

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CITRIX SYSTEMS, INC.

Petitioners

v.

K.MIZRA LLC,

Patent Owner

Inter Partes Review No.: IPR2025-01468

**DECLARATION OF DR. CLAY SHIELDS IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 8,234,705**

I hereby declare under penalty of perjury under the laws of the United States of America that the following is true and correct, and that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I understand that willful false statements are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code.

Date: 8/28/2025



Clay Shields, Ph.D.

TABLE OF CONTENTS

	Page
I. BACKGROUND AND QUALIFICATIONS	1
A. Qualifications	1
B. Technology Background	4
C. Materials Reviewed	5
II. RELEVANT PATENT LAW AND LEGAL STANDARDS.....	6
A. Legal Standards for Anticipation	6
B. Legal Standards for Obviousness.....	6
III. THE '705 PATENT	11
A. Overview of the '705 Patent.....	11
B. File History of the '705 Patent	12
C. Person of Ordinary Skill in the Art	12
D. Claim Construction.....	14
1. “trusted computing base” (claims 1, 12, 19).....	14
2. “trusted platform module” (claims 1, 12, 19)	14
IV. GROUND 1: CLAIMS 1-19 ARE OBVIOUS OVER GLEICHAUF IN VIEW OF OVADIA, AND LEWIS.....	15
A. Overview of Gleichauf	15
B. Overview of Ovadia	17
C. Overview of Lewis	19
D. Motivation to Combine Gleichauf and Ovadia	21
E. Motivation to Combine Gleichauf, Ovadia, and Lewis	26
F. Claim 1	30
1. [1pre] A method for protecting a network, comprising:.....	30
2. [1a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,.....	30

3. [1b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,33
4. [1c] [wherein detecting the insecure condition includes ...] receiving a response, and.....39
5. [1d] [wherein detecting the insecure condition includes ...] determining whether the response includes a valid digitally signed attestation of cleanliness,40
6. [1e] 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;.....44
7. [1f] 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,46
8. [1g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,.....48
9. [1h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and49
10. [1i] 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.....51

11.	[1j] permitting the first host to communicate with the remediation host.....	56
G.	Claim 2 - A method as recited in claim 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.	56
H.	Claim 3 – A method as recited in claim 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.....	58
I.	Claim 4 - A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.....	59
J.	Claim 5	60
1.	[5pre] A method as recited in claim 1, wherein permitting the first host to communicate with the remediation host includes:	60
2.	[5a] detecting an outbound communication from the first host; and	61
3.	[5b] forwarding the outbound communication if it is addressed to the remediation host.....	62
K.	Claim 6	62
1.	[6pre] A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:	62
2.	[6a] detecting an outbound communication from the first host; and	62
3.	[6b] 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.....	63

L.	Claim 7 – A method as recited in claim 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.	64
M.	Claim 8 - A method as recited in claim 1, performed at an Internet service provider.....	66
N.	Claim 9 - A method as recited in claim 1, wherein the software component on the first host is an operating system.	68
O.	Claim 10 - A method as recited in claim 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.	68
P.	Claim 11 - A method as recited in claim 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.	69
Q.	Claim 12	70
1.	[12pre] A system for protecting a network, comprising:.....	70
2.	[12a] a processor configured to:	70
3.	[12b] detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,.....	71
4.	[12c] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,	71
5.	[12d] [wherein detecting the insecure condition includes ...] receiving a response, and.....	71
6.	[12e] [wherein detecting the insecure condition includes ...] determining whether the response includes a valid digitally signed attestation of cleanliness,	71

7. [12f] 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;.....71
8. [12g] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,72
9. [12h] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,.....72
10. [12i] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and72
11. [12j] 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.....72
12. [12k] permit the first host to communicate with the remediation host; and73
13. [12l] a memory coupled to the processor and configured to provide instructions to the processor.73

R.	Claim 13 - A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.....	73
S.	Claim 14 - A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.....	74
T.	Claim 15 - A system as recited in claim 12, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.....	74
U.	Claim 16 - A system as recited in claim 12, wherein the software component on the first host is an operating system.	75
V.	Claim 17 - A system as recited in claim 12, 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.	75
W.	Claim 18 - A system as recited in claim 17, 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.....	76
X.	Claim 19	76
1.	[19pre] 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:	76
2.	[19a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,.....	77

3. [19b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,77
4. [19c] [wherein detecting the insecure condition includes...] receiving a response, and78
5. [19d] [wherein detecting the insecure condition includes...] determining whether the response includes a valid digitally signed attestation of cleanliness,78
6. [19e] 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;.....78
7. [19f] 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,78
8. [19g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,.....79
9. [19h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and.....79
10. [19i] 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.....79

11.	[19j] permitting the first host to communicate with the remediation host.....	79
V.	GROUND 2: CLAIMS 1-19 ARE OBVIOUS OVER FREUND IN VIEW OF BALL AND DANFORTH.....	80
A.	Overview of Freund.....	80
B.	Overview of Ball	83
C.	Overview of Danforth	86
D.	Motivation to Combine	89
1.	Freund and Ball.....	89
2.	Freund and Danforth	91
E.	Claim 1	94
1.	[1pre] A method for protecting a network, comprising:.....	94
2.	[1a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,.....	94
3.	[1b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,	98
4.	[1c] receiving a response, and.....	102
5.	[1d] determining whether the response includes a valid digitally signed attestation of cleanliness,	103
6.	[1e] 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;.....	104
7.	[1f] 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,	109

8. [1g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,.....111
9. [1h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and113
10. [1i] 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.....116
11. [1j] permitting the first host to communicate with the remediation host.121
- F. Claim 2 – A method as recited in claim 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.122
- G. Claim 3 - A method as recited in claim 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.....123
- H. Claim 4 - A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.....124
- I. Claim 5125
 1. [5pre] A method as recited in claim 1, wherein permitting the first host to communicate with the remediation host includes:125

2.	[5a] detecting an outbound communication from the first host; and	125
3.	[5b] forwarding the outbound communication if it is addressed to the remediation host.....	127
J.	Claim 6	127
1.	[6pre] A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:	127
2.	[6a] detecting an outbound communication from the first host; and	128
3.	[6b] 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.....	128
K.	Claim 7 - A method as recited in claim 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.	128
L.	Claim 8 - A method as recited in claim 1, performed at an Internet service provider.....	130
M.	Claim 9 - A method as recited in claim 1, wherein the software component on the first host is an operating system.	130
N.	Claim 10 - A method as recited in claim 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.	131
O.	Claim 11 - A method as recited in claim 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.	132
P.	Claim 12	134
1.	[12pre] A system for protecting a network, comprising:.....	134
2.	[12a] a processor configured to:	134

3. [12b] detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,.....136
4. [12c] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,136
5. [12d] [wherein detecting the insecure condition includes ...] receiving a response, and.....136
6. [12e] [wherein detecting the insecure condition includes ...] determining whether the response includes a valid digitally signed attestation of cleanliness,136
7. [12f] 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;.....136
8. [12g] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,137
9. [12h] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,.....137
10. [12i] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and137

11. [12j] 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.....137
12. [12k] permit the first host to communicate with the remediation host; and138
13. [12l] a memory coupled to the processor and configured to provide instructions to the processor.138
- Q. Claim 13 - A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.....139
- R. Claim 14 - A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.....139
- S. Claim 15 - A system as recited in claim 12, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.140
- T. Claim 16 - A system as recited in claim 12, wherein the software component on the first host is an operating system.140
- U. Claim 17 - A system as recited in claim 12, 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. ...141
- V. Claim 18 - A system as recited in claim 17, 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.141

W.	Claim 19	142
1.	[19pre] 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:.....	142
2.	[19a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,.....	142
3.	[19b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,	142
4.	[19c] [wherein detecting the insecure condition includes...] receiving a response, and	143
5.	[19d] [wherein detecting the insecure condition includes...] determining whether the response includes a valid digitally signed attestation of cleanliness,	143
6.	[19e] 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;.....	143
7.	[19f] 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,	143
8.	[19g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,.....	144

9.	[19h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and.....	144
10.	[19i] 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.....	144
11.	[19j] permitting the first host to communicate with the remediation host.....	144
VI.	SECONDARY CONSIDERATIONS	144
VII.	RIGHT TO SUPPLEMENT	145
VIII.	CONCLUSION.....	145

INDEX OF EXHIBITS

Exhibit No.	Description
1001	U.S. Patent No. 8,234,705.
1002	Declaration of Dr. Clay Shields.
1003	File History of U.S. Patent No. 8,234,705.
1004	U.S. Patent No. 9,436,820 (“ Gleichauf ”).
1005	U.S. Patent No. 7,747,862 (“ Ovadia ”).
1006	U.S. Patent No. 7,533,407 (“ Lewis ”).
1007	U.S. Patent Pub. No. 2003/0055962 (“ Freund ”).
1008	U.S. Patent Pub. No. 2006/0005009 (“ Ball ”).
1009	U.S. Patent No. 7,571,460 (“ Danforth ”).
1010	U.S. Patent no. 7,568,107 (“ Rathi ”).
1011	U.S. Patent Pub. No. 2004/0177276 (“ MacKinnon ”).
1012	U.S. Patent no. 7,330,977 (“ Cromer ”).
1013	U.S. Patent No. 6,829,654 (“ Jungck ”).
1014	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 .
1015	TPM Main – Part 1 Design Principles, Specification Version 1.2 (Rev. 62 Oct. 2, 2003), available at: https://trustedcomputinggroup.org/wp-content/uploads/tpm-wg-mainrev62_Part1_Design_Principles.pdf .
1016	U.S. Patent Pub. No. 2003/0061494 (“ Girard ”).
1017	U.S. Patent Pub. No. 2005/0078668 (“ Wittenberg ”).
1018	U.S. Patent Pub. No. 2005/0097199 (“ Woodard ”).
1019	U.S. Patent Pub. No. 2005/0033987 (“ Yan ”).
1020	Microsoft Security Bulletin MS99-008 - Critical Microsoft Learn, https://learn.microsoft.com/en-us/security-updates/securitybulletins/1999/ms99-008
1021	What’s Inside A Router, https://web.archive.org/web/20040112004448/http://www2.ic.uff.br/~michael/kr1999/4-network/4_06-inside.htm (Jan. 12, 2004)
1022	<i>Cisco Systems, Inc. v. K.Mizra LLC</i> , IPR2021-00593, Paper 2 (March 15, 2021).

Exhibit No.	Description
1023	<i>Cisco Systems, Inc. v. K.Mizra LLC</i> , IPR2021-00593, Paper 41 (September 19, 2022).
1024	<i>Cisco Systems, Inc. v. K.Mizra LLC</i> , 2022-2290, 2023-1183 (Fed. Cir. 2024)
1025	<i>Cisco Systems, Inc. v. K.Mizra LLC</i> , IPR2021-00593, Paper 23 (January 7, 2022).
1026	<i>Netskope, Inc. v. K.Mizra LLC</i> , IPR2025-01115, Paper 2 (April 13, 2025).
1027	Tony Piltzecker et al., <i>How to Cheat at Managing: Windows Server Update Services</i> (2005).

CHART OF CLAIMS
[1pre] A method for protecting a network, comprising:
[1a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
[1b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,
[1c] [wherein detecting the insecure condition includes...] receiving a response, and
[1d] [wherein detecting the insecure condition includes...] determining whether the response includes a valid digitally signed attestation of cleanliness,
[1e] 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;
[1f] 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,
[1g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,
[1h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and
[1i] 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
[1j] permitting the first host to communicate with the remediation host.
[2] A method as recited in claim 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.
[3] A method as recited in claim 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.

CHART OF CLAIMS
[4] A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.
[5pre] A method as recited in claim 1, wherein permitting the first host to communicate with the remediation host includes:
[5a] detecting an outbound communication from the first host; and
[5b] forwarding the outbound communication if it is addressed to the remediation host.
[6pre] A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:
[6a] detecting an outbound communication from the first host; and
[6b] 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.
[7] A method as recited in claim 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.
[8] A method as recited in claim 1, performed at an Internet service provider.
[9] A method as recited in claim 1, wherein the software component on the first host is an operating system.
[10] A method as recited in claim 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.
[11] A method as recited in claim 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.
[12pre] A system for protecting a network, comprising:
[12a] a processor configured to:
[12b] detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,
[12c] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,
[12d] [wherein detecting the insecure condition includes...] receiving a response, and
[12e] [wherein detecting the insecure condition includes...] determining whether the response includes a valid digitally signed attestation of cleanliness,

CHART OF CLAIMS	
[12f]	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;
[12g]	when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,
[12h]	wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,
[12i]	[wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and
[12j]	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
[12k]	permit the first host to communicate with the remediation host; and
[12l]	a memory coupled to the processor and configured to provide instructions to the processor.
[13]	A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.
[14]	A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.
[15]	A system as recited in claim 12, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.
[16]	A system as recited in claim 12, wherein the software component on the first host is an operating system.

CHART OF CLAIMS
[17] A system as recited in claim 12, 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.
[18] A system as recited in claim 17, 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.
[19pre] 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:
[19a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
[19b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,
[19c] [wherein detecting the insecure condition includes...] receiving a response, and
[19d] [wherein detecting the insecure condition includes...] determining whether the response includes a valid digitally signed attestation of cleanliness,
[19e] 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;
[19f] 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,
[19g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,
[19h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and
[19i] 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

CHART OF CLAIMS
associated with a remediation host configured to provide data usable to remedy the insecure condition; and
[19j] permitting the first host to communicate with the remediation host.

I, Clay Shields, declare as follows:

1. My name is Clay Shields. I have been asked by Petitioner Citrix Systems, Inc. to provide my expert opinions in support of the above-identified petition for *inter partes* review of U.S. Patent No. 8,234,705 (“’705 patent,” EX1001), challenging the validity of claims 1-19 (the “Challenged Claims”).

2. In summary, it is my opinion that the references cited below render obvious the Challenged Claims. My detailed opinions on the claims are set forth below and summarized in the following chart.

Ground	Claims	Stat. Basis	Prior Art
1	1-19	§103	Gleichauf in view of Ovadia and Lewis
2	1-19	§103	Freund in view of Ball and Danforth

3. I am being compensated at my normal consulting rate of \$600 per hour for my time. My compensation is not contingent on the outcome of this proceeding or of any proceedings relating to the ’705 patent.

I. BACKGROUND AND QUALIFICATIONS

A. Qualifications

4. All of my opinions stated herein are based on my own personal knowledge, professional judgment, and analysis of the materials and information I considered in preparing this Declaration. In forming my opinions, I have relied on

my knowledge and experience in designing, developing, researching, and teaching the technology referenced in this Declaration.

5. I am over 18 years of age and, if I am called upon to do so, I would be competent to testify as to the matters set forth herein. I have been informed that a copy of my current curriculum vitae, which details my education and professional and academic experience, is being submitted as Exhibit A. The following provides a brief overview of some of my experience that is relevant to the matters set forth in this Declaration.

6. I received a Bachelor of Science degree in Electrical Engineering from the University of Virginia in 1989. After serving in the US Army, I received a Master's and a Ph.D. in Computer Engineering University of California at Santa Cruz in 1996 and 1999, respectively. My thesis topics focused on efficient multi-party network communications and on maintaining anonymity on the internet using peer-to-peer protocols.

7. I currently am a Professor in the Computer Science department of Georgetown University, where I have worked since 2001.

8. I have taught more than 45 classes on computer science on subjects ranging from introductory courses in programming for incoming freshmen, to upper-level classes on computer systems, security, and networking, to graduate

level courses and doctoral seminars on advanced computer and network security topics.

9. I have been the Principal Investigator (PI) or co-PI on over \$12,000,000 of externally funded grants.

10. Since I became a faculty member in 1999 (initially at Purdue University before joining Georgetown in 2001), I have written a number of research papers that have appeared in many of the most prestigious venues. These include highly cited papers in a variety of areas, including: secure ad-hoc routing; detection of IP covert channels; attacks against computer voice input systems; and attacks and defenses for peer-to-peer network anonymity systems. I have additionally been part of the design and deployment of peer-to-peer network forensics software used by law enforcement around the world to identify and arrest those sharing child-abuse imagery. Though we are not aware of all arrests that have been made, my co-authors and I know of many cases where children were saved from severely abusive situations by law enforcement using the tools we developed.

11. My technical qualifications uniquely qualify me for this proceeding as they are particularly relevant to the issues raised by the '705 patent. My career has been dedicated to advancing the state of the art in network security, distributed computing, and protocol engineering. I have led research and development efforts

focused on secure network architectures, including the design of mechanisms for authenticating devices, detecting and mitigating malicious activity, and ensuring the integrity and confidentiality of data in transit. My work has required a deep understanding of both the theoretical underpinnings and practical implementation challenges associated with secure, scalable, and reliable networked systems. I have also been responsible for evaluating and integrating emerging security technologies—such as hardware-based trust anchors and remote attestation protocols—into real-world deployments. This experience gives me a comprehensive perspective on the technical problems addressed by the '705 patent, including the challenges of establishing trust in distributed environments and the practical considerations involved in deploying such solutions at scale. My familiarity with both academic research and operational systems allows me to critically assess the novelty, feasibility, and impact of the claimed inventions in the context of the state of the art at the relevant time.

B. Technology Background

12. The technology at issue, at the time of the alleged priority date of September 27, 2004 was well known. In particular, each of the components/disciplines involved had been well known.

13. The need to protect networks by excluding malicious hosts had been known for years, and a wide variety of solutions to do so had become available.

One difficulty lay in knowing when hosts were compromised or otherwise malicious. The development of the Trusted Platform Module (TPM) in the late 1990s provided a way to do this, as it became possible to remotely attest to a computer's internal state using trusted hardware. Any computer that could not provide an attestation to a known non-malicious state could be considered potentially harmful to the network.

C. Materials Reviewed

14. My opinions contained in this Declaration are based on the documents I reviewed, my professional judgment, as well as my education, experience, and knowledge of the field.

15. In preparing this declaration, I have reviewed and/or considered at least the documents cited in the List of Exhibits, and the documents referenced in this declaration.

16. I have been informed that the '705 patent was the subject of a previously filed *inter partes* review – IPR2021-00593. EX1022. I have reviewed the prior petition (EX1022), the prior final written decision (EX1023), and the Federal Circuit opinion vacating the Board's decision (EX1024).

II. RELEVANT PATENT LAW AND LEGAL STANDARDS

17. I am not an attorney and offer no legal opinions, but in the course of my work, I have had experience studying and analyzing patents and patent claims from the perspective of a person skilled in the art.

18. For the purposes of this Declaration, I have been informed about certain aspects of the law that are relevant to my analysis, as summarized below.

A. Legal Standards for Anticipation

19. I understand that documents and materials that qualify as prior art can be used to invalidate a patent claim via anticipation or obviousness.

20. I understand that, once the claims of a patent have been properly construed, the second step in determining anticipation of a patent claim requires a comparison of the properly construed claim language to the prior art on a limitation-by-limitation basis.

21. I understand that a prior art reference “anticipates” an asserted claim, and thus renders the claim invalid, if all elements of the claim are disclosed in that prior art reference, either explicitly or inherently (*i.e.*, necessarily present).

22. I understand that anticipation in an *inter partes* review must be shown by a preponderance of the evidence.

B. Legal Standards for Obviousness

23. I understand that even if a patent is not anticipated, it is still invalid if the differences between the claimed subject matter and the prior art are such that

the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in the pertinent art.

24. I understand that a person of ordinary skill in the art provides a reference point from which the prior art and claimed invention should be viewed. This reference point prevents one from using his or her own insight or hindsight in deciding whether a claim is obvious.

25. I also understand that an obviousness determination includes the consideration of the following factors: (1) the scope and content of the prior art, (2) the differences between the prior art and the asserted claims, (3) the level of ordinary skill in the pertinent art, and (4) the existence of secondary considerations of non-obviousness such as commercial success, long-felt but unresolved needs, failure of others, etc.

26. I understand that an obviousness evaluation can be based on a combination of multiple prior art references. I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but other times the nexus linking two or more prior art references is simple common sense. I further understand that obviousness analysis recognizes that market demand, rather than scientific literature, often drives innovation, and that a motivation to combine references may be supplied by the direction of the marketplace.

