 8:16-31; Ex.1003, ¶¶ 240-241.

[19.1]-[19.10] (elements recited in claim 19)

Elements [19.1]-[19.10] are substantively identical to the steps of claim 1 and are rendered obvious for the same reasons. Ex.1003, ¶¶ 242-251.

X. DISCRETIONARY DENIAL IS INAPPROPRIATE

A. Discretionary Denial under 35 U.S.C. § 325(d) is Not Appropriate

The combinations of references presented in the grounds below have not previously been presented to the Office. Neither Gleichauf nor Ovadia were cited or considered by the Examiner during prosecution of the '705 patent. While Lewis

was before the Examiner, the relevant teachings of Lewis were never disputed by the applicants, nor was Lewis distinguished on the basis of the teachings relied upon in this petition. Ex.1002, 98-99, 73-74.

While the Examiner cited U.S. Patent Pub. No. 2005/0033987 to Yan for its description of trusted computing concepts (Ex.1002, 98-99), the applicants argued that Yan and the other cited art failed to disclose the claimed "*attestation.*" Ex.1002, 73-74. Yan bluntly states that it does not provide the claimed "*attestation that the trusted computing base has ascertained that the first host is not infested*":

> Attestation, however, only allows a remote party to ascertain what configuration was launched on a particular platform and establishes a session key for future interaction with that configuration on that particular platform. This does not provide trustworthiness in the usual sense because a software component could be buggy and produce incorrect results. Additionally, **attestation provides no information about the current state of the running system, such as a software component that has been** compromised by a buffer overflow attack, **infected by a virus,** replaced by a newer version of code, etc.

Ex.1021, [0062].

In contrast to the art considered by the Examiner, the combination of Gleichauf and Ovadia render obvious the claimed *attestation* feature, as discussed above at [1.4]-[1.5]. Accordingly, discretionary denial under 35 U.S.C. § 325(d) is not appropriate.

B. Discretionary Denial under the *Fintiv* Factors is Not Appropriate

The Board balances six factors in considering denial under § 314. *Apple Inc. v. Fintiv, Inc*., IPR2020-00019, Paper 11 (Mar. 20, 2020) (precedential). These factors strongly favor institution. The district court case is in its very early stages. Patent Owner filed its complaint on November 6, 2020. Ex.1018. Patent Owner provided its preliminary infringement contentions on February 5, 2021. Ex.1019, 4. Petitioner has since worked diligently to prepare this Petition, which is being filed well within the one-year timeframe allowed by Congress.

1. Whether Evidence Exists that a Stay May be Granted if a Proceeding is Instituted

If an IPR is instituted, a stay of the co-pending litigation would be appropriate. However, given that a motion to stay has not yet been filed, the Board should not infer or attempt to predict the outcome if such a motion is later filed. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative); *see also Dish Network L.L.C. v. Broadband iTV, Inc.*, IPR2020-01359, Paper 15 (Feb. 12, 2021) ("It would be improper to speculate, at this stage, what the Texas court might do regarding a motion to stay…"). Thus, this factor is neutral on discretionary denial.

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

The Agreed Scheduling Order proposes July 27, 2021 as the date for the *Markman* hearing and June 6, 2022 as the trial date. Ex.1022, 3-4. The expected date for a Final Written Decision in this case is Q3 2022.

This factor weighs against discretionary denial because the Petitioner has worked expeditiously to prepare and file this petition approximately one month after receiving Patent Owner's infringement contentions on February 5, 2021. Ex.1019, 4; *Fintiv*, Paper 11 at 11–12.

Furthermore, the current average time-to-trial for the district court hearing the co-pending litigation is over two years. Ex.1020 (showing W.D. Texas median time-to-trial for patent cases of 748 days); *In re Apple Inc.*, 979 F.3d 1332, 1350 (Fed. Cir. 2020). Moreover, Petitioner notes that "a court's general ability to set a fast-paced schedule is not particularly relevant… where, like here, the forum itself has not historically resolved cases so quickly." *In re Apple Inc.*, 979 F.3d 1332, 1344 (Fed. Cir. 2020).

As such, this factor weighs against discretionary denial. *See Sand Revolution II, LLC v. Continental Intermodal Grp.—Trucking LLC*, IPR2020-01393, Paper 24 (June 16, 2020) (panel granting institution on rehearing based on finding that uncertainty over district court's trial date weighed against discretionary denial).

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

The co-pending litigation is in its early stages, and the investment in it has been minimal. The 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. Ex.1022, 3; *see PEAG LLC v. Varta Microbattery GMBH*, IPR2020-01214, Paper 8 at 17 (Jan. 6, 2021) (finding that since no claim construction hearing had yet been held and discovery was not completed, the little investment in the parallel proceeding weighed against discretionary denial).

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

There is no overlap of prior art issues at this time. Preliminary invalidity contentions are not due until April 2, 2021. Instituting a proceeding will allow the Board to address the asserted prior art, and the issues will be narrowed in the co-pending litigation due to the estoppel provisions of 35 U.S.C. § 315(e)(2).

Moreover, there will be no overlap of prior art issues. If 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. This factor weighs against discretionary denial.

As noted above, Petitioner is challenging claims not asserted in the co-pending litigation. Thus, there will be no overlap of prior art issues with regard to those claims at any time.

5. Whether the Petitioner and the Defendant in the Parallel Proceeding are the Same Party

Petitioner is a defendant in the litigation. Ex.1018. That is true of most Petitioners in IPR proceedings. While the *Fintiv* case indicates that a difference between the district court defendant and the petitioner may weigh against discretionary denial, nothing within the *Fintiv* case suggests that the same party between the proceedings weighs in favor of discretionary denial. Accordingly, this factor is neutral and should not be a basis for denying institution.

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

As discussed in detail above, the prior art presented in this Petition renders the Challenged Claims unpatentable as obvious. The merits of Petitioner's arguments are strong, and this factor weighs against discretionary denial.

As such, because the *Fintiv* factors are either neutral or weigh against discretionary denial. Because this Petition was filed approximately eight months before the statutory bar date, institution should not be denied on discretionary factors.

C. Discretionary Denial under *General Plastic* is Not Appropriate

The '705 patent has not been challenged in any prior IPR petition, so none of *General Plastic* discretionary institution factors apply to this Petition. *See General Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 16 (Sept. 6, 2016) (Section II.B.4.i. precedential).

XI. CONCLUSION

Petitioner has established a reasonable likelihood that the Challenged Claims are unpatentable.

Respectfully submitted,

Dated: March 15, 2021
HAYNES AND BOONE, LLP
2323 Victory Avenue, Suite 700
Dallas, Texas 75219
Customer No. 27683

/Theodore M. Foster/
Theodore M. Foster
Lead Counsel for Petitioner
Registration No. 57,456

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,062. Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: March 15, 2021

/Theodore M. Foster/
Theodore M. Foster
Lead Counsel for Petitioner
Registration No. 57,456

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

Date of service	March 15, 2021
Manner of service	FEDERAL EXPRESS
Documents served	Petition for *Inter Partes* Review Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S. 8,234,705; Petitioner's Exhibit List; Exhibits 1001-1023; and Petitioner's Power of Attorney.
Persons served	BrainSpark Associates, LLC 528 South Meadows Drive Chandler, AZ 85224

/Theodore M. Foster/
Theodore M. Foster
Lead Counsel for Petitioner
Registration No. 57,456