27. I understand that if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

28. I also understand that practical and common-sense considerations should guide a proper obviousness analysis, because familiar items may have obvious uses beyond their primary purposes. I further understand that a person of ordinary skill in the art looking to overcome a problem will often be able to fit together the teachings of multiple publications. I understand that obviousness analysis therefore takes into account the inferences and creative steps that a person of ordinary skill in the art would employ under the circumstances.

29. I understand that a particular combination may be proven obvious merely by showing that it was obvious to try the combination. For example, when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp because the result is likely the product not of innovation but of ordinary skill and common sense.

30. The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results. When a

work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, the patent claim is likely obvious.

31. It is further my understanding that a proper obviousness analysis focuses on what was known or obvious to a person of ordinary skill in the art, not just the patentee. Accordingly, I understand that any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed.

32. I understand that a proposed obviousness combination does not need to be the preferred, or most desirable, combination available, in order to render a claim obvious. Instead, there must be something that suggests the desirability of the proposed combination, not necessarily something that suggests that the proposed combination is the most desirable combination available.

33. Similarly, I understand that for purposes of obviousness, when a motivating benefit comes at the expense of another benefit, that does not nullify the proposed obviousness combination or modification. Likewise, a proposed obviousness combination does not fail merely because it may be inferior to other systems used for the same use.

34. I also understand that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements between the multiple references. Likewise, the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. Instead, the test is whether a claim is rendered obvious by the teachings of the prior art as a whole.

35. I understand that a claim can be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found explicitly or inherently in the reference can be supplied by the common sense of one of skill in the art.

36. I understand that secondary indicia of non-obviousness may include: (1) a long felt but unmet need in the prior art that was satisfied by the invention of the patent; (2) commercial success of processes covered by the patent; (3) unexpected results achieved by the invention; (4) praise of the invention by others skilled in the art; (5) taking of licenses under the patent by others; (6) deliberate copying of the invention; (7) failure of others to find a solution to the long felt need; and (8) skepticism by experts.

37. I also understand that there must be a relationship between any such secondary considerations and the invention. I further understand that

contemporaneous and independent invention by others is a secondary consideration supporting an obviousness determination.

38. In sum, my understanding is that prior art teachings are properly combined where a person of ordinary skill in the art having the understanding and knowledge reflected in the prior art and motivated by the general problem facing the inventor, would have been led to make the combination of elements recited in the claims. Under this analysis, the prior art references themselves, or any need or problem known in the field of endeavor at the time of the invention, can provide a reason for combining the elements of multiple prior art references in the claimed manner.

39. I understand that obviousness in an *inter partes* review must be shown by a preponderance of the evidence.

III. THE '705 PATENT

A. Overview of the '705 Patent

40. The '705 patent issued from U.S. Patent Application No. 11/237,003, filed September 27, 2005, and claims priority to U.S. Provisional Application No. 60/613,909, filed September 27, 2004. I have been informed that the '705 patent's priority date is no earlier than September 27, 2004.

41. 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. EX1001, Abstract. A device in quarantine “is provided only limited access to the protected network.” EX1001, 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.” EX1001, 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.” EX1001, 3:14-17.

B. File History of the ‘705 Patent

42. During prosecution, the Examiner issued Office Actions rejecting the pending claims under 35 U.S.C. §103. EX1003, 232-252, 281-297, 356-376, 414-431. In response, Applicant filed responses amending the claims, including an appeal brief, which the examiner removed from the appeal track. EX1003, 219-226, 259-271, 329-340, 389-399. The Examiner then issued a notice of allowance. EX1003, 37-52.

C. Person of Ordinary Skill in the Art

43. I understand that the patent claims must be considered through the eyes of a hypothetical “person of ordinary skill in the art” (POSITA). I understand

that a POSITA is not a specific or real individual, but rather a hypothetical individual having the qualities reflected by the following criteria: (a) the type of problems encountered in the art; (b) prior art solutions to those problems; (c) the rapidity with which innovations are made; (d) the sophistication of the technology; and (e) the education level of active workers in the field. Furthermore, a POSITA would be familiar with the entire prior art literature.

44. In my opinion, a person of ordinary skill in the art at the time of the alleged invention of the '705 patent (September 27, 2004) ("POSITA") would have had a bachelors' degree in electrical engineering, computer science, computer engineering or a comparable field of study, plus approximately two years of professional experience in the field of network communications, and more specifically, network security. Additional graduate education could substitute for professional experience, and significant experience in the field could substitute for formal education.

45. As I have an expertise in the field of network communications and network security, I am well acquainted with the level of ordinary skill that would be required to implement the systems and methods described in the '705 patent. I am also capable of rendering informed opinions as to the understanding of one of ordinary skill in the art as of the time of the '705 patent's September 27, 2004 claimed U.S. priority date.

D. Claim Construction

46. In my opinion, no claim term requires an express construction and all terms should be construed according to their plain and ordinary meaning.

Nevertheless, I have been informed that in the previous petition (IPR2021-00593), the previous petitioner identified and construed two terms. To the extent there is a dispute as to whether these terms require an express construction, I have reviewed and adopted the prior petitioner's construction from IPR2021-00593, as set forth below:

1. “trusted computing base” (claims 1, 12, 19)

47. For this limitation, I have been informed that the previous parties agreed that the term 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.” EX1022, 12-13; EX1025, 5-6; EX1023, 14.

2. “trusted platform module” (claims 1, 12, 19)

48. For this limitation, I have been informed that the previous petitioner proposed that this limitation be construed as “*a secure cryptoprocessor that implements a Trusted Platform Module specification from the Trusted Computing Group.*” EX1022, 13-16; EX1025, 5-6. Although the Patent Owner disputed this construction, the Board did not identify any issue that would turn on this construction and determined that no claim terms require express construction.

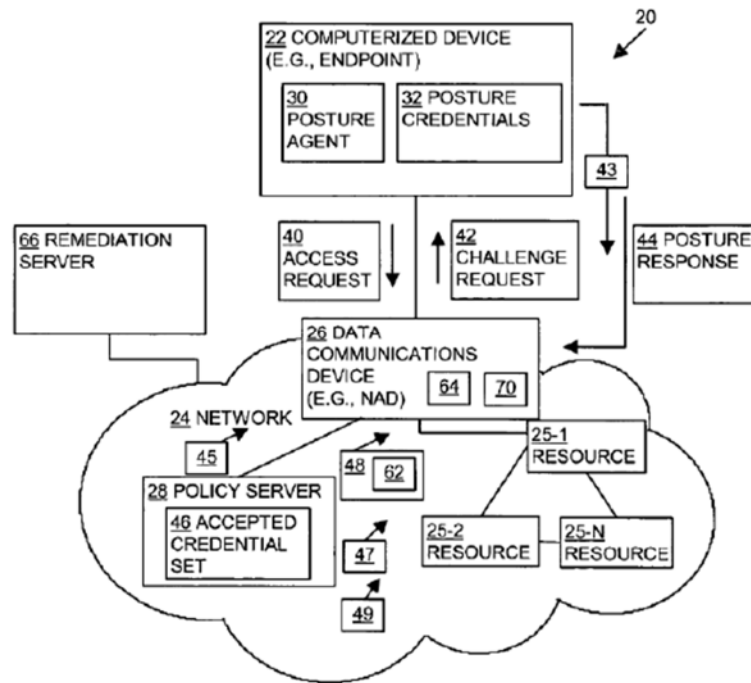
EX1023, 14. Nevertheless, should a similar dispute arise, I have reviewed and adopted the previous petitioner's construction of this limitation.

IV. GROUND 1: CLAIMS 1-19 ARE OBVIOUS OVER GLEICHAUF IN VIEW OF OVADIA, AND LEWIS

A. Overview of Gleichauf

49. U.S. Patent No. 9,436,820 ("Gleichauf") was filed August 2, 2004, and published September 6, 2016. EX1004, cover page. I have been informed that Gleichauf is prior art under 35 U.S.C. §102(e) (pre-AIA).

50. Gleichauf generally relates to the field of network security. EX1004, 7:55-61. Gleichauf teaches controlling a computerized device's access to network resources based on the security posture of the device. EX1004, 3:4-9. Gleichauf illustrates a data communications system in Figure 1 that includes a device that is attempting to access a network resource on the network:



EX1004, FIG. 1. Gleichauf's policy server controls the device's access to the network. EX1004, 7:4-8, 10:20-23. When the policy server detects a security issue with a device, e.g., an out-of-date anti-virus application, the device is quarantined. EX1004, 15:55-61. 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. EX1004, 16:13-21. Normal access is generally granted after the device is updated. EX1004, 16:40-43.

51. In my opinion, Gleichauf is analogous art to the '705 patent because both Gleichauf and the '705 patent are in the same field of endeavor and address network security by controlling access to network resources based on the security

posture or condition of a device attempting to connect to resources. EX1004, 3:4-9 (“embodiments of the present invention significantly overcome such deficiencies and provide mechanisms that include 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”); EX1001, 3:13-20 (“If the host is required to be quarantined, the host is provided only limited access to the protected network” such as “access the protected network only as required to remedy a condition that caused the quarantine to be imposed”). In addition, Gleichauf is reasonably relevant to the problem the ’705 patent is concerned with, as shown in my analysis below.

52. Based on my review of the ’705 patent’s prosecution history (EX1003), Gleichauf appears to have not been considered during prosecution of the ’705 patent.

B. Overview of Ovadia

53. U.S. Patent No. 7,747,862 (“Ovadia”) was filed June 28, 2004, and published June 29, 2010. EX1005, cover page. I have been informed that Ovadia is prior art under 35 U.S.C. §102(e) (pre-AIA).

54. Ovadia discloses network security measures and describes steps to ensure that a device seeking to access a network has an authorized configuration. EX1005, 1:8-11, Abstract. Ovadia’s security scheme generates security keys,

including attestation identity keys (“AIKs”), using a trusted platform module.

EX1005, Abstract. The trusted platform module is used “to verify [that] a current configuration of a subscriber station platform is an authorized configuration.”

EX1005, Abstract. A subscriber station seeking network access “sends authentication information including a manifest signed with the SS’s [subscriber station’s] private AIK key.” EX1005, Abstract. An authentication server receives the information and authenticates the subscriber station via the subscriber station’s public AIK key. EX1005, Abstract.

55. In my opinion, Ovadia is analogous art to the ’705 patent because both Ovadia and the ’705 patent are in the same field of endeavor and address security schemes for wireless networks. EX1005, 1:8-11 (“The field of invention relates generally to security schemes for wireless networks, and, more specifically but not exclusively relates to techniques for enhancing security for broad band wireless networks”); EX1001, 1:38-41 (“there is a need for a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network”).

56. Based on my review of the ’705 patent’s prosecution history (EX1003), Ovadia appears to have not been considered during prosecution of the ’705 patent.

C. Overview of Lewis

57. U.S. Patent No. 7,533,407 (“Lewis”) was filed April 14, 2004, and published May 12, 2009. EX1006, cover page. I have been informed that Lewis is prior art under 35 U.S.C. 102(e) (pre-AIA).

58. Lewis describes network security measures, including verifying the configuration state of a device that seeks to access a network. EX1006, 4:7-9. Lewis provides “a system for ensuring that machines having invalid or corrupt states are restricted from accessing network resources.” EX1006, 4:7-9. Lewis describes how the device must provide a “bill of health” to a quarantine server before gaining access to the network. EX1006, 4:13-15. The quarantine server determines if the bill of health is valid or invalid. EX1006, 4:16-23. A valid bill of health indicates that the device has up-to-date security software, and the device is granted access to the network. EX1006, 4:18-21. 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. EX1006, 13:44-52.

59. The lock-down configuration puts the device in quarantine. EX1006, 13:63-65. 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.” EX1006,

10:61-66. 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. EX1006, 13:12-15.

60. 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. EX1003, 249-250. 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. EX1003, 224-225. I am 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.

61. In my opinion, Lewis is analogous art to the '705 patent because both Lewis and the '705 patent are in the same field of endeavor and address security schemes for wireless networks by controlling access to wireless networks. EX1006, 1:9-12 ("The present invention relates generally to network access management, and relates more particularly to checking the security state of clients before allowing them to access network resources"); EX1001, 1:38-41 ("there is a need for a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network"), 3:13-20 ("If the host is required to be quarantined, the host is provided only limited access to the

protected network” such as “access the protected network only as required to remedy a condition that caused the quarantine to be imposed”).

D. Motivation to Combine Gleichauf and Ovadia

62. In my opinion, 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. EX1004, 3:4-9; EX1005, 1:8-11. 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. 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.

63. In my opinion, 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. EX1005, 4:32-35; EX1014, 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. EX1014, 2-4; EX1016, ¶11 (“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.”); EX1012, 2:8-11 (TCPA is the former name of TCG); EX1019, ¶¶3-4. 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. 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 providing the credentials. Following the industry standard would also promote the interoperability of devices from diverse manufacturers. Ensuring the interoperability of devices is a common and important goal in the computer networking arts.

64. Ovadia describes applying technology from the “Trusted Computing Group (TCG)” which addresses “network security” and “covers trust in computing platforms in general.” EX1005, 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.

65. In my opinion, 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. In my opinion, 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. EX1008, ¶33. In my opinion, a POSITA also would have recognized that use of a digital signature would improve Gleichauf’s process by enabling the policy server to confirm that the posture credentials originated with the device attempting to access the network.

66. In my opinion, 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. Gleichauf provides that

“policy server 28 authenticates an identity of the computerized device 22 to generate an authentication result.” EX1004, 22:3-5. Ovadia explains that one way to authenticate a device is to check that device’s digital signature. EX1005, 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.

67. In my opinion, a POSITA would have had a reasonable expectation of success in combining Gleichauf and Ovadia. Notably, components of Ovadia’s trusted computing architecture have corresponding components in Gleichauf’s architecture, and a POSITA would have recognized how the descriptions provided for components in Ovadia would be applicable to the corresponding components in Gleichauf. For example, 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.” EX1004, 3:8, 12:21-31; EX1005, 4:40-43, 14:1-6; Fig. 8. Ovadia’s integrity measurement is stored in the trusted platform module. EX1005, 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. EX1005, 4:43-45, 13:61-63, Fig. 8; EX1004, 10:63-11:3. Ovadia’s

integrity measurement is “digitally signed with appropriate keys” before it is sent to the authentication server. EX1005, 13:63-64, Fig. 8. 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.” EX1005, 14:9, 5:35-36. In my opinion, 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 security assurances available with digital signatures and limited-use integrity keys. Such a combination would have involved application of known techniques (e.g., trusted platform module functionality) to improve the network security of Gleichauf’s computerized devices in the same way in which Ovadia’s trusted platform module operates (e.g., storing, providing, and digitally signing integrity measurements). Such a combination would also have involved the combination of prior art elements (e.g., combining Ovadia’s well-known trusted platform module with Gleichauf’s computerized devices) according to known methods to yield predictable results (improved network security to Gleichauf’s computerized devices).

68. 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. EX1004, 4:50-67; EX1005, 16:62-65. In my opinion, 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. In my opinion, 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. EX1004, 27:24-29; EX1005, 18:64-19:4.

69. In my opinion, the proposed combination permits but do not require physical incorporation of elements from Ovadia into Gleichauf.

E. Motivation to Combine Gleichauf, Ovadia, and Lewis

70. In my opinion, 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. EX1004, 3:4-9; EX1005, 1:8-11; EX1006, 4:7-9. In my opinion, 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. 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.

71. In my opinion, 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. In my opinion, 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. EX1006, 10:61-66, 13:63-14:1. Lewis's quarantine webpage would also be advantageous to Gleichauf's or Ovadia's notification message. Gleichauf discloses notifications in the form of "extensible messaging format, such as a Type-Length-Value (TLV) or an extensible markup language (XML) format" which "are well-defined, application independent form for representing information or data." EX1004, 20:56-60. In comparison, Lewis's webpage served by the quarantine server is displayed in the browser that a user already has opened. Therefore, modifying the XML/TVL notification approach in Gleichauf to Lewis's webpage based notifications would advantageously avoid

necessitating additional software components running on the device to receive and display the notification message to the user. EX1004, 4:56-60; EX1005, 16:62-65.

72. In my opinion, 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. A user attempting to access the network from a fixed location (e.g., an office) may have time to proceed with remediation. In this instance, the webpage would direct the user to a remediation server that can resolve the security issues per Gleichauf. EX1004, 5:4-11. 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. In my opinion, a POSITA would have understood the benefits of giving the user the option to choose their desired course of action.

73. Additionally, A POSITA at the time would have understood that directing a user to a quarantine server rather than a remediation server would provide business benefits as well. Patch management and its associated costs and complications was well known at the time. EX1027, xxi-xxii, 2. While it was possible to redirect a system joining to the network to a Microsoft Update server, which would be the remediation server of the patent, doing so might cause wasted bandwidth from duplicate download and would not allow an organization's IT service to track what updates were installed on the system. Instead, in my opinion,

a POSITA would have understood that directing the system to a quarantine server would allow distribution of a locally-downloaded and cached version of system updates, saving network bandwidth, and would enable maintenance of a central database of what was installed and updated on each system. These are all part of normal IT operations and would be enabled by use of the quarantine server. Additionally, a system that required updates from several sources (e.g., Microsoft, Adobe, Oracle, etc.) could place those updates on one server, instead of requiring repeated attempts at joining the network and redirection to a variety of remediation servers.

74. In my opinion, a POSITA would have had a reasonable expectation of success in combining the teachings of Gleichauf and Ovadia with Lewis. As explained, Gleichauf's policy server sends a notification message to a quarantined device with information and remediation instructions. EX1004, 5:4-11. Put differently, the policy server identifies whether a device is to be quarantined and, if it is, what actions should be taken to remediate the security issue before the device is allowed access to the network. EX1004, 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. In my opinion, such a

modification involves a software change that is straightforward and is within the skillset of a POSITA at the alleged time of invention.

75. In my opinion, the proposed combinations permit but do not require physical incorporation of elements from Lewis and Ovadia into Gleichauf.

F. Claim 1

76. In my opinion, claim 1 would have been obvious to a POSITA at the time of the invention, in view of the combination of Gleichauf, Ovadia, and Lewis.

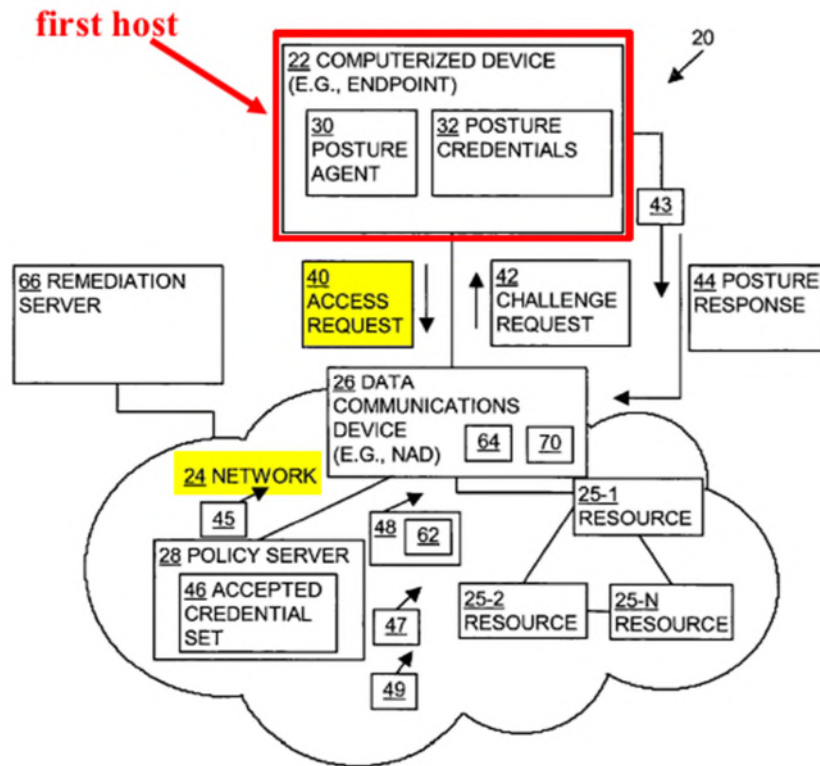
1. [1pre] A method for protecting a network, comprising:

77. In my opinion, Gleichauf discloses a “computer-implemented method to control access to resources in a network.” EX1004, 27:61-62. 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. EX1004, 5:55-60, 7:56-61, 8:16-31, 12:57-67.

2. [1a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,

78. In my opinion, Gleichauf discloses this limitation.

79. Gleichauf describes a “computerized device, such as a personal computer attempting to communicate with restricted resources in the network.” EX1004, 3:50-56, 8:1-4. Figure 1 illustrates the computerized device sending an access request to the network (“*attempting to connect to a protected network*”):



EX1004, FIG. 1. Gleichauf's computerized device is a *first host*, and, the network, which contains resources protected by access control measures, is a *protected network*. In my opinion, the computerized device's attempt to access the restricted network resources through an access request shows that the device has *connected or is attempting to connect* to the network.

80. Gleichauf's policy server *detects an insecure condition* in the computerized device. The device's attempt to connect to the network triggers a "posture based challenge-response" exchange where the device transmits its posture credentials to the network. EX1004, 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. EX1004, 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).” EX1004, 14:16-34. 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.” EX1004, 22:38-59, 11:58-12:13. A device would also be vulnerable to any malware that might be transmitted by network resources. EX1004, 1:10-14, 8:52-56. Thus, in my opinion, the absence of an anti-virus application or up-to-date anti-virus application is an example of an *insecure condition*.

81. 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.” EX1004, 1:65-2:3, 8:65-9:1, 3:36-45, 31:1-7. Gleichauf explains that there may be “known vulnerabilities in the device operating system, resident applications, associated security programs, and their respective configurations.” EX1004, 1:65-2:3. Additional examples of a potential *insecure condition* are discussed *infra* at [1d] in relation to the *attestation of cleanliness*.

82. In my opinion, by gathering information relating to a computerized device's vulnerabilities—such as the presence of an up-to-date anti-virus application and operating system patches or when an anti-virus scan was last run—Gleichauf discloses *detecting an insecure condition*.

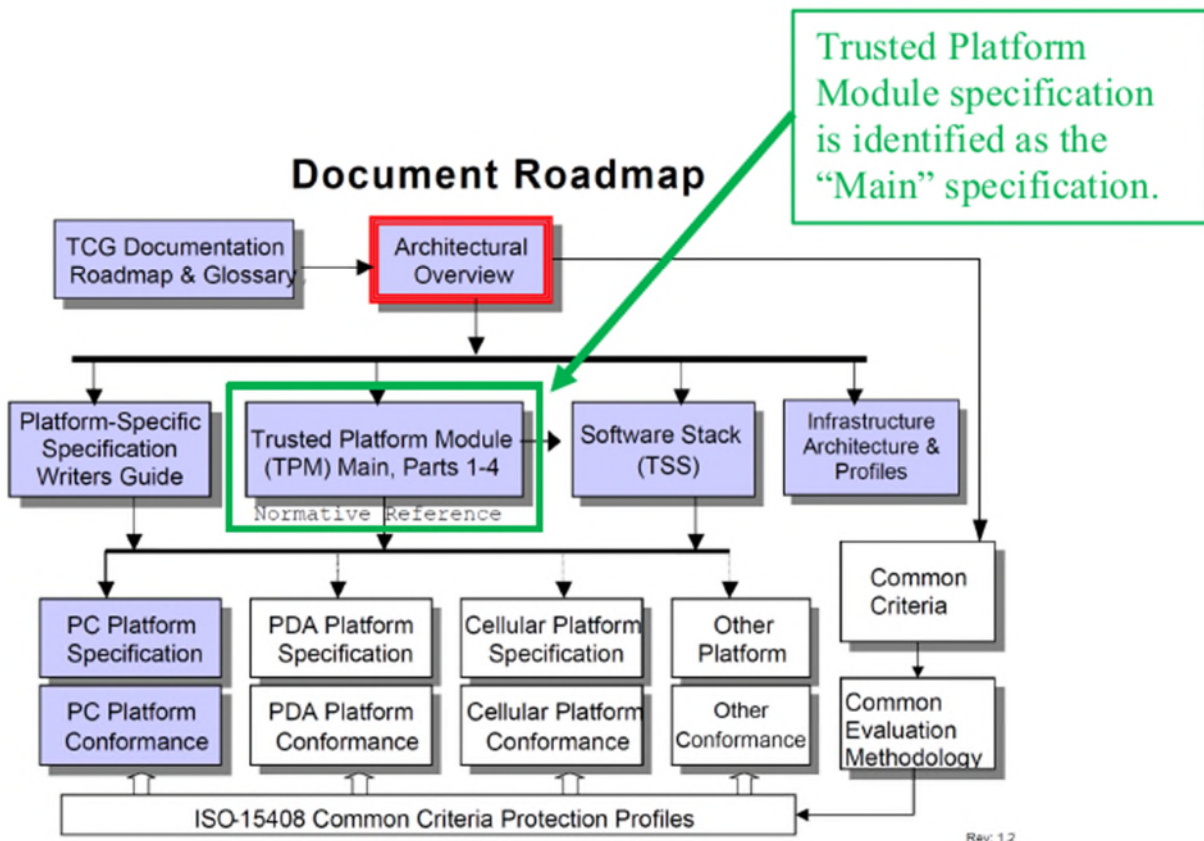
3. [1b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,

83. In my opinion, the combination of Gleichauf and Ovadia discloses this limitation.

84. 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. EX1004, 3:9-16. 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. EX1004, 9:24-39. Gleichauf's posture agent is "embodied as a software or hardware application." EX1004, 9:29-39. Since the posture credentials are used to secure access to the restricted resources, in my opinion, 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. Thus, the combined functionality of the posture agent and plug-ins is a *trusted*

computing base within the computerized device that provides security Gleichauf's data communication system. §III(D)(1) (construction of "trusted computing base").

85. In my opinion, Ovadia discloses a security apparatus that employs a trusted platform module implementing the Trusted Computing Group "main specification (Version 1.2, October 2003...)." EX1005, 4:16-47. The main specification from TCG is the Trusted Platform Module Main Specification:

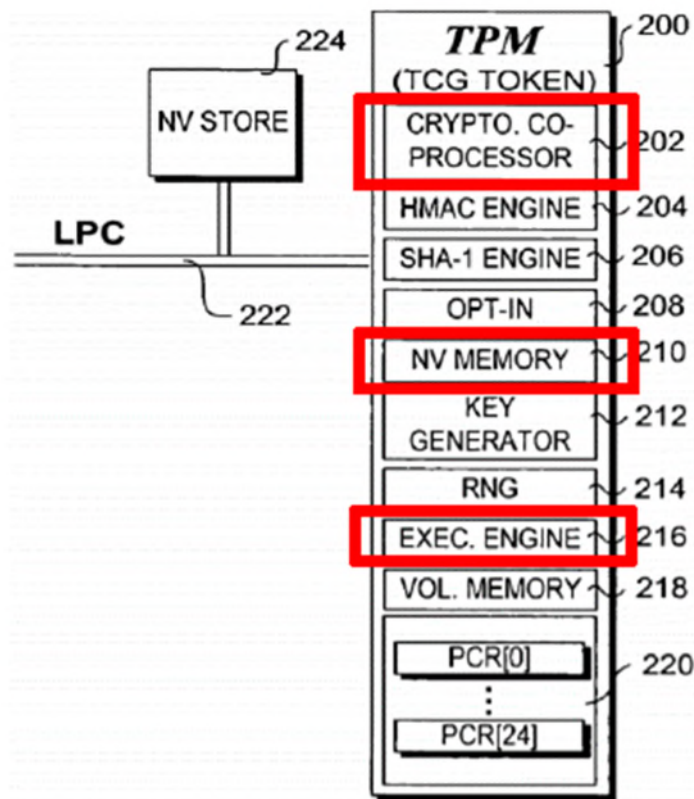


EX1014, iv. EX1015.

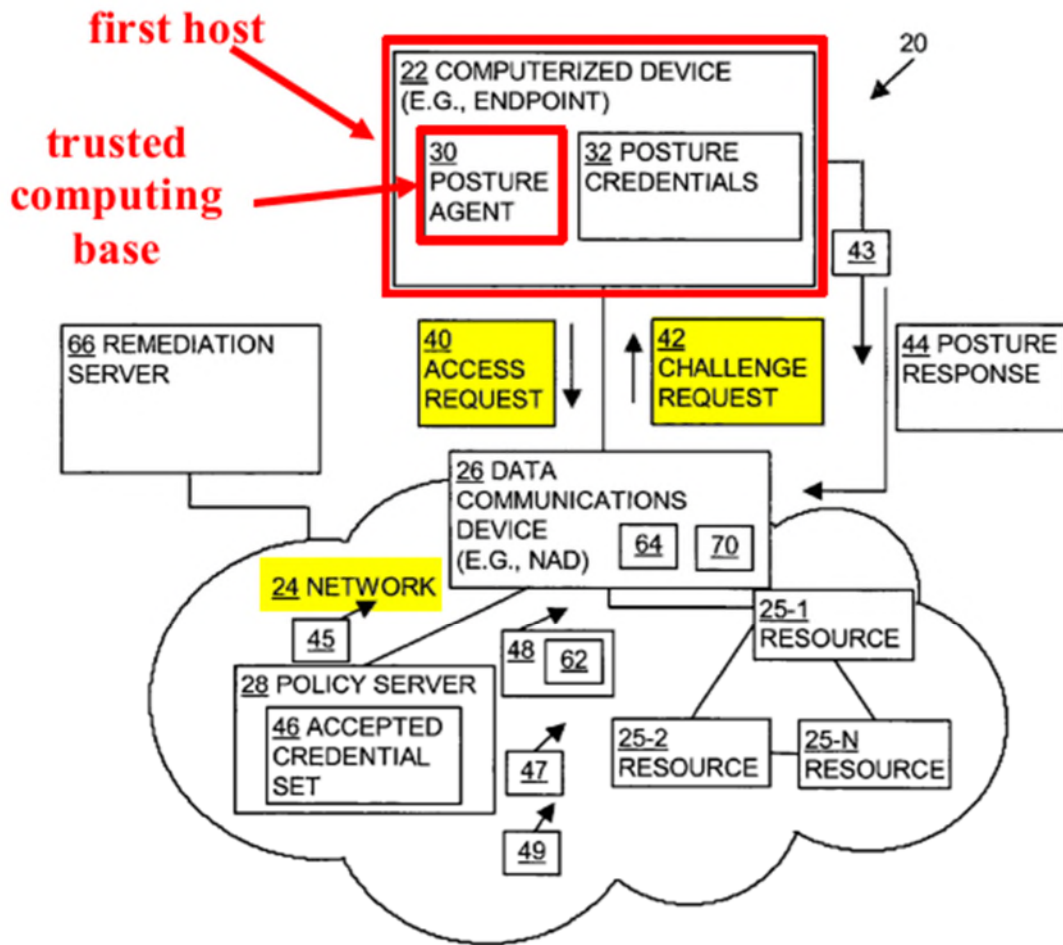
86. Ovadia's trusted platform module implements the Trusted Platform Module main specification from the TCG and includes a "cryptographic co-

processor,” “non-volatile (NV) memory,” and an “execution engine.” EX1005, 4:46-55, Fig. 2. Since Ovadia’s trusted platform module implements the Trusted Platform Module main specification, in my opinion, 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. EX1013, 19; EX1008, 19; EX1005,

FIG. 2:



87. Further, 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. EX1004, 4:7-11, 3:28-36. Gleichauf’s Figure 1, below, shows the posture agent *within* the device:



EX1004, FIG. 1. In my opinion, it would have been obvious to a POSITA that the *trusted platform module* would likewise be *within* the device. Therefore, in my opinion, Ovadia’s trusted platform module is a *trusted platform module* as claimed. §III(D)(2) (construction of “trusted platform module”). Furthermore, in my opinion, the “computerized device” constitutes the hardware portion of the trusted computing base.

88. Ovadia’s trusted platform module “may be embodied as a hardware device (most common) or via software.” EX1005, 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."

EX1006, Abstract. The configuration (called the integrity measurement) includes information about the subscriber station, including the "current measurement of the firmware and/or software" of the station. EX1006, 13:57-14:12.

89. In my opinion, 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. §IV(D) (motivation to combine). A POSITA would have appreciated the value in implementing Gleichauf's posture agent with trusted platform module functionality. §IV(D) (motivation to combine). The TCG, which prepares the TCG specification discussed above, is "an **industry consortium** concerned with platform and network security." EX1005, 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. EX1005, 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. 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

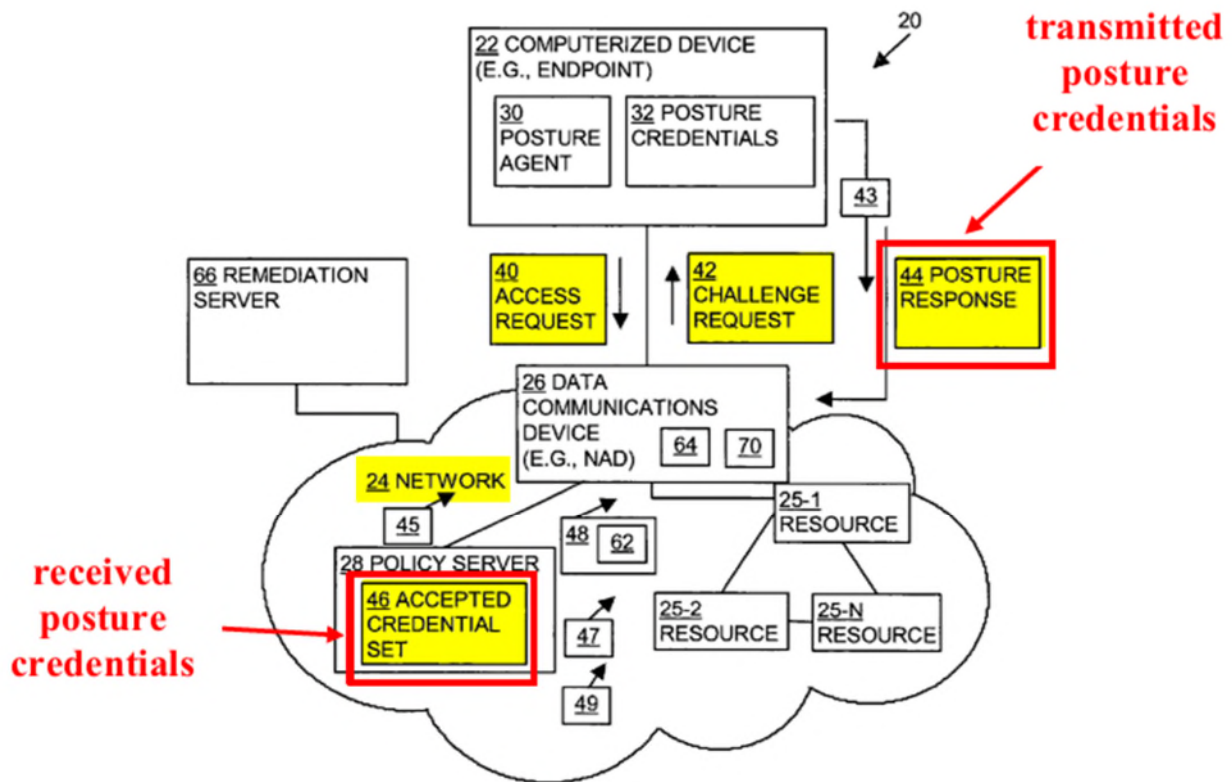
modules would be consistent throughout the adopting industry. In my opinion, on the network side, a policy server receiving Gleichauf's posture credentials would process them more quickly and with more confidence. Indeed, the policy server would be able to process all received posture credentials in substantially the same way because such credentials would have been gathered in substantially the same way. In the combination, Gleichauf's posture agent would be implemented with trusted platform module functionality, i.e., a *trusted platform module*, per Ovadia.

90. For example, in my opinion, one straight-forward way a POSITA would have implemented Gleichauf's posture agent with trusted platform module functionality would be for the posture agent software to be executed in combination with the execution engine in Ovadia's trusted platform module. EX1005, 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. EX1004, 9:24-28. With the posture agent executing in combination with 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. EX1005, 5:36.

91. As another example, in an 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. EX1005, 4:24-26 ("TPM functionality may be embodied... via software."). In my opinion, 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*.

**4. [1c] [wherein detecting the insecure condition includes ...]
receiving a response, and**

92. In my opinion, Gleichauf discloses this limitation. 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. EX1004, 3:28-36, 4:11-15. Gleichauf's Figure 1 illustrates the transmission and reception of posture credentials:



EX1004, FIG. 1. Thus, in my opinion, the policy server “receiv[es] a response” to its request for the posture credentials.

**5. [1d] [wherein detecting the insecure condition includes ...]
determining whether the response includes a valid digitally
signed attestation of cleanliness,**

93. In my opinion, the combination of Gleichauf and Ovadia discloses this limitation.

94. As discussed above, Gleichauf’s posture response includes posture credentials. §IV(F)(4) (limitation 1c). 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*. EX1004, 3:36-49.

95. The policy server analyzes and “validate[s] the posture credentials” (i.e., “*determining whether the response includes a valid ... attestation of cleanliness*”). EX1004, 10:30-33. For example, the policy server checks for (i.e., “*determin[es]*”) the presence of an anti-virus application. EX1004, 10:30-33. If a current anti-virus application 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.*” EX1004, 11:45-58. If a current anti-virus application 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.*” EX1004, 11:58-67.

96. The posture agent “securely transmit[s]” posture credentials to the policy server. EX1004, 11:3-12.

97. Ovadia provides further details about secure transmission of a device’s configuration information for the purpose of requesting access to a network. 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.” EX1005, 14:1-6. The integrity measurement is stored in the trusted platform module. EX1005, 13:61-63, Fig. 8. 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].” EX1005, 14:6-10. The subscriber station “is authenticated” and allowed access to the network if the integrity measurement is acceptable and “the digital signature is authentic.” EX1005, 14:13-23, 16:66-17:6.

98. In my opinion, a POSITA would have been motivated to combine the teachings of Gleichauf and Ovadia and would have had the skills to do so. §IV(D) (motivation to combine). A POSITA would have understood that Ovadia’s digital signature decreases the risk of accepting credentials that have been altered by a malicious actor. Furthermore, a POSITA would understand that Ovadia’s digital signature provides the necessary confidence that the credentials have not been altered. As discussed above, in the combination, Gleichauf’s posture credentials would be prepared by a posture agent implemented with trusted platform module functionality (as taught by Ovadia). §IV(F)(3) (limitation 1b). In my opinion, 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 confirm that the posture

credentials have not been forged or tampered with. 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." EX1005, 14:9, 5:35-36. Since only the trusted platform module (Gleichauf's posture agent implemented with trusted platform module functionality (§IV(F)(3) (limitation 1b)) 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. 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. In my opinion, 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. 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. In my opinion, a POSITA would have further found it obvious to substitute Ovadia's teachings of digitally signing the integrity measurement for Gleichauf's generic recitation of secure transmission. §IV(D) (motivation to combine).

- 6. [1e] 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;**

99. In my opinion, Gleichauf discloses and/or renders this limitation obvious.

100. The computerized device's posture credentials transmitted to the policy server (the "attestation of cleanliness" in §IV(F)(5) (limitation 1d)), contain information about "the last time a local antivirus scan was executed." EX1004, 3:41. 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. EX1004, 22:38-47. In my opinion, it would have been understood to a POSITA that the opposite showing would have had the opposite effect. In other words, it would have been well understood from the disclosure that a posture credential that does show timely execution of the anti-virus application is to be treated as "an attestation that the trusted computing base has ascertained that the first host is not infested."

101. The posture credentials also contain information about "what particular virus software and virus definition versions are installed," "what operating system patches are installed," and what "types and versions of software applications" are on the device. EX1004, 3:36-49. In my opinion, such information

concerning patches associated with software 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.*”

102. Gleichauf’s posture agent prepares posture credentials from information it collects from posture plug-ins. EX1004, 3:9-16, 9:24-39. 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.” EX1004, 9:50-53. In my opinion, the combined functionality of the posture agent and plug-ins, i.e., *trusted computing base*, thus “*ascertains*” the security posture of the device.

103. In my opinion, Gleichauf’s disclosures regarding the claimed *attestation* are substantially the same as those of the ’705 patent specification. 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.**

EX1001, 14:12-19.

104. In my opinion, a POSITA would have understood Gleichauf’s disclosure that posture credentials contain information about “the last time a local

antivirus scan was executed” (EX1004, 3:36-49) to equate to the ’705 patent’s note about the currency of a virus scan.

7. [1f] 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,

105. In my opinion, Gleichauf discloses and/or renders this limitation obvious.

106. As I explained in §IV(F)(5) (limitation 1d), Gleichauf’s policy server reviews and validates posture credentials. EX1004, 10:30-33, 11:45-58. 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. EX1004, 11:45-58, 22:38-42.

107. Further, Gleichauf describes using the posture credentials to determine whether to place the device in quarantine (“*quarantining the first host*”). EX1004, 4:24-27, 7:3-8. 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 (EX1004, 4:50-56), if its behavior is found to be anomalous, suggesting that it may have been compromised (EX1018, ¶39), or if it is found to be infected with a virus or has been hijacked by an unauthorized entity. EX1009, 4:8-14.

108. 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., “*it is determined that the response does not include a valid digitally signed attestation of cleanliness*”).

EX1004, 11:59-60. Gleichauf provides that “devices that are out of compliance with admission requirements [are assigned] to a quarantine.” EX1004, 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.” EX1004, 11:58-67,.

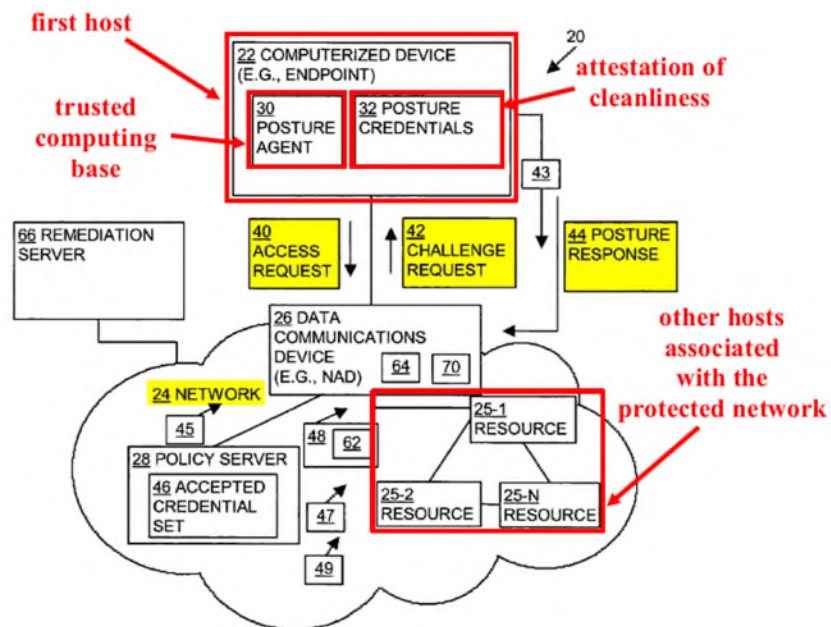


FIG. 1. The resources 25-1 through 25-N are other hosts within the computerized data network. EX1004, 9:65-67 (“The network resources 25-1, 25-2, 25-N, in one

arrangement, are configured as servers that contain content accessible by the user device 22 via the network 24”). Unless the first host is quarantined, for example, the network resources 25-1 through 25-N run the risk of becoming infected through the first host. EX1004, 8:21-28 (“By detecting the real-time security state of the computerized device prior to providing the computerized device with access to the network resources, thereby limiting at-risk or vulnerable computerized devices from accessing the network resources and minimizing the risk that the network resources receive or transmit malware”). Therefore, in my opinion, restricting or completely rejecting communications from the computerized device to network resources, e.g., resources 25-1 through 25-N, discloses *preventing the first host from sending data to one or more other hosts associated with the protected network*.

8. [1g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,

109. In my opinion, Gleichauf discloses this limitation.

110. Gleichauf describes how the computerized device transmits an “access request” or “signaling request” in an “attempt to access the network resources within the network.” EX1004, 3:50-56, 8:1-4. Such access attempts can occur even after the device has been placed in quarantine. EX1004, 13:52-65. A request to access network resources is a “*service request*.” The request is received and acted

upon by a data communications device. EX1004, 3:60-65. Therefore, in my opinion, Gleichauf discloses “*receiving a service request sent by the first host.*”

9. [1h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and

111. In my opinion, the combination of Gleichauf and Lewis discloses and/or renders this limitation obvious.

112. As I explained in §IV(F)(7) (limitation 1f), Gleichauf discloses that a computerized device that is out of compliance with network admission policy is quarantined. EX1004, 4:50-56. Communications from a quarantined device are restricted or rejected. EX1004, 11:58-67. Limited communications to certain destinations, such as a remediation server, may be permitted. EX1004, 14:62-66. For example, Gleichauf provides that “a redirect access instruction” is applied to “HTTP traffic.” EX1004, 15:55-67. In my opinion, 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. This is evidenced by the fact that Gleichauf refers to the redirection as a “URL Redirect.” EX1004, 15:45. In my opinion, 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.

EX1017, ¶3. This technique is commonly used to redirect a user's web browser to a login page at a hotel or airport. EX1010, 4:56-57; EX1011, ¶44.

113. Further, Gleichauf describes providing “one or more notification messages” for display to a user “indicating that the device has been quarantined.” EX1004, 4:56-63, 21:1-12. The message may include “a link to a remediation server or the IP address of the remediation server.” EX1004, 21:1-12.

114. Similar to Gleichauf, Lewis also discloses the use of redirection with a client device that is quarantined. EX1006, 4:24-31. 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. EX1006, 13:7-12. 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*”). EX1006, 13:12-15. The webpage informs the user that the device “is in quarantine and corrective action must be taken.” EX1006, 10:61-66.

115. In my opinion, a POSITA would have been motivated to combine the teachings of Gleichauf, Ovadia, and Lewis and would have had the skill to do so. §IV(E) (motivation to combine). 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. The user of the quarantined device

would receive information about the quarantine reasons via a webpage served by the quarantine server. The user would then have the option to either proceed with remediation or terminate the connection attempt. 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. In the combination, HTTP traffic from a quarantined device would be redirected to a quarantine server as taught by Lewis. The quarantine server would then serve a webpage to the user, as taught by Lewis. The webpage would inform the user that the device is in quarantine (a “*quarantine notification page*”).

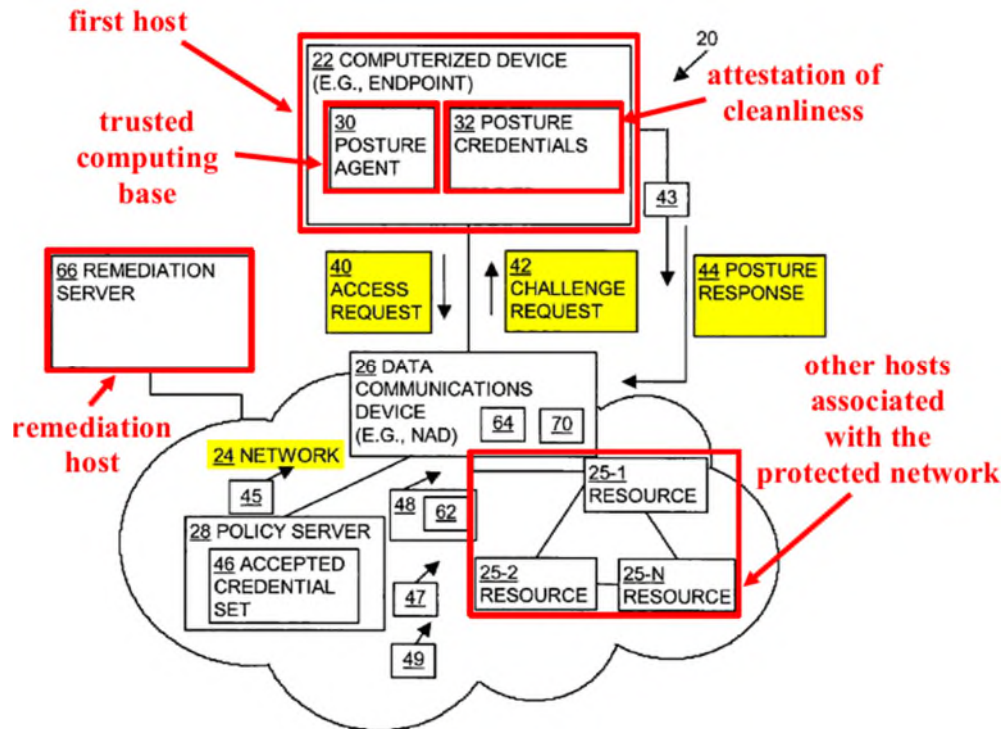
10.[1i] in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

116. In my opinion, the combination of Gleichauf and Lewis discloses and/or renders this limitation obvious.

117. As I discussed in §IV(F)(7) (limitation 1f), Gleichauf discloses that a computerized device that is out of compliance with a network admission policy is quarantined and that communications from a quarantined device to protected resources in the network are restricted or rejected. EX1004, 4:50-56, 11:58-67.

118. In my opinion, Gleichauf discloses a remediation server, shown in

Fig. 1:



EX1004, FIG. 1. 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*”). EX1004, 5:4-11. HTTP traffic from the device directed to the remediation server is permitted while HTTP traffic directed to other destinations is redirected. EX1004, 14:62-66, 15:55-67.

119. In my opinion, 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*”). 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. The device accesses a webpage by sending an HTTP request to the DNS-resolved IP address. These steps were commonly known and ubiquitously employed by web browsers in the prior art. EX1010, 5:49-63.

120. Further, Lewis describes a “hijack DNS component 421 for intercepting DNS queries from quarantined clients.” EX1006, 11:15-17. The operation of the hijack DNS component is such that “[w]henver the client performs name resolution on any address, it will receive the IP [address] of QS [quarantine server].” EX1006, 14:22-23. As discussed at [1h], Lewis’s quarantine server (QS) provides a default webpage including a *quarantine notification*. 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. EX1006, 10:61-66, 13:12-15. Thus, in my opinion, the IP address of Lewis’s quarantine server is *an IP address of a quarantine server configured to serve the quarantine notification*.

121. Additionally, 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. EX1004, 5:4-13; EX1007, 13:12-17, 14:17-31. In my

opinion, it would have been well understood and obvious to a POSITA that communications with such servers would be preceded by a DNS request to resolve the remediation server's name into its IP address. 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. The domain name must first be resolved, using DNS, into the server's IP address. The IP address is then specified as the destination for the IP packet. In my opinion, a POSITA would have been familiar with the use and operation of DNS.

122. 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.” EX1004, 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. In my opinion, 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. 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. Thus, in my opinion, 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.*

123. In my opinion, a POSITA would have been motivated to combine the teachings of Gleichauf, Ovadia, and Lewis and would have had the skills to do so. §IV(E) (motivation to combine). 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. 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.” EX1004, 21:8-12. Gleichauf further explains that the “link” to the remediation server would be provided as a Universal Resource Link (URL). EX1004, 21:3-4. It was well known that a “URL typically includes the domain name of the provider of the identified resource.” EX1013, 9:12-14. Thus, in my opinion, 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. It would have been obvious and understood 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. 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).

11.[1j] permitting the first host to communicate with the remediation host.

124. In my opinion, Gleichauf discloses this limitation.

125. As I explained in §IV(F)(7) (limitation 1f), 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. EX1004, 4:50-56, 11:58-67. HTTP traffic from the device to a remediation server is permitted, however (i.e., “*permitting the first host to communicate with the remediation host*”). EX1004, 14:62-66.

G. Claim 2 - A method as recited in claim 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.

126. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

127. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1*. See §IV(F) (claim 1).

128. In my opinion, Gleichauf renders obvious this additional limitation.

129. As I explained in §IV(F)(2) (limitation 1a), Gleichauf teaches that a policy server *detects an insecure condition* in the computerized device by reviewing the device's posture credentials. EX1004, 3:36-45, 11:29-32, 11:58-12:3, 14:16-34, 22:39-59.

130. 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” and is “vulnerable.” EX1004, 3:36-49, 22:54-56. The failure to show “timely execution of the anti-virus application” is another indication that the device is “vulnerable” and in an *insecure condition*. EX1004, 22:38-59. In my opinion, 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*.”

131. The posture credentials also contain information about whether the device can “resist reception or transmission of... content (spam and/or data theft).” EX1004, 8:52-56. In my opinion, a POSITA would have understood that spam is a type of “*malicious data*” because it is unsolicited. A POSITA would also have understood that the disclosed device would be “*scanned*” to determine whether the device can resist reception or transmission of spam. Furthermore, malicious data is known in the art to generate “*anomalous network traffic*.” Thus, in my opinion, a

detection of spam is a detection of anomalous network activity, and therefore is an identification of an insecure condition, thereby meeting the claim language.

132. The posture credentials further include information about the presence or absence of anti-virus software, whether the anti-virus software is up-to-date, and the status of a firewall application. EX1004, 3:36-49, 8:62-65. In my opinion, 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. 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.*”

H. Claim 3 – A method as recited in claim 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.

133. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

134. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1. See §IV(F) (claim 1).*

135. In my opinion, Gleichauf renders this additional limitation obvious.

136. As I explained in §IV(F)(2) (limitation 1a), Gleichauf teaches that a policy server *detects an insecure condition* in the computerized device by

reviewing posture credentials. EX1004, 3:36-45, 11:29-32, 11:58-12:3, 14:16-34, 22:39-59.

137. The posture credentials contain information about “operating system patches [that] are installed within the computing system” (i.e., “*updates to an operating system*”). EX1004, 3:36-49. Gleichauf explains, and in my opinion a POSITA would have known, that an outdated operating system may make the device “vulnerable” to network threats. EX1004, 1:65-2:3, 4:50-56. 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.” EX1004, 21:8-12, 5:8-11. Once remediated, the device “should be admitted” into the network. EX1004, 5:11-13. In my opinion, a POSITA would have understood (and 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.*”

I. Claim 4 - A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.

138. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

139. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1*. See §IV(F) (claim 1).

140. In my opinion, Gleichauf renders this additional limitation obvious. Gleichauf discloses a posture plugin that executes on the device and indicates a security posture. EX1004, 8:45-52. In one embodiment, the posture plugin is maintained by the operating system of the computerized device. EX1004, 8:65-67, 9:21-24. Gleichauf's policy server receives the security posture information from the posture plugin and uses these credentials to determine whether to quarantine the computerized device. EX1004, 9:29-34. A POSITA would have understood and found obvious that because the operating system has access to the posture information generated by the posture plugin, the operating system can quarantine the device upon startup, such in those situations where the computerized device has installed a new version of the operating system, but has not verified the new version with the policy server.

J. Claim 5

141. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

1. [5pre] A method as recited in claim 1, wherein permitting the first host to communicate with the remediation host includes:

142. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1*. §IV(F) (claim 1).

**2. [5a] detecting an outbound communication from the first host;
and**

143. In my opinion, Gleichauf discloses and/or renders obvious this limitation.

144. 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." EX1004, 21:5-12. The device responds to the message by activating the link and being directed to the remediation server. EX1004, 21:20-23.

145. In my opinion, 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. Gleichauf explains that data communications device 26 "is configured to **detect attempted connections** to the network 24 by the user device." EX1004, 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*." In my opinion, 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. EX1004, 13:52-65, 14:3-7, 14:20-34, 22:38-47.

3. [5b] forwarding the outbound communication if it is addressed to the remediation host.

146. In my opinion, Gleichauf discloses and/or renders this limitation obvious.

147. Gleichauf discloses that communications from a quarantined device are restricted or rejected. §IV(J)(2) (limitation 5a); EX1004, 22:38-47. A quarantined device is generally permitted to engage in HTTP communication with a remediation server. EX1004, 14:62-66. In my opinion, 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.*”

K. Claim 6

148. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

1. [6pre] A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

149. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1. See §IV(F) (claim 1).*

2. [6a] detecting an outbound communication from the first host; and

150. In my opinion, Gleichauf discloses and/or renders obvious this limitation. §IV(J)(2) (limitation 5a).

3. [6b] 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.

151. In my opinion, the combination of Gleichauf and Lewis discloses and/or renders obvious this limitation.

152. Gleichauf restricts or rejects communications from a quarantined device. EX1004, 11:58-67. 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.” EX1004, 14:62-66. In my opinion, 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*”).

153. As discussed in §IV(F)(10) (limitation 1i), Gleichauf discloses that HTTP traffic (an “*approved service*”) from the device to a remediation server is permitted. EX1004, 14:62-66. 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.” EX1004, 15:55-16:6. As I discussed above at §§IV(F)(9)-(10) (limitations 1h-1i), in my opinion, 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. EX1006, 11:15-17, 14:22-23.

L. Claim 7 – A method as recited in claim 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.

154. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

155. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1*. See §IV(F) (claim 1).

156. As explained in §IV(F)(7) (limitation 1f), Gleichauf discloses that a computerized device that is out of compliance with network admission policy is quarantined. EX1004, 4:50-56. Outbound communications from a quarantined device are not permitted to destinations that are not the remediation server. EX1004, 11:58-67, 14:62-66. From this disclosure, it would have been obvious and well understood to a POSITA that inbound communications would be similarly subject to access restrictions. 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. Since Gleichauf teaches that a device in quarantine may only communicate with remediation-related servers, it would have been obvious and understood 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”*).

157. To the extent that this claim is interpreted as requiring the blocking of all non-remediation-related traffic from reaching the device, in my opinion, this restriction would have been obvious to a POSITA. Gleichauf is concerned with limiting or preventing the risk that network resources “receive or transmit malware” **from or to** “vulnerable computerized devices.” EX1004, Abstract, 8:52-55. 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. EX1004, 4:25-26. It would thus have been obvious and understood 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. In my opinion, 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. EX1004, 14:3-7, 14:20-25.

158. Further, to the extent that Gleichauf does not explicitly disclose restricting inbound communications to quarantined devices, Lewis discloses that

the component responsible for quarantining the device (i.e., local enforcement component 314) also restricts inbound communication to the device. EX1006, 9:60-66 (“local enforcement component 314 is responsible for quarantining (i.e. restricting outside access to the local machine) when client 202 is in a quarantine state” and “is used to isolate the local client 202 from other machines” which “allows the client 202 to protect itself from being attacked if it finds itself insecure but not infected”). In my opinion, a POSITA would have found it obvious to modify Gleichauf’s system to implement Lewis’s limitations on inbound communications to provide its computerized devices with a more robust security protocol so that compromised computerized devices can protect themselves from further attacks. Such a modification would have involved the application of a known technique (restricting inbound communication) to improve similar devices (Gleichauf’s computerized device) in the same way (preventing a computerized device from being attacked from other machines on the LAN).

M. Claim 8 - A method as recited in claim 1, performed at an Internet service provider.

159. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

160. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1. See §IV(F) (claim 1).*

161. 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." EX1005, 3:50-56, 9:57-64 Network resources 25 are "servers that contain content accessible by the . . . device." EX1005, 9:65-67.

162. In my opinion, 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. The policy server determines whether to quarantine the device (by means of instructions to the data communications device) and protect the network. EX1004, 4:50-56, 10:30-33, 11:45-67. While in quarantine, the device is unable to communicate with network resources. EX1004, 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. 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." Moreover, in my opinion, it would have

been obvious for the data communications device and policy server to be owned by a company that provides Internet service.

N. Claim 9 - A method as recited in claim 1, wherein the software component on the first host is an operating system.

163. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

164. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1. See §IV(F) (claim 1).*

165. In my opinion, Gleichauf discloses this limitation for at least the reasons provided above. §IV(H) (claim 3).

O. Claim 10 - A method as recited in claim 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.

166. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

167. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1. See §IV(F) (claim 1).*

168. Gleichauf further discloses that its computerized device's posture response includes posture credentials. The posture credentials contain information about the "particular **virus software and virus definition versions**" installed on the device. EX1004, 3:36-49, 8:56-9:5. If updated software or current virus

definitions are not present, the device is quarantined and communications from it to the network will be restricted or completely rejected, because of a determination that the response does not include “*a valid . . . attestation of cleanliness.*” EX1004, 11:58-67.

P. Claim 11 - A method as recited in claim 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.

169. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

170. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] method as recited in claim 1. See §IV(F) (claim 1).*

171. As I described above in limitation 1d, Gleichauf’s 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.” §IV(F)(5) (limitation 1d). To the extent that the patches inquiry is limited to the operating system, in my opinion, a POSITA would have understood and found obvious that the same inquiry related to patch level could be made with respect to the virus software installed on the host device.

Q. Claim 12

172. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

1. [12pre] A system for protecting a network, comprising:

173. In my opinion, Gleichauf discloses this limitation.

174. 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.” EX1004, 3:4-9. 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. EX1004, 8:16-31.

2. [12a] a processor configured to:

175. In my opinion, Gleichauf discloses this limitation.

176. Gleichauf’s policy server operates to protect the network. §IV(F)(1)-(2) (limitations 1pre-1a). The policy server “includes a controller 209 formed of a memory 210 and a **processor 212**.” EX1004, 25:44-46. The processor 212 performs operations, such as those recited in limitations 12b-12l and claims 13-18 below, associated with protecting the network by reducing the risk of the network becoming infected by executing application 246 to perform the limitations described below. EX1004, 27:16-21 (“the credential analysis process 248 represents one or more portions of the logic instructions of the credential analysis

application 246 while being executed or otherwise performed on, by, or in the processor 212 within the policy server 28”).

3. [12b] detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,

177. In my opinion, Gleichauf discloses this limitation. §IV(F)(2) (limitation 1a).

4. [12c] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,

178. In my opinion, the Gleichauf-Ovadia combination discloses this limitation. §IV(F)(3) (limitation 1b).

5. [12d] [wherein detecting the insecure condition includes ...] receiving a response, and

179. In my opinion, Gleichauf discloses this limitation. §IV(F)(4) (limitation 1c).

6. [12e] [wherein detecting the insecure condition includes ...] determining whether the response includes a valid digitally signed attestation of cleanliness,

180. In my opinion, the Gleichauf-Ovadia combination discloses this limitation. §IV(F)(5) (limitation 1d).

7. [12f] 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;

181. In my opinion, Gleichauf discloses this limitation. §IV(F)(6)

(limitation 1e).

8. [12g] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,

182. In my opinion, Gleichauf discloses this limitation. §IV(F)(7)

(limitation 1f).

9. [12h] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,

183. In my opinion, Gleichauf discloses this limitation. §IV(F)(8)

(limitation 1g).

10.[12i] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and

184. In my opinion, the Gleichauf-Ovadia-Lewis combination discloses this limitation. §IV(F)(9) (limitation 1h).

11.[12j] 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

185. In my opinion, the Gleichauf-Ovadia-Lewis combination discloses this limitation. §IV(F)(10) (limitation 1i).

12.[12k] permit the first host to communicate with the remediation host; and

186. In my opinion, Gleichauf discloses this limitation. §IV(F)(11) (limitation 1j).

13.[12l] a memory coupled to the processor and configured to provide instructions to the processor.

187. In my opinion, Gleichauf discloses this limitation.

188. Gleichauf's policy server "includes a controller 209 formed of a **memory 210** and a processor 212." EX1004, 25:41-46. A POSITA would have understood that memory 210 is coupled to processor 212 because they are part of the same controller 209.

189. 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." EX1004, 26:66-27:8.

R. Claim 13 - A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by

performing one or more of the following: scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.

190. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

191. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] system as recited in claim 12. See §IV(Q) (claim 12).*

192. Furthermore, in my opinion, Gleichauf discloses and/or renders obvious this limitation. *See §IV(G) (claim 2).*

S. Claim 14 - A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.

193. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

194. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] system as recited in claim 12. See §IV(Q) (claim 12).*

195. Furthermore, in my opinion, the combination of Gleichauf and Lewis discloses and/or renders obvious this limitation. *See §IV(I) (claim 4).*

T. Claim 15 - A system as recited in claim 12, wherein the processor is configured to quarantine the first host at least in part by

preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

196. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

197. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] system as recited in claim 12. See §IV(P) (claim 12).*

198. Furthermore, in my opinion, the combination of Gleichauf and Lewis discloses and/or renders obvious this limitation. *See §IV(K) (claim 7).*

U. Claim 16 - A system as recited in claim 12, wherein the software component on the first host is an operating system.

199. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

200. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] system as recited in claim 12. See §IV(Q) (claim 12).*

201. Furthermore, in my opinion, Gleichauf discloses and/or renders obvious this limitation. *See §IV(N) (claim 9).*

V. Claim 17 - A system as recited in claim 12, 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.

202. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

203. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] system as recited in claim 12. See §IV(Q) (claim 12).*

204. Furthermore, in my opinion, Gleichauf discloses and/or renders obvious this limitation. *See §IV(O) (claim 10).*

W. Claim 18 - A system as recited in claim 17, 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.

205. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

206. As I explained above, the combination of Gleichauf, Ovadia, and Lewis discloses *[a] system as recited in claim 17. See §IV(V) (claim 17).*

207. Furthermore, in my opinion, Gleichauf discloses and/or renders obvious this limitation. *See §IV(P) (claim 11).*

X. Claim 19

208. In my opinion, the combination of Gleichauf, Ovadia, and Lewis renders this claim obvious.

1. [19pre] 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:

209. In my opinion, Gleichauf discloses this limitation.

210. Gleichauf describes how 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. EX1004, 25:46-51, 3:4-9. In my opinion, POSITA would have understood that Gleichauf’s computer program product *comprises computer instructions*.

211. As I described for claim 12, Gleichauf’s policy server operates to protect the network and directs the operation of the data communications device 26. See §IV(Q)(2) (limitation 12a). The policy server includes a “*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. EX1004, 26:66-27:8. Gleichauf’s system protects the network by reducing the risk of the network becoming infected with malware or suffering a virus outbreak. EX1004, 8:16-31.

2. [19a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,

212. In my opinion, Gleichauf discloses this limitation. §IV(F)(2) (limitation 1a).

3. [19b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,

213. In my opinion, Gleichauf discloses this limitation. §IV(F)(3) (limitation 1b).

**4. [19c] [wherein detecting the insecure condition includes...]
receiving a response, and**

214. In my opinion, the combination of Gleichauf and Ovadia discloses this limitation. §IV(F)(4) (limitation 1c).

**5. [19d] [wherein detecting the insecure condition includes...]
determining whether the response includes a valid digitally
signed attestation of cleanliness,**

215. In my opinion, Gleichauf discloses this limitation. §IV(F)(5) (limitation 1d).

**6. [19e] 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;**

216. In my opinion, the combination of Gleichauf and Ovadia discloses this limitation. §IV(F)(6) (limitation 1e).

**7. [19f] 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,**

217. In my opinion, Gleichauf discloses this limitation. §IV(F)(7) (limitation 1f).

- 8. [19g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,**

218. In my opinion, Gleichauf discloses this limitation. §IV(F)(8) (limitation 1g).

- 9. [19h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and**

219. In my opinion, the combination of Gleichauf, Ovadia, and Lewis discloses this limitation. §IV(F)(9) (limitation 1h).

- 10.[19i] 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**

220. In my opinion, the combination of Gleichauf, Ovadia, and Lewis discloses this limitation. §IV(F)(10) (limitation 1i).

- 11.[19j] permitting the first host to communicate with the remediation host.**

221. In my opinion, Gleichauf discloses this limitation. §IV(F)(11) (limitation 1j).

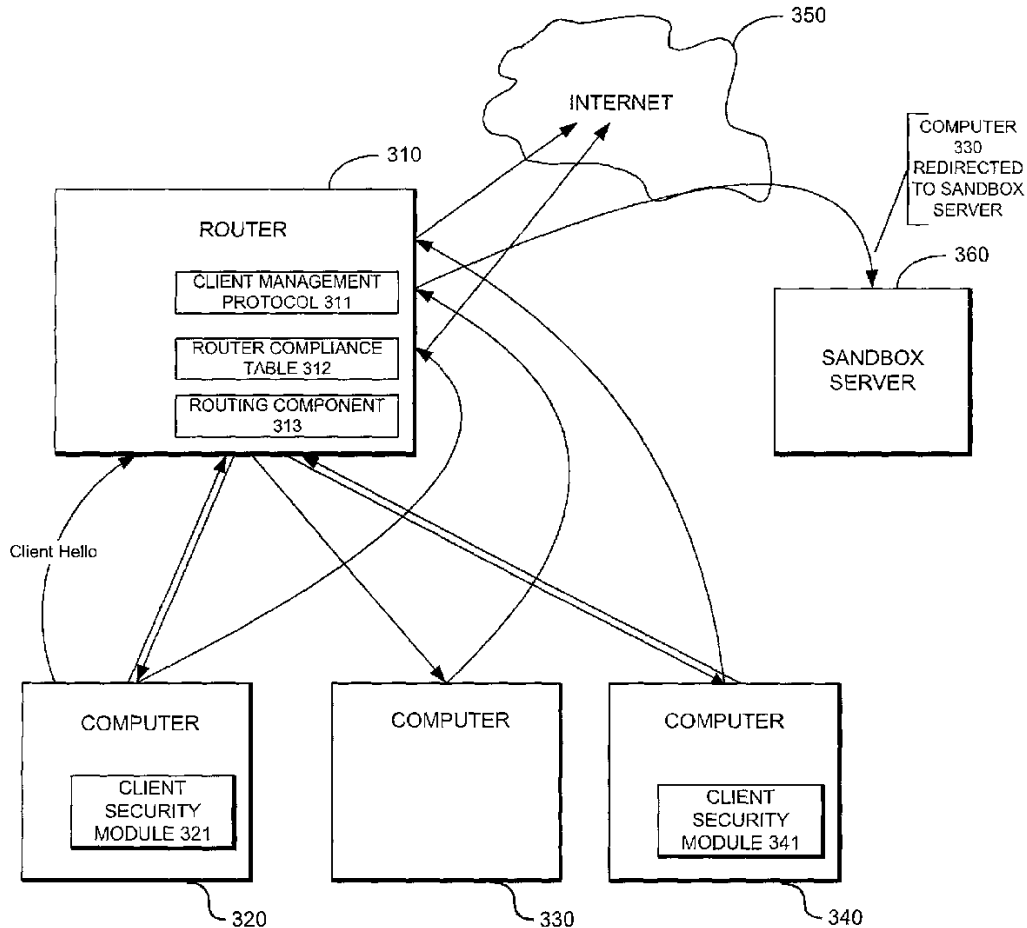
V. GROUND 2: CLAIMS 1-19 ARE OBVIOUS OVER FREUND IN VIEW OF BALL AND DANFORTH

A. Overview of Freund

222. U.S. Patent Pub. No. 2003/0055962 (“Freund”) was filed August 30, 2001 and published March 20, 2003. EX1007, cover page. I have been informed that Freund is prior art under at least 35 U.C.C. §§102(a), (b), (e).

223. Freund generally relates to systems and methods for managing and enforcing security policies for Internet access on local area networks (LANs) using a router-based enforcement mechanism. The system is designed to ensure that all client computers connected to a LAN are running required security software and are compliant with established security policies before being allowed to access the Internet. EX1007, Abstract; ¶¶39-42.

224. FIG. 3 broadly illustrates the core components of the system:



EX1007, FIG. 3.

225. As shown, the system includes a router (310) equipped with a security enforcement module, one or more client computers (320, 330, 340) connected to the router, and a sandbox server (360) accessible via the Internet. Each client computer is expected to run a client-side security module (321, 341). The router periodically issues a “router challenge” to all connected clients. If a client responds appropriately, demonstrating that the required security software is installed and operational, the router allows that client to access the Internet. If a client fails to

respond or is non-compliant, the router redirects its Internet requests to the sandbox server, which provides information and remediation steps. EX1007, ¶¶41-42, 74-78, 81. Note that “sandbox” has other connotations in computer security, commonly about providing an environment where malicious software can execute without harm, but in the context of the Freund it clearly refers to a “quarantine server” and is described at EX1007 42 as “the security module only allows the non-compliant computer to access the sandbox server to perform a defined set of tasks to address the non-compliance.”

226. In my opinion, Freund is analogous art to the '705 patent because both Freund and the '705 patent are in the same field of endeavor and describe network-based systems for enforcing security compliance and isolation of non-compliant or potentially compromised devices. EX1001, 1:38-41 (“there is a need for a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network”); EX1007, Abstract (“A centralized security enforcement module on the router maintains access rules for the client computers and verifies the existence and proper operation of a client-based security module on each client computer”). Both Freund and the '705 patent describe mechanisms for detecting whether a device meets security requirements and, if not, restricting its network access. EX1001, 3:9-13 (“a request is received from a host...to connect to a protected network....[i]t is determined whether the

host is required to be quarantined” and “[i]f the host is required to be quarantined, the host is provided only limited access to the protected network”); EX1007, ¶89 (“If the local computer is not in compliance with these policies, then the routing component invokes its re-routing manager” and “redirect[s] the local computer to the sandbox server instead of the address originally requested”).

227. Based on my review of the ’705 patent’s prosecution history (EX1003), Freund appears to have not been considered during prosecution of the ’705 patent.

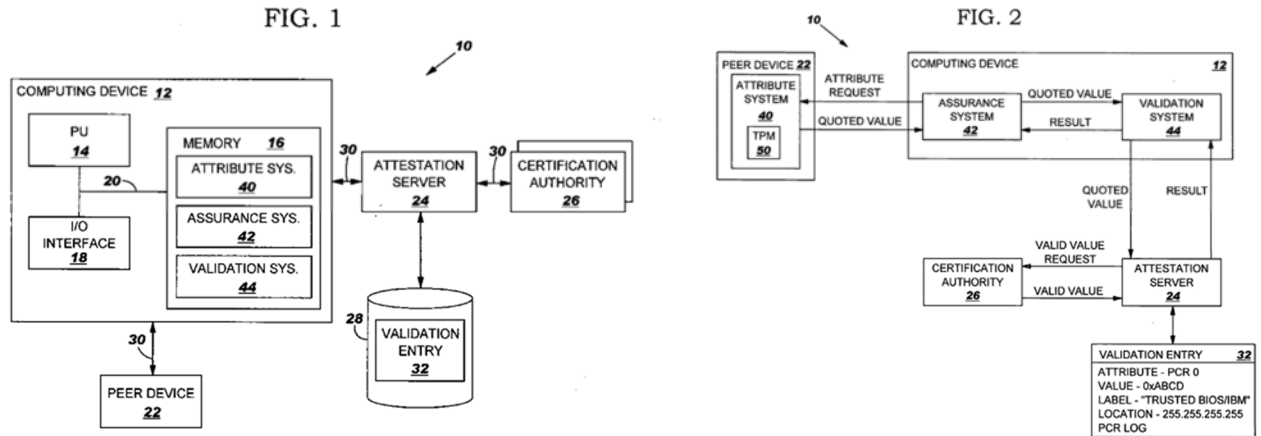
B. Overview of Ball

228. U.S. Patent Pub. No. 2006/0005009 (“Ball”) was filed June 30, 2004 and published January 5, 2006. I have been informed that Ball is prior art under at least 35 U.S.C. 102(e) (pre-AIA).

229. Ball generally relates to methods, systems, and program products for verifying an attribute of a computing device, particularly in the context of trusted computing environments. The invention addresses the need for infrastructure protocols that allow one computing device to securely and efficiently verify whether another device is trustworthy, i.e., whether it has not been compromised by malware, unauthorized access, or other threats by checking specific device attributes measured and reported by a Trusted Platform Module (TPM). EX1008, Abstract, ¶¶2-7. Ball incorporates by reference into its disclosure the entirety of

Revision 1.2 of the Trusted Computing Group's "TCG Specification Architecture Overview" (EX1014). EX1008, ¶ 6.

230. FIGS. 1-2 illustrate the core components of the system:



EX1008, FIG. 1.

231. As shown, the system includes a computing device (12) seeking to verify an attribute of a peer device (22). The peer device is equipped with a TPM (50) that measures and reports device attributes (such as hardware configuration, firmware, operating system, or integrity metrics) in the form of a "quoted value." This quoted value is cryptographically signed using an Attestation Identity Key (AIK) generated by the TPM, ensuring the authenticity and integrity of the reported attribute. EX1008, ¶6, ¶¶28-34.

232. In my opinion, Ball is analogous art to the '705 patent because both Ball and the '705 patent are in the same field of endeavor and address verification and management of the security status of computing devices within a networked

environment. EX1001, 1:38-41 (“there is a need for a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network”), EX1008, ¶5 (“it may be desired to obtain some assurances that the computing device...has not been corrupted with a virus accessed by an authorized user, or the like, i.e., that the computing device is a ‘trusted computer system’”). Both Ball and the ’705 patent rely on trusted measurements and attestations to assess whether a device is secure or compromised, and both involve mechanisms for controlling network access based on the device’s security posture. EX1001, 14:10-12 (“trusted code bases may digitally sign assertions about the cleanliness (e.g. infestation status) and/or state of their computers”); EX1008, ¶31 (“computing device 12 obtains an attribute from peer device 22 and verifies the attribute using attestation server 24” where “an ‘attribute’ can comprise any aspect of peer device 22 that another computing device...may desire to know...and could comprise any software configuration, hardware configuration, event...virus detection, etc.”).

233. Based on my review of the ’705 patent’s prosecution history (EX1003), Ball appears to have not been considered during prosecution of the ’705 patent.

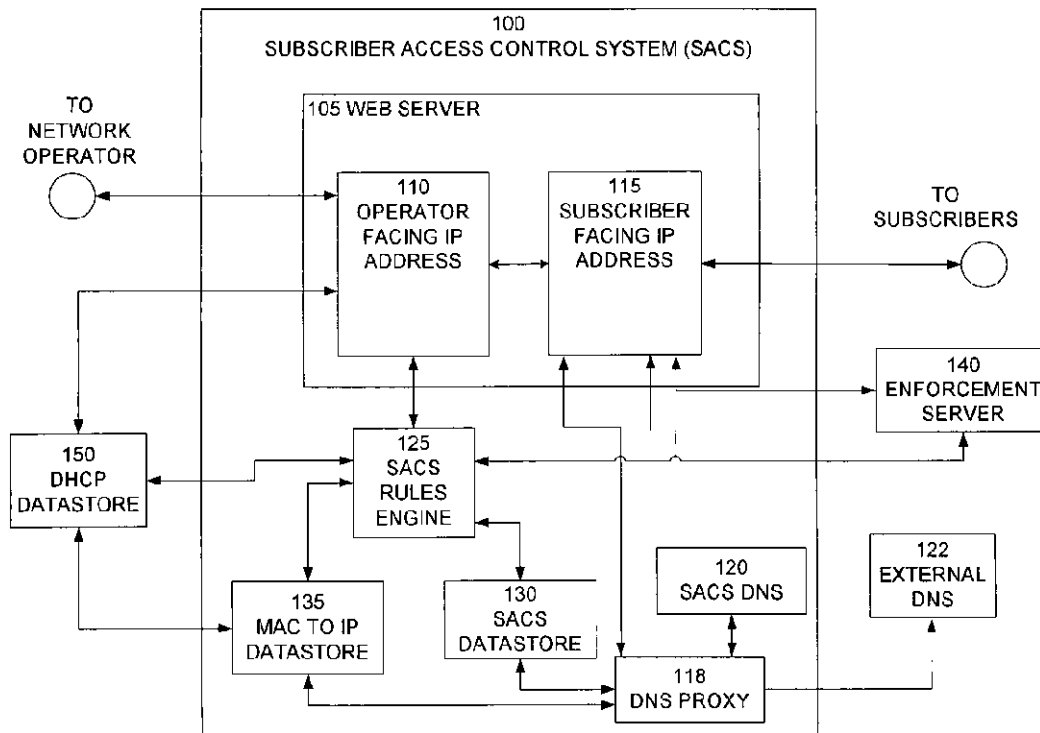
C. Overview of Danforth

234. U.S. Patent No. 7,571,460 (“Danforth”) was filed August 6, 2004 and published August 4, 2009. EX1009, cover page. I have been informed that Danforth is prior art under at least 35 U.S.C. §102(e) (pre-AIA).

235. Danforth generally relates to systems and methods for controlling and affecting the behavior of network devices (such as customer premises equipment, or CPE) connected to a cable network, particularly for the purposes of quarantine, remediation, and subscriber management. The Subscriber Access Control System (SACS) described in the patent enables network operators to dynamically isolate (quarantine) subscriber devices by modifying their network configuration, redirecting DNS queries, and applying IP filters, in order to enforce network rules, protect against misuse (such as virus spreading), and facilitate service upgrades or notifications. EX1009, Abstract, 1:41-2:3, 3:1-3:20.

236. Figure 1 broadly illustrates the core components of the SACS system:

FIGURE 1



EX1009, FIG. 1. As shown, the SACS system includes a rules engine (125), a datastore (130) for tracking subscriber states and quarantine requests, a DNS proxy server (118), a DNS server (120), a web server (105), and an enforcement server (140). Subscriber devices (such as computers or media terminal adapters) connect to the cable network and are assigned IP addresses via DHCP. When a device is quarantined, the SACS system modifies its configuration so that DNS queries are redirected to the SACS DNS server, which in turn can either return the IP address of the enforcement server (for most queries) or, in some embodiments, allow access to specific remediation or support hosts by returning their real IP addresses.

EX1009, 8:8-9:7; 9:1-9:13.

237. In my opinion, Danforth is analogous art to the '705 patent because both Danforth and the '705 patent are in the same field of endeavor and disclose systems and methods for enforcing network access control based on the compliance of security state of devices attempting to connect to a network. EX1001, 1:38-41 (“there is a need for a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network”); EX1009, 2:11-14 (“An embodiment of the present invention uses a subscriber access control system (SACS) to isolate a network device connected to cable network and to affect the behavior of that device”). Both Danforth and the '705 patent address the problem of protecting a network by dynamically restricting or redirecting access of non-compliant or potentially harmful devices, using network infrastructure to enforce security policies. EX1001, Abstract (“attempts to communicate with hosts not involved in remediation are redirected to a quarantine system, such as a server, that provides information, notices, updates, and/or instructions to the user”); EX1009, 7:64-66 (“If the subscriber device is not quarantined, the DNS proxy server 118 redirects the DNS queries to an “external” DNS server 122”).

238. Based on my review of the '705 patent's prosecution history (EX1003), Danforth appears to have not been considered during prosecution of the '705 patent.

D. Motivation to Combine

1. Freund and Ball

239. Freund is directed to protecting against compromised computers on a network, where those compromised computers provide false assurances that they are not comprised by infection or vulnerable to such compromise (or vulnerable to being compromised without detection) (§V(A) (overview of Freund)), but, in my opinion, Freund's protection is limited. Freund's client-side security module is a piece of software executing on the user's machine, which can be disabled, tampered with, or spoofed if the user's machine is compromised by malware or a sophisticated attacker, or even in situations where the software is disabled as a result of user error. EX1007, ¶68 ("all of the software that runs on a local machine is subject to being overwritten or controlled by the malicious code that is resident on the machine"), ¶19 ("even if appropriate security software is deployed, security may be at risk when one or more users inadvertently or intentionally disables his or her security software"). Accordingly, in my opinion, a POSITA would have been motivated by the teachings of Ball to modify Freund's system by moving away from Freund's software-based solution to Ball's hardware-based trusted platform module. A POSITA would have understood at the time of the purported invention that a TPM is specifically advantageous when protecting against compromised computers in a network because it is a hardware-based solution that provides

reliable, verifiable attestations from a remote computer before connecting to any such computers.

240. In my opinion, a POSITA, therefore, would have combined Freund with Ball to create an improved process for connecting to trusted computers, understanding that a hardware-based solution offers advantages that a software-based solution cannot, such as preventing malicious actors from overwriting or disabling these software-based solution. A POSITA would have combined Freund with Ball to take advantage of a standards-based solution (as opposed to a proprietary solution) that is open, supported by industry leaders, and increasingly adopted. In my opinion, a POSITA would have had a reasonable expectation of success in modifying Freund's router to include Ball's hardware-based solution because TCG's TPM, at the time of alleged invention, was a well-known hardware component that could be installed on computing devices for performing secure functions, and such a modification would have been within the technical capacity of a POSITA. Furthermore, in my opinion, this modification would have been nothing more than the use of a known technique (Ball's standards based solution) to improve Freund's host computers to provide a hardware based solution to for protecting network security.

2. Freund and Danforth

241. Freund discloses a sandbox server 360 to which the router 310 redirects a non-compliant computer. EX1007, ¶74, ¶78. Sandbox server 360 displays the non-compliant computer an error message based on the type of compliance problem detected by the router. EX1007, ¶115. Sandbox server 360 makes this determination based on the particular port sandbox server 360 received the communication packet. EX1007, ¶115. If for example, the compliance problem is a software update or a software download, sandbox server 360 presents a webpage that includes a selectable link for downloading the software update or software. EX1007, ¶116, FIGS. 7-8.

242. Danforth similarly discloses a quarantine server in the form of an enforcement server to which a quarantined client is redirected when it attempts to access a website, where the enforcement server provides a web page to the user that notifies the user of the quarantine and reasoning for being quarantined, along with what the user must do to lift the quarantine. EX1009, 3:5-7, 3:22-32, 3:57-55, 9:56-58. However, rather than Danforth's enforcement server providing links to download upgraded software, Danforth discloses a separate remediation server in the form of a "service upgrade server" that provides upgraded software to a client device that is quarantined. EX1009, 2:49-51, 9:23-28.

243. In my opinion, a POSITA would have been motivated to modify Freund's system to include separate remediation and quarantine servers to improve system performance and scalability. For example, a POSITA would have understood that software upgrades often involve the transfer of significant data. By modifying Freund's system to offload these tasks to a dedicated server, such as the remediation server, Freund's sandbox server would no longer be prone to becoming a bottleneck, particularly during mass upgrade events (e.g., a LAN with several computers requiring simultaneous security software upgrades). In my opinion, a POSITA would have had a reasonable expectation of success in modifying Freund's Internet-based system to offload remediation functionality from the sandbox server to a dedicated remediation server, as distributing tasks across servers or computing devices, at the time of alleged invention, was a well-known in the art, and such a modification would have been within the technical capacity of a POSITA.

244. Furthermore, Freund discloses that in order to re-route packets from a non-compliant computer to the sandbox server, the router modifies the packet by changing the destination IP address and port. EX1007, ¶148. This is performed so that the packet is re-routed not only to the sandbox server but to a specific port of the sandbox server based on the detected problem or condition of the non-compliant computer. EX1007, ¶95, ¶¶114-118. This process can become

cumbersome, for example, when multiple Internet access requests are received from multiple non-compliant computers, which would require Freund's router to modify each of these packets resulting in an overall slowdown of the LAN. In my opinion, a POSITA would have understood this to be a limitation of the system, and would have looked to Danforth's teachings related to DNS and redirection to replace (or augment) Freund's dependence on packet modification. It would have been obvious to a POSITA (and a POSITA would be motivated and have good reason) to apply Danforth's techniques to Freund to remove Freund's packet modification-based redirection to result in a system in which Freund's Router has a DNS system that, like Danforth, forwards DNS requests from compliant computers to the external DNS system (e.g., EX1007, FIG. 9 (boxes 960 and 980)), and also like Danforth, provides the IP address of the Sandbox Server for DNS requests from noncompliant computers that are not associated with a remediation host (while providing the IP address of a remediation host in response to a query for a domain name that is associated with a remediation host). In my opinion, a POSITA would have had a reasonable expectation of success in modifying Freund's system to apply Danforth's techniques, and such a combination would have been well within the skillset of the POSITA at the time of alleged invention. Furthermore, in my opinion, this modification is nothing more than the application of a known prior art technique (DNS-based redirection) to Freund's system to improve Freund

in a similar way (e.g., achieve the very same performance and scalability benefits Danforth already demonstrate).

E. Claim 1

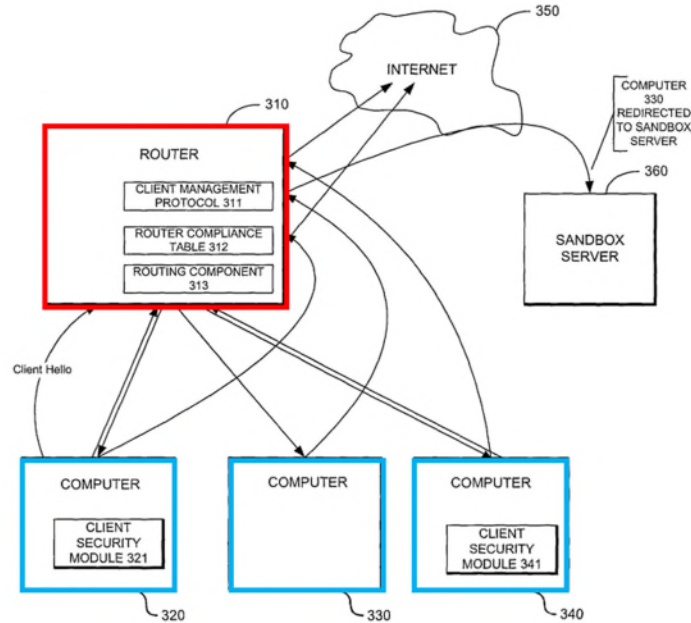
1. [1pre] A method for protecting a network, comprising:

245. In my opinion, Freund discloses this limitation. Freund discloses “methods for regulating access and maintaining security of individual computer systems and Local Area Networks (LANs) connected to larger open networks (Wide Area Networks or WANs), including the Internet.” EX1007, ¶4. Freund’s invention is “a simple, but effective solution...that can provide protection against...malicious code by denying it the ability to initiate a connection to a LAN or a Wide Area Network to transmit unauthorized code or data.” EX1007, ¶68, ¶¶147-151, FIG. 9.

2. [1a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,

246. In my opinion, Freund discloses *detecting an insecure condition* (non-compliant response) *on a first host* (first computer) *that has connected or is attempting to connect to a protected network* (LAN). EX1007, ¶71, ¶¶74-75, ¶78, ¶81, ¶85, ¶88, ¶¶126-132, ¶145, ¶147, FIG. 3.

247. Freund’s system includes a router (red) and a plurality of personal computers (blue) that connect to the Internet through the router:



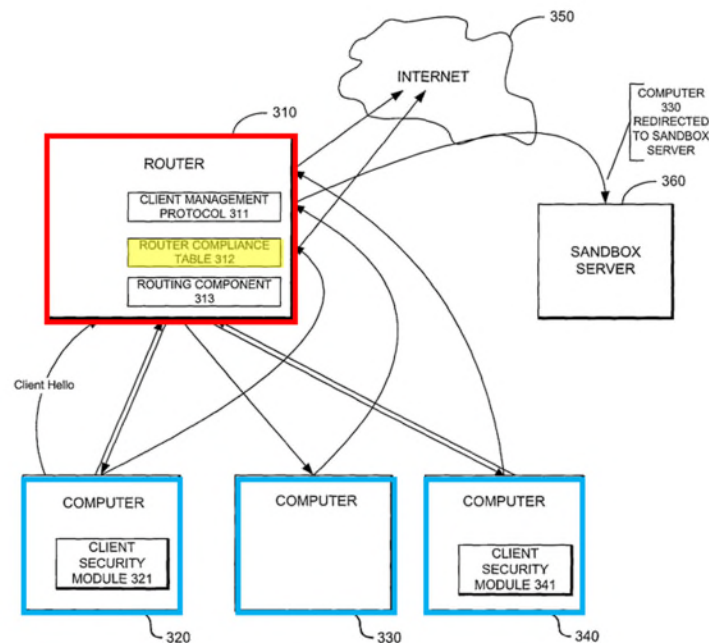
EX1007, FIG. 3, ¶74. Freund’s router enforces security rules and procedures, such as, but not limited to verifying that a computer (e.g., any of computers 320-340) “has installed and is running appropriate security software, and is in compliance with other established security policies” prior to allowing that computer to connect to the Internet. EX1007, ¶71. To determine whether a computer is compliant with the security rules and procedures, the router periodically sends a “router challenge” to the computer that requests a response from the computer within a predefined time period (e.g., “a few seconds”). EX1007, ¶75 (“Every few seconds the CMP component 311 sends out a communication via Internet broadcast to computers 320, 330 and 340 that is described as a ‘router challenge,’” which “requests a response from computers...within a few seconds), ¶¶126-132.

248. One example of the router detecting an insecure condition is if the computer does not respond to the router challenge, as this may indicate that there is no client-side security module installed on the computer, which could be the result of a Trojan horse problem. EX1007, ¶75 (“Computers 320 and 340 have the client-side security module installed and are shown on FIG. 3 as responding to the router challenge. For this example deployment, computer 330 does not respond to the router challenge, as there is no client-side security module installed on this computer”), ¶88 (“This failure to respond could result from the deactivation of the client-side security module....[t]he deactivation of the client-side security component...may be caused by a Trojan horse problem on the computer”).

Another example of the router detecting an insecure condition is if the computer does not respond to the router challenge within the prescribed amount of time. EX1007, ¶78 (“If a computer has not responded to a router challenge within the specified time frame allowed or if a computer has not answered at all, then the computer is not allowed to connect to the Internet as requested”). Yet another example of the router detecting an insecure condition is if the computer responds with an indication that it is not in compliance with a security requirement, such as not having the most up to date version of the security software. EX1007, ¶78 (“A computer may also be precluded from connecting to the Internet if it answered the router challenge with a response that indicated it was not in compliance...with one

or more of the security policy requirements indicated in the router challenge” such as “a computer running an older version of the security software may respond in the negative to a router challenge requesting confirmation that the computer is running a current version of the software”), ¶85 (“the system administrator may establish a policy requiring that a specific version of the security solution or a specific virus protection program is operational on each of these computers”), ¶132. In my opinion, a POSITA would have understood and found obvious that all these examples indicate the presence or detection thereof of an insecure condition as defined by the Client Management Protocol (CMP) of the router.

249. The router maintains each computer’s responses in a router compliance table (yellow):



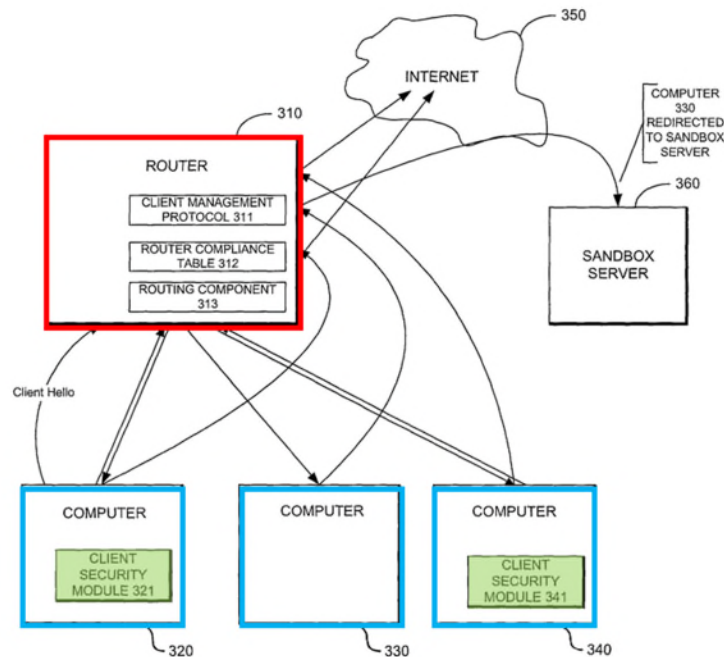
EX1007, FIG. 3, ¶86 (“The second component is a centralized table known as the “router compliance table”. Responses received by the CMP from each client machine are entered into the router compliance table.”). Freund detects an insecure condition when a computer attempts to connect to the Internet by cross-referencing the computer’s previous responses in the router compliance table. EX1007, ¶81 (“The currently preferred embodiment also includes a sandbox server to which non-compliant computers are re-directed when they attempt to connect to the Internet”), ¶147 (“In step 910, a connection attempt from one of the local computers to the Internet is received by the router...in step 930 the CMP looks up the router compliance table entry under the client computer source IP address....[and] [i]n step 940, the CMP evaluates the response in the router compliance table”), ¶145 (“Every time a client computer attempts a connection with the Internet, the router-side security module will look up the value in the router response table and verify that the client has Internet access”).

3. [1b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,

250. In my opinion, the combination of Freund and Ball discloses *wherein detecting the insecure condition (non-compliant response) includes contacting a trusted computing base (TPM) associated with a trusted platform module within*

the first host (computer). EX1007, ¶¶74-75, ¶¶91-93, FIG. 3; EX1008, ¶6, ¶27, ¶30, FIG. 2.

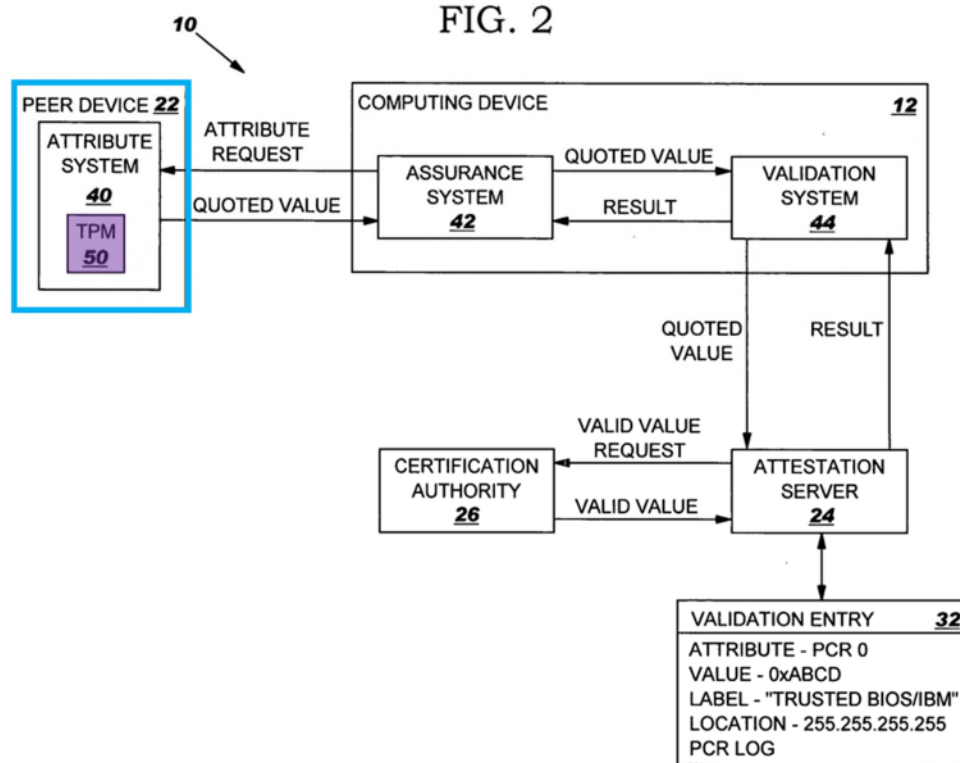
251. One or more of Freund's computers 320, 330, 340 include a client security module (green):



EX1007, FIG. 3 (“client security module 321”), ¶74. In operation, Freund’s router contacts the computer’s client security module installed thereon when the router sends the “router challenge” message to the computer. EX1007, ¶75 (“Computers 320 and 340 have the client-side security module installed and are shown on FIG. 3 as responding to the router challenge” and “[f]or this example deployment, computer 330 does not respond to the router challenge, as there is no client-side security module installed on this computer”), ¶¶91-93 (“The client-side security

module has two main functions...[f]irst the client-side security module can determine if a device is a local device connected on the same LAN...[and] [t]he second set of functions for this client-side security module is handling the receipt of router challenges and responding to these router challenges”). Because the client security module is a piece of software that is utilized to provide security in Freund’s computing environment by receiving and responding to router challenges, in my opinion, the client security module constitutes the claimed “trusted computing base.” §III(D)(1) (construction of “trusted computing base”).

252. In my opinion, to the extent that Freund does not expressly disclose that the client security module is *associated with a trusted platform module in the first host*, Ball discloses this functionality. In particular, Ball discloses a Trusted Platform Module (TPM) (purple) on a computing device (blue):



EX1008, FIG. 2, ¶27, ¶30. TPM is a hardware component that “comprises a passive device that is installed in a computing device, and which can accurately measure, securely store, and securely communicate information on one or more attributes of the computing device.” EX1008, ¶6. The TPM is compliant with Trusted Computing Group (TCG) Specification Architecture overview. EX1008, ¶6 (“The [TCG] specification...is described in detail in a document entitled “TCG Specification Architecture Overview,” Rev. 1.2, 28 Apr. 2004, which...calls for a computing device to be built with an integrated Trusted Platform Module (TPM)”). Ball’s TPM stores cryptographic keys for encrypting information sent to another computing device. EX1008, ¶6 (“the TPM can create an Attestation Identity Key

(AIK) that is used to encrypt the attribute information and authenticate identification when the attribute information is communicated to another computing device”). The Trusted Platform Module specification describes a trusted platform module that includes various components for performing cryptographic operations. Accordingly, in my opinion, Ball’s TPM constitutes the claimed *trusted platform module*. §III(D)(2) (construction of “trusted platform module”).

253. In my opinion, a POSITA would have been motivated by the teachings of Ball to modify Freund’s teachings regarding computer devices in its protected network by including Ball’s hardware-based trusted platform module. §V(D) (motivation to combine).

4. [1c] receiving a response, and

254. In my opinion, Freund discloses *receiving a response*. EX1007, ¶75, ¶93.

255. Freund’s router receives a response from the client-security modules responsive to issuing the router challenge. EX1007, ¶75 (“Computers 320 and 340 have the client-side security module installed and are shown on FIG. 3 as responding to the router challenge”), ¶93 (“The second set of functions for this client-side security module is handling the receipt of router challenges and responding to these router challenges”), Abstract (“If the client-side security

module is installed and properly operating, the client-side security module responds to the router challenge”).

5. [1d] determining whether the response includes a valid digitally signed attestation of cleanliness,

256. Freund discloses *determining whether the response* (response to router challenge) *includes a valid digitally signed* (encrypted) *attestation of cleanliness* (indication that the computer is in compliance with security policy requirements indicated in the router challenge). EX1007, ¶78, ¶122, ¶127, ¶134, ¶144.

257. Freund’s router receives encrypted responses from a computer’s client security module responsive to sending the computer a router challenge. EX1007, ¶122 (“Every packet is encrypted using the router's key and decrypted using the client computer's key or vice versa”), ¶127 (“The router challenge packet is encrypted by the router's public key” and “is decrypted by the client computer using the client's private key”), ¶134 (“The router-side security module...decrypts, verifies and interprets each client response and stores the result in its router compliance table”). The response from the computer can include an indication of whether the computer is in compliance with the security policy requirements indicated in the router challenge. EX1007, ¶78 (“A computer may also be precluded from connecting to the Internet if it answered the router challenge with a response that indicated it was not in compliance in some particular manner with one or more of the security policy requirements indicated in the router challenge”).

When the router receives the encrypted response, the router checks whether the response is valid. EX1007, ¶144 (“Unless the result is ‘Packet invalid’ the result is stored in the router compliance table”). In my opinion, a POSITA would have understood and found obvious that encrypting the client response that includes an indication of whether the computer is in compliance with the security policy requirements indicated in the router challenge is digitally signed through the encryption process using the router’s public key.

258. To the extent that merely encrypting the response to the router challenge does not amount to the claimed *valid digitally signed attestation of cleanliness*, in my opinion, Ball discloses this functionality. Ball’s TPM stores cryptographic keys for encrypting information sent to another computing device. EX1008, ¶6 (“the TPM can create an Attestation Identity Key (AIK) that is used to encrypt the attribute information and authenticate identification when the attribute information is communicated to another computing device”). In my opinion, a POSITA would have understood and found it obvious to modify Freund’s computing devices to digitally sign their router challenge responses using the AIK created by Ball’s TPM because such a modification would have been the application of a known technique (Ball’s TPM) to Freund’s host devices to improve Freund in a similar way the TPM improves Ball.

6. [1e] 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;

259. In my opinion, Freund discloses this limitation. EX1007, ¶110, ¶¶121-122, ¶127, ¶132, ¶134, ¶144; §V(E)(3) (limitation 1b), §V(E)(5) (limitation 1d).

260. In my opinion, Freund discloses *wherein the valid digitally signed attestation of cleanliness* (indication that the computer is in compliance with security policy requirements indicated in the router challenge) *includes at least one of an attestation that the trusted computing based has ascertained that the first host is not infested* (response to anti-virus challenge). EX1007, ¶78, ¶102, ¶110, ¶¶121-122, ¶127, ¶132, ¶134, ¶144; §V(E)(3) (limitation 1b), §V(E)(5) (limitation 1d).

261. One of the router challenges sent by Freund's router to the trusted computer base is an "anti-virus challenge" that "allows the administrator to use the router for anti-virus enforcement and distribution." EX1007, ¶132. Examples of the fields in the "anti-virus challenge" include an indication of the antivirus product ID, antivirus version, whether antivirus auto-update enforcement is selected, whether antivirus real-time monitoring enforcement is selected, etc.:

Element	Size	Comment
Option ID	WORD	ANTI_VIRUS_CHALLENGE (= = 4)
Option size	WORD	32
Antivirus Product ID	DWORD	Code to identify AntiVirus name (TRENDMICRO = = 1)
Antivirus version	4xWORD	Optional: CMPVERS "7.0.0"
Antivirus Auto-Update Enforcement	BOOL	Optional: Boolean to identify if the Auto-Update enforcement option is selected
Antivirus Real-Time Monitoring Enforcement	BOOL	Optional: Boolean to identify if the Real-Time Monitor enforcement option is selected
Antivirus Reserved1	DWORD	Reserved
Antivirus Reserved2	DWORD	Reserved

EX1007, ¶132. Freund's trusted computer base sends a response to the router's anti-virus challenge that is encrypted by the trusted computer base. EX1007, ¶144; §V(E)(5) (limitation 1d). The response includes fields such as, but not limited to, an indication of the antivirus product ID, antivirus version, whether antivirus auto-update enforcement is selected, whether antivirus real-time monitoring enforcement is selected, etc.:

Response	Value	Comment
Client time out	1	No recent valid client response.
No client response	2	No client response ever received.
Reserved	3-32	Reserved.
ZAP version outdated	33	Client application incorrect or old.
Invalid license	34	Invalid license key, contact administrator.
License exceeded	35	Max users exceeded for license - contact administrator.
No Antivirus program installed	36	AV not installed.
Antivirus wrong version	37	AVold version.
Antivirus Auto-Update not configured	38	AV Auto-Update is not configured.
Antivirus Real-Time Monitor not running	39	AV Real-Time Monitor not running on client
Packet time stamp	>256	Current time stamp in seconds + 256

EX1007, ¶144. In my opinion, a POSITA would have understood and found obvious that real-time monitoring for viruses includes scanning the first host for computer virus infection in real-time. Therefore, if Freund's router determines that real-time monitoring is running on the computer, the client security module has ascertained that the first host is not infested.

262. To the extent that Freund does not explicitly disclose an attestation that the trusted computing base has ascertained that the first host is not infested, in my opinion, a POSITA would have had good reason to and been motivated, based on the disclosure of Freund, to include an indication of the results of the most recent virus scan in Freund's client response, where a result of no virus infection is an attestation that the first host is not infected. Freund's anti-virus software is part of the client security module within the computer. §V(E)(3) (limitation 1b). Freund explicitly provides an extensible message format for its challenge and response to enforce security policies, including the ability to modify the format (via versioning of the protocol) and to include additional options to ascertain additional anti-virus information. EX1007, ¶¶121-122, ¶127, ¶132, ¶134, ¶110. In my opinion, a POSITA would have had a good reason to make this improvement because it is simply the use of a known technique (adding fields, such as the date and result of the most recent virus scan) to improve a known product ready for improvement (Freund's extensible message client response) to yield predictable results (a

message with additional data fields). In my opinion, a POSITA would have been motivated to make such a modification to ensure that computers that were not subject to real-time monitoring for viruses still had an attestation that the computer was not infested. For the same reasons, a POSITA would have further found it obvious to modify Freund to include a determination on the router of whether the client response included an attestation that the computer was not infested, where that attestation was an acceptably recent clean virus scan result.

263. In my opinion, Freund also discloses *wherein the valid digitally signed attestation of cleanliness includes at least one of...an attestation that the trusted computing base has ascertained the presence of a path or a patch level associated with a software component on the first host* (response to anti-virus challenge). EX1007, ¶78, ¶102, ¶132, ¶144.

264. As I previously discussed above in this limitation, Freund's router issues an "anti-virus challenge" to the computer and receives a response to the challenge. EX1007, ¶132, ¶144. One of the fields in the "anti-virus challenge" and one of the fields in the response to the anti-virus challenge is related to an indication of whether the antivirus program installed on the computer is the correct version. EX1007, ¶78 ("a computer running an older version of the security software may respond in the negative to a router challenge requesting confirmation that the computer is running a current version of the software"), ¶132 ("Antivirus

version...Optional: CMPVERS '7.0.0'), ¶144 (“Antivirus wrong version”), ¶102 (“Field 404 shows an example that allows the router to enforce the requirement for the client computers to run a minimum version level of the security solution of the present invention”). In my opinion, a POSITA would have understood and found obvious that versions of a software product, such as an antivirus software, would include patches to address specific issues from the previous version of the antivirus software. To the extent that this is not explicitly disclosed in Freund, in my opinion, a POSITA would have found this feature to be nothing more than the application of a well-known technique of using patches to improve the anti-virus software product.

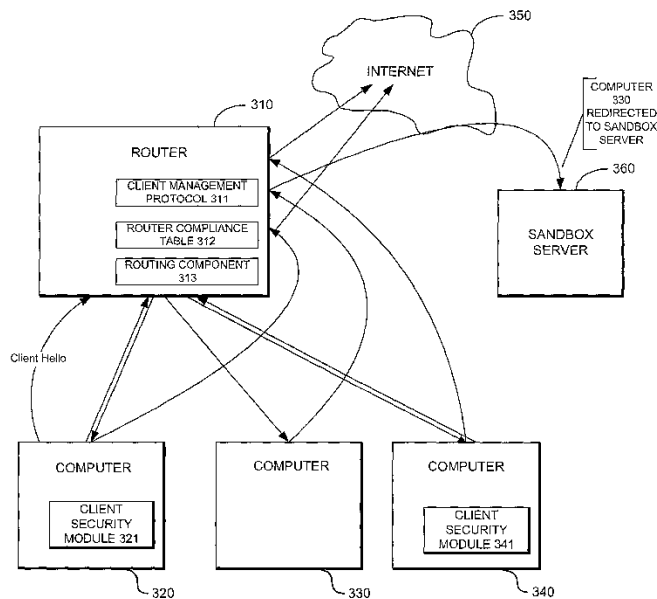
265. Therefore, in my opinion, a response that the antivirus software on the computer is the correct version of the security software is an attestation that the client security module ascertained the presence of a patch or patch level.

7. [1f] 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,

266. In my opinion, Freund discloses *when it is determined that the response does not include a valid digitally signed attestation of cleanliness (e.g., the antivirus software version is incorrect or the computer is infested), quarantining the first host (computer), including by preventing the first host*

(computer) *from sending data to one or more other hosts* (other computers)
associated with the protected network (LAN). EX1007, ¶¶74, ¶78, FIG. 3.

267. After determining that the response from the computer is not valid, Freund's router prevents the first computer from sending data to any other computers associated with the LAN. EX1007, ¶68 ("The present invention...serves to avoid or reduce the impact of Trojan horse or similar types of attacks from malicious code that may be running on a machine in the LAN"), ¶69 ("The security component on the client premises equipment serves as the traffic cop that prevents the unauthorized transfer of code or data from the local machine to a local network"), ¶78. As shown in FIG. 3 below, the router is responsible for routing packets to and from each of the computers in the LAN:

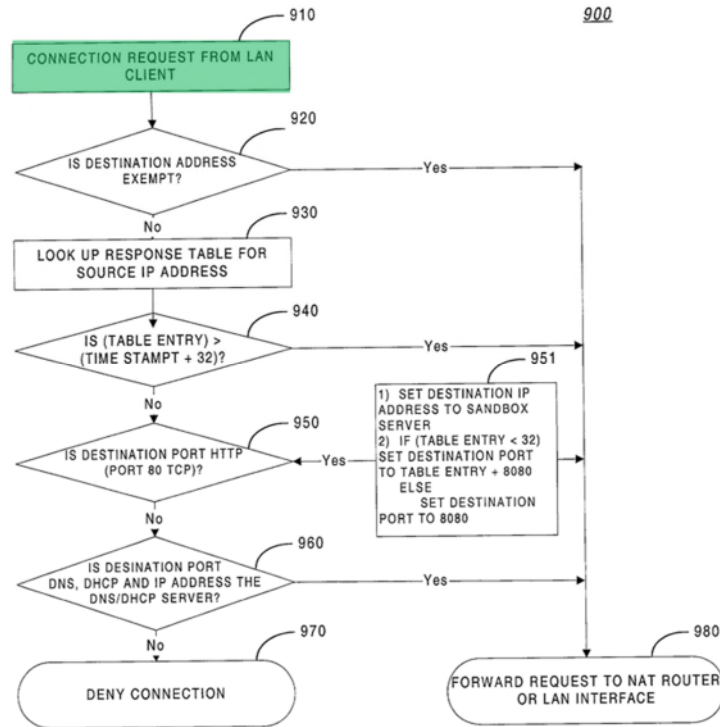


EX1007, FIG. 3, ¶74 (“The three personal computers 320, 330 and 340 connect to the Internet through router 310 via DSL or cable modem or another method of transport”). In other words, network traffic sent by the first computer 320 must first travel through the router 310 before, for example, reaching any other computer 330, 340. EX1007, FIG. 3. Accordingly, if the router determines that the first computer is not in compliance, the router prevents the first computer from sending data to the other computers in the LAN thereby “prevent[ing] the unauthorized transfer of code or data from the local machine to a local network.” EX1007, ¶69.

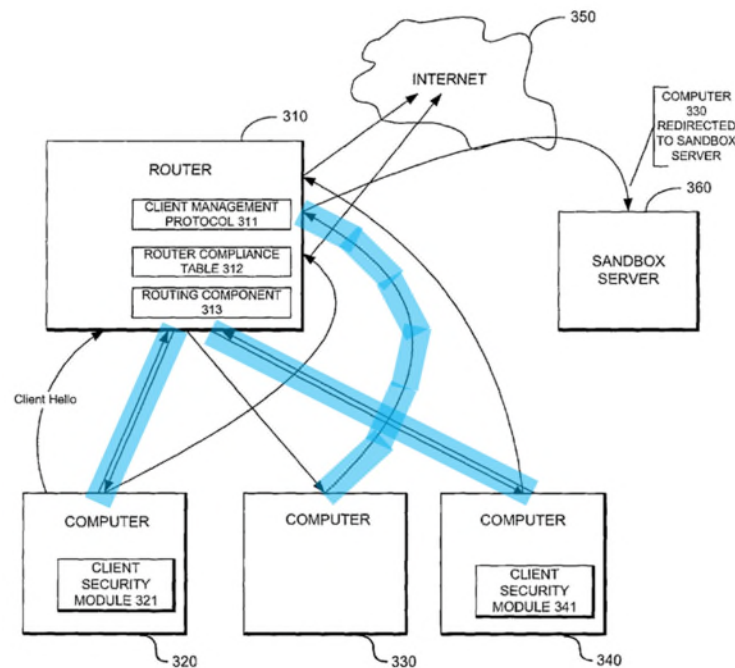
8. [1g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,

268. In my opinion, Freund discloses *wherein preventing the first host from sending data to one or more other hosts associated with the protected network* (limitation 1f) *includes receiving a service request* (connection request) *sent by the first host* (computer). EX1007, ¶147, FIG. 3, FIG. 9.

269. As part of the process for preventing the first computer from sending data to the other computers in the LAN, Freund’s router first receives a connection request from the first computer:



EX1007, FIG. 9 (block 910 (green)),

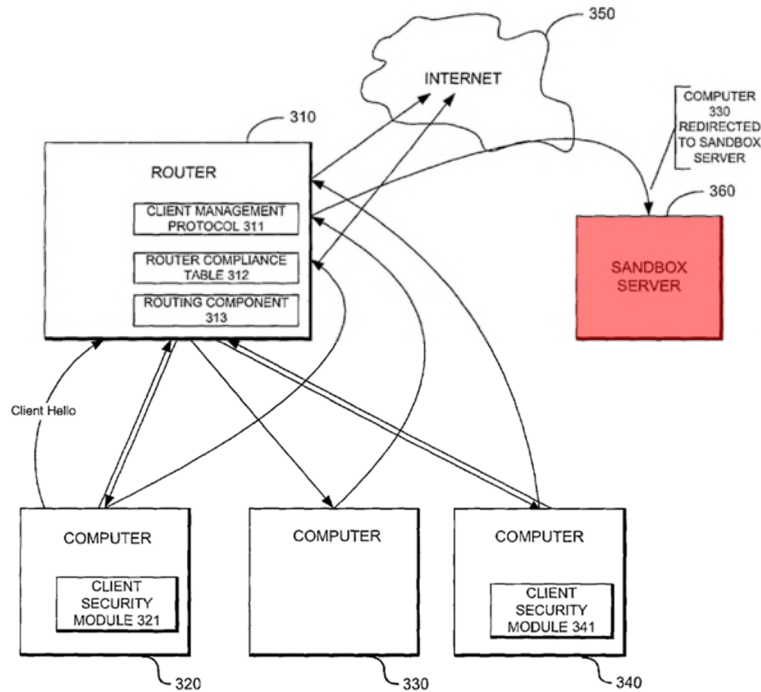


EX1007, FIG. 3 (illustrating service requests (blue)), ¶147 (“In step 910, a connection attempt from one of the local computers to the Internet is received by the router”), FIG. 9 (block 910).

9. [1h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and

270. In my opinion, Freund discloses *serving a quarantine notification page* (sandbox webpage) *to the first host* (first computer) *when the service request* (connection request) *comprises a web server request* (HTTP request). EX1007, ¶40, ¶71, ¶78, ¶81, ¶89 ¶¶94-95, ¶¶113-115, FIG. 3, FIG. 7.

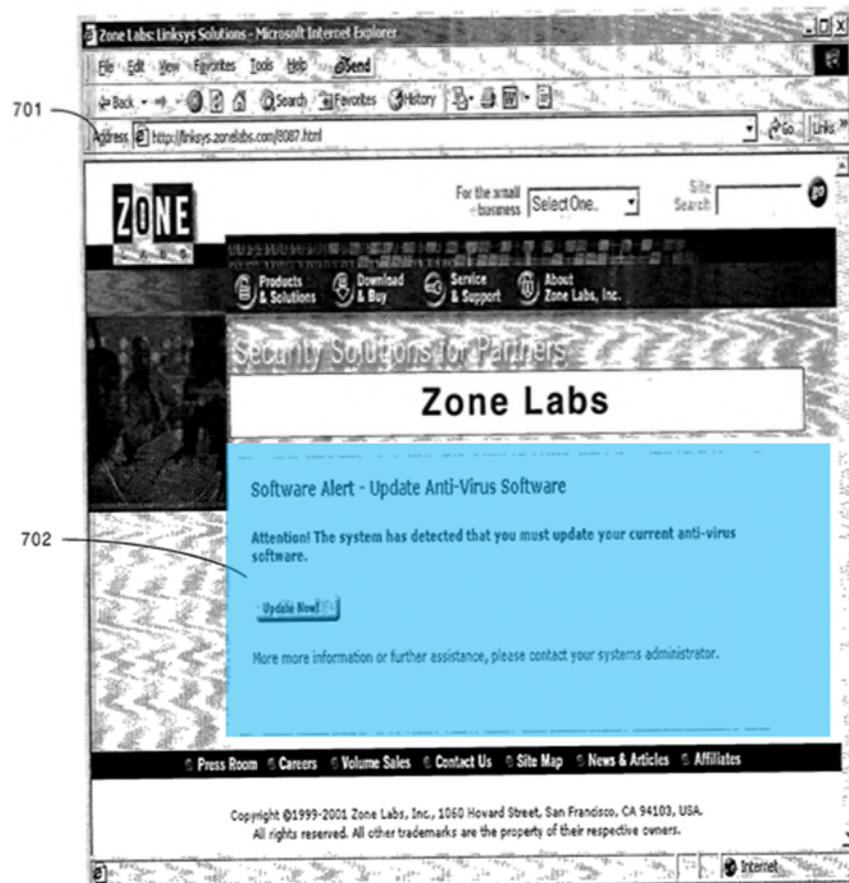
271. When Freund’s router determines that the response is not compliant, the router redirects the user’s request to a sandbox server (red):



EX1007, FIG. 3, ¶40 (“a ‘sandbox’ server is located somewhere on the Internet” and “[r]equests to connect to the Internet from non-compliant computers are redirected to the sandbox server”), ¶89 (“The re-routing manager operates to redirect the local computer to the sandbox server instead of the address originally requested”), ¶71 (“If a computer is not in compliance, then the computer's access to the Internet is restricted to those activities necessary to get the computer back into compliance...by redirecting the attempted connection by a non-compliant computer to a designated ‘sandbox’ server”). When the user is redirected to the sandbox server, they are only able to perform “a defined set of tasks to address the non compliance” and “[a]ll other Internet access by [the non-compliant] computer...is disabled.” EX1007, ¶78, ¶81, ¶¶94-95. In this manner, in my

opinion, a POSITA would have understood and found obvious that redirection to the sandbox server is serving a quarantine notification page to the non-compliant computer.

272. Indeed, when the user is redirected to the sandbox server, they are served a notification (blue) that they have been quarantined:



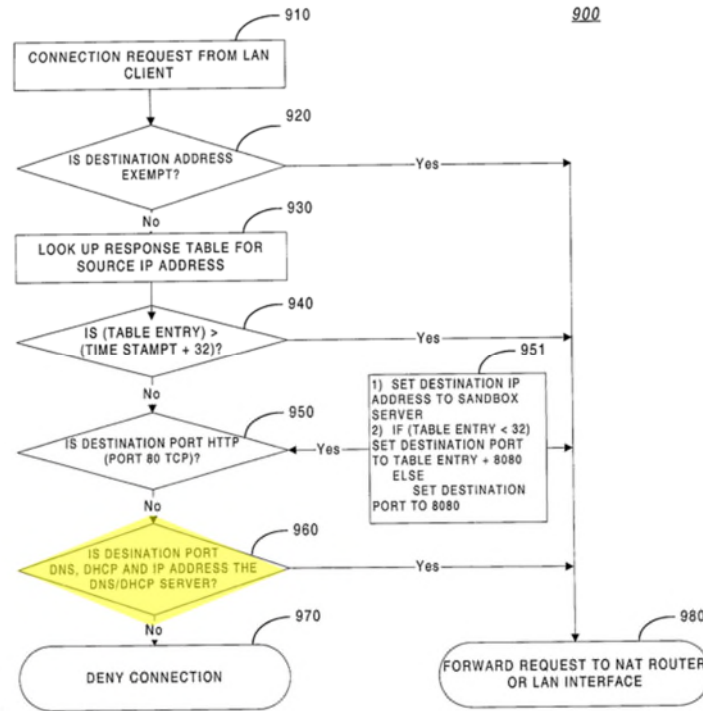
EX1007, FIG. 7, ¶195 (“When a computer is not compliant, the security solution redirects the user to the sandbox server to inform him or her of the non-compliance”), ¶114 (“the sandbox server...display[s] this window 700 to the user”

which “informs the user that he or she needs to update the virus protection software installed on the computer”), ¶113, ¶115.

10.[1i] 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

273. In my opinion, the combination of Freund and Danforth discloses *in the event the service request comprises a DNS query (DNS query), providing in response an IP address of a quarantine server (sandbox server) configured to serve the quarantine notification page (sandbox server webpage) if a host name that is the subject of the DNS query is not associated with a remediation host (antivirus software server) configured to provide data usable to remedy the insecure condition*. EX1007, ¶95, ¶102, ¶114, ¶150, FIGS. 7-9; EX1009, 4:49-54, 8:23-27, 9:23-24, 9:26-28.

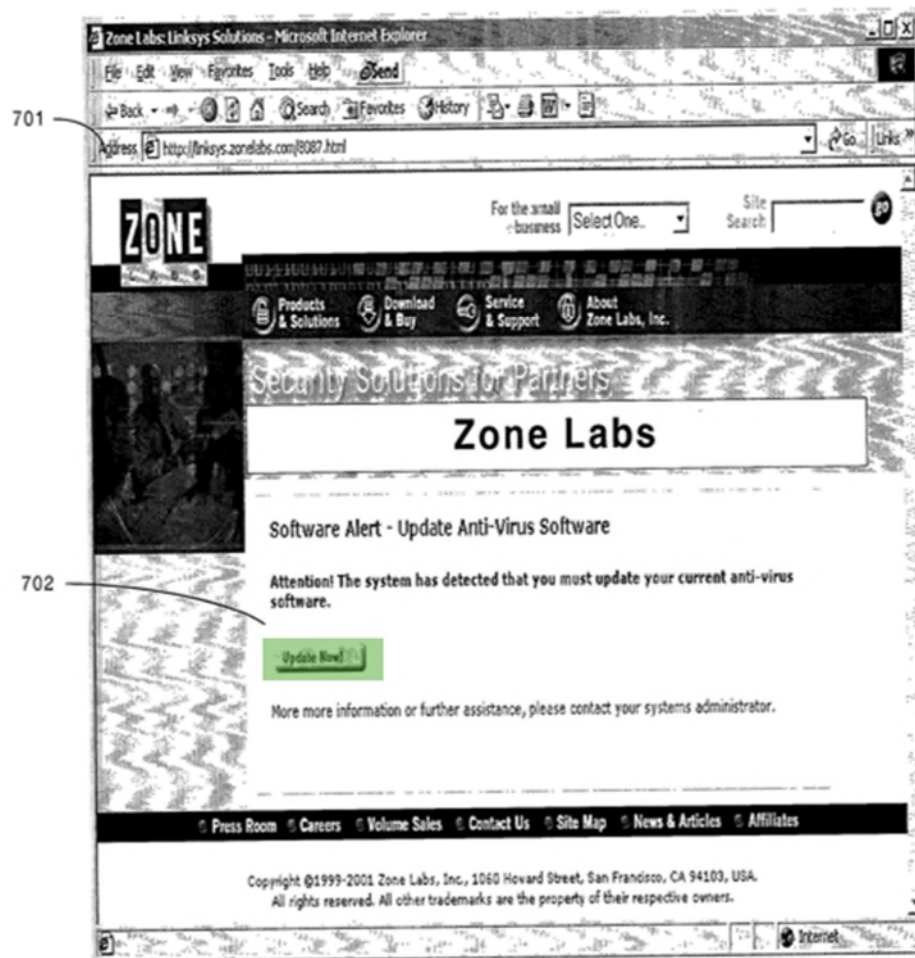
274. Freund’s router can receive a service request in the form of a DNS query (yellow):



EX1007, FIG. 9 (block 960), ¶150 (“If in step 950 the destination port was not HTTP, then the re-routing manager proceeds to step 960 to evaluate whether or not the destination port was DNS or DHCP and the destination IP address that of the DNS/DHCP server”). If the service request is a DNS query, Freund’s router allows the computer “to communicate with the DNS server regardless of whether or not compliant” otherwise “the browser [on the computer] would fail prior to being redirected to the sandbox server because it could not lookup the IP address of the sandbox server.” EX1007, ¶150. It is only after a computer in Freund’s system has the IP address and initiates an HTTP request using the IP address that the router can redirect the HTTP request to the sandbox server. EX1007, ¶95 (“When a computer is not compliant, the security solution redirects the user to the sandbox

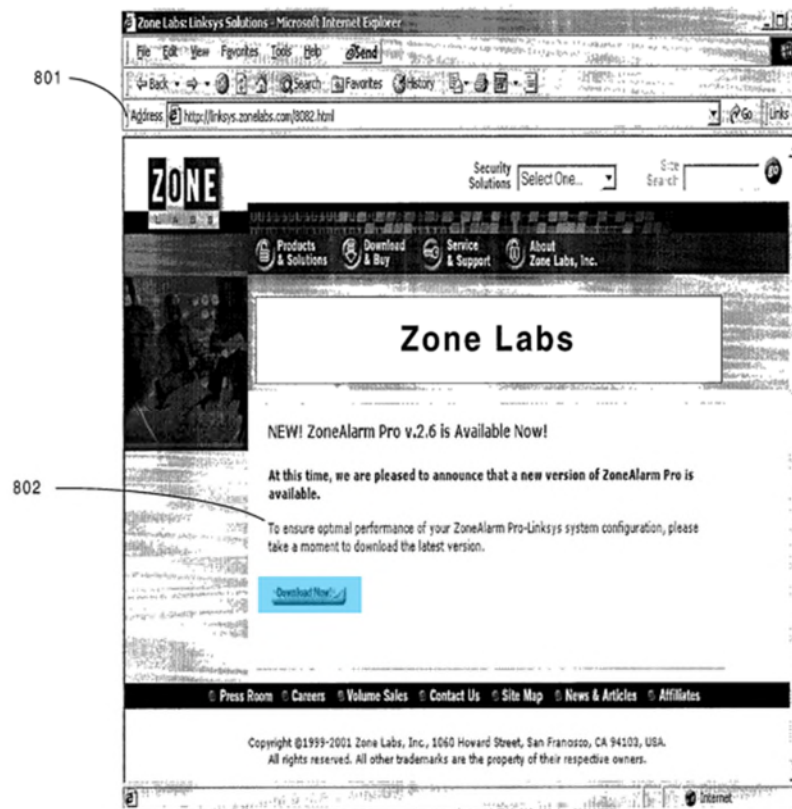
server to inform him or her of the non-compliance”), ¶114 (“the sandbox server...display[s] this window 700 to the user” which “informs the user that he or she needs to update the virus protection software installed on the computer”).

275. As shown in FIG. 7 below, when the computer is served the sandbox server webpage, the quarantine notification webpage includes a link (green) that the user can select to download a software update:



EX1007, FIG. 7, ¶114. In another example, such as when the user does not have current security software installed on their computer, the quarantine notification

webpage includes a link (blue) that the user can select to download a software update:



EX1007, FIG. 8, ¶114. Although not explicitly disclosed by Freund, in my opinion, a POSITA would have understood and found obvious that the virus protection software update or the virus protection software itself can be hosted on a server separate from the sandbox server. EX1007, ¶102 (“using the router to enforce a requirement for a totally separate piece of software, in this case a third party anti-virus program”).

276. While Freund does not explicitly disclose 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, in my opinion, Danforth discloses this limitation. Danforth discloses a system in which, when a device is quarantined, DNS queries from that device are intercepted and responded to with the IP address of a special server. EX1009, 4:49-51 (“If the current subscriber state is unquarantined, the DNS request is redirected to an external DNS server”), 4:51-54 (“If the current subscriber state is quarantined, the DNS request is forwarded to the SACS DNS server” by “respond[ing] to the DNS request with the IP address of a SACS web server”), 8:24-27 (“a quarantined device is configured such that all DNS requests are directed to the subscriber facing IP address 115 of the SACS web server 105”). SACS DNS can also be configured with a list of specific domain names that it is permitted to resolve, i.e., a list of specific domain names which the SACS DNS server is permitted to return their IP addresses. EX1009, 9:23-24 (“SACS DNS server 120 comprises a list of domain names it is permitted to resolve”). These domain names can include, for example, domain names associated with a remediation host, such as a host from which the device user can download software updates. EX1009, 9:26-28 (“the list may comprise the domain name of an enforcement server, a validation server, a virus scan server, and a service upgrade server”). In my opinion, a POSITA would have understood and found obvious to

modify Freund's router to prevent DNS queries from reaching the DNS server using the techniques taught by Danforth. §V(D) (motivation to combine). Such a modification involves the application of a known technique (interception of DNS requests from devices) to improve similar devices (Freund's user devices) in a similar way, with a reasonable expectation of success. In my opinion, a POSITA would have further understood and found obvious to modify Freund's router to include a "white list" of domain names that the SACS server is permitted to resolve, such as a service upgrade server through which the user can download the anti-virus software update or the anti-virus software package linked in the sandbox server notification webpages, and if the DNS query is for a domain name not on the "white list," to have the router respond with the IP address of the sandbox server. §V(D) (motivation to combine). Such a modification involves the application of a known technique (whitelisting access to permissible destinations in Danforth's Internet-based system) to improve similar devices (Freund's Internet-based system) in a similar way, with a reasonable expectation of success (preventing compromised devices from distributing unauthorized code to local or larger networks such as the Internet).

11.[1j] permitting the first host to communicate with the remediation host.

277. In my opinion, the combination of Freund and Danforth discloses *permitting the first host (computer) to communicate with the remediation host*

(server hosting anti-virus software update or the anti-virus software package).

When Freund's router determines the response is not compliant, the router permits users to communicate with a sandbox server that provides users with the ability to download a software update. EX1007, FIG. 3, ¶40, ¶89, ¶71. In my opinion, the Freund-Danforth combination discloses the ability of Freund's router to whitelist other domains, in addition to the sandbox server, such as the remediation host.

§V(E)(10) (limitation 1i). Accordingly, because the Freund-Danforth combination discloses whitelisting the remediation host, the Freund-Danforth combination renders obvious permitting the non-compliant device to communicate with a server hosting an anti-virus software update or the antivirus software package.

§V(E)(10)(limitation 1i); §V(D) (motivation to combine).

F. Claim 2 – A method as recited in claim 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.

278. In my opinion, the combination of Freund, Ball, and Danforth discloses this limitation.

279. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

280. In my opinion, Freund discloses this limitation. Freund discloses that a computer's response to a router challenge includes fields such as an indication of

the antivirus product ID (*determining whether a security software is stalled*) and whether antivirus real-time monitoring enforcement is selected (*scanning for a vulnerability or for malicious data*). EX1007, ¶132. A POSITA would have understood and found obvious that the presence of malicious data can result in anomalous network traffic emanating from the infected device. Accordingly, a POSITA would have understood and found obvious that the security software detecting anomalous network traffic outbound from the device is an indication of the presence of malware.

G. Claim 3 - A method as recited in claim 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.

281. In my opinion, the combination of Freund, Ball, and Danforth discloses this limitation.

282. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

283. In my opinion, Freund renders obvious this limitation. As previously discussed, one example of the router detecting an insecure condition is if the computer responds to a router challenge with an indication that it does not have the correct version of security software installed. EX1007, ¶71 ¶78 (“A computer may also be precluded from connecting to the Internet if it answered the router challenge with a response that indicated it was not in compliance...with one or

more of the security policy requirements indicated in the router challenge” such as “a computer running an older version of the security software may respond in the negative to a router challenge requesting confirmation that the computer is running a current version of the software”), ¶85 (“the system administrator may establish a policy requiring that a specific version of the security solution or a specific virus protection program is operational on each of these computers”), ¶132. While Freund does not explicitly disclose that the security policy is related to the version of the operating system executing on the computer, in my opinion, a POSITA would have understood and found obvious that Freund’s technique for quarantining a computer responsive to determining that the computer is running an older version of the security software can be applied to determining that the computer’s operating system version is not current with reasonable expectations of success.

H. Claim 4 - A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.

284. In my opinion, the combination of Freund, Ball, and Danforth renders this claim obvious.

285. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

286. In my opinion, Freund renders this additional limitation obvious.

Freund discloses that the functionality of the router can be installed “on a device that resides on the client’s premises of LAN.” EX1007, ¶69. Accordingly, in some embodiments, Freund discloses that its router-side functionality can be installed on a host, such as computer 320. In my opinion, a POSITA would have understood and found obvious that because the client management protocol 311, compliance table 312, and routing component 313 could exist on computer 320, the computer 320’s operating system can quarantine the device upon startup, such in those situations where the computer has installed a new version of the operating system, but has not verified the new version.

I. Claim 5

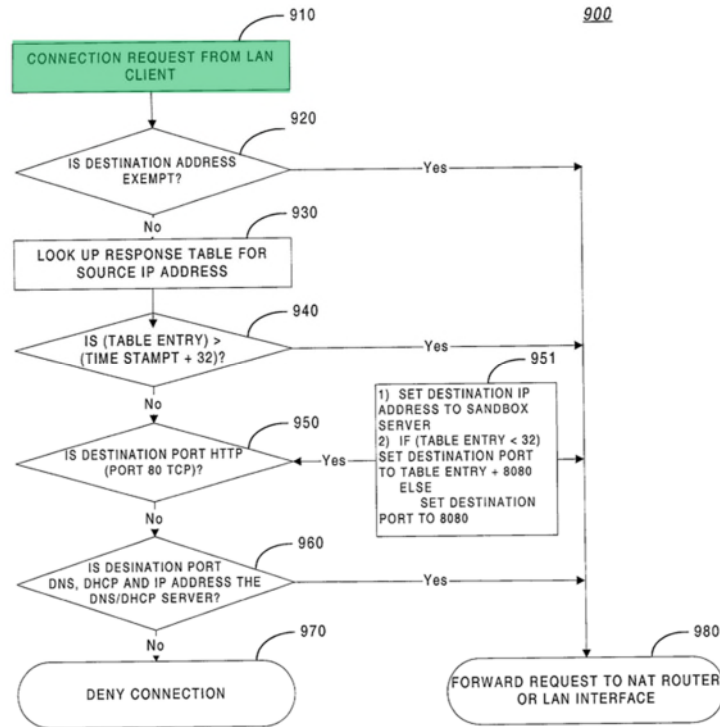
287. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

1. [5pre] A method as recited in claim 1, wherein permitting the first host to communicate with the remediation host includes:

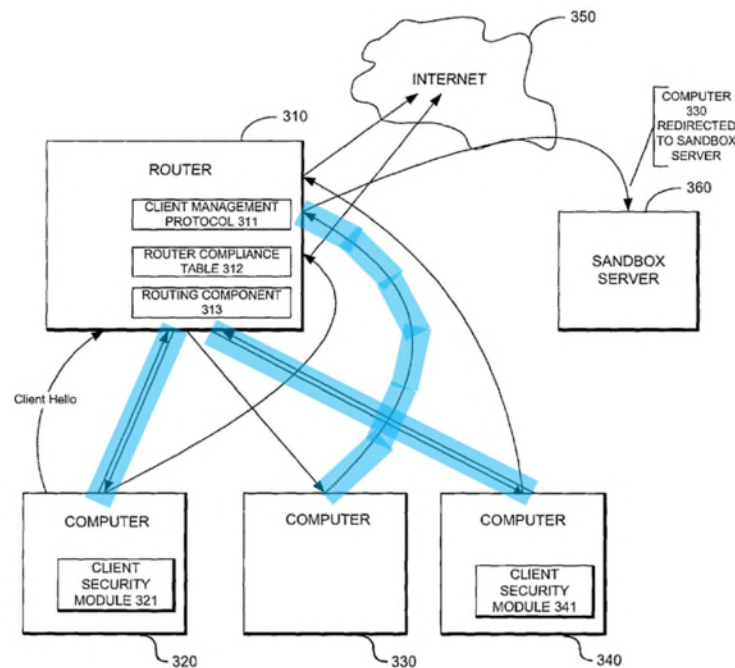
288. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

2. [5a] detecting an outbound communication from the first host; and

289. In my opinion, Freund discloses this limitation. Freund’s router first receives an outbound communication in the form of a connection request from the first computer:



EX1007, FIG. 9 (block 910 (green)),



EX1007, FIG. 3 (illustrating service requests (blue)), ¶147 (“In step 910, a connection attempt from one of the local computers to the Internet is received by the router”), FIG. 9 (block 910).

3. [5b] forwarding the outbound communication if it is addressed to the remediation host.

290. In my opinion, the combination of Freund and Danforth discloses this limitation. Danforth’s SACS DNS forwards outbound communications to the appropriate server if the outbound request is to a whitelisted set of specific domain names that it is permitted to resolve. EX1007, 9:23-24 (“SACS DNS server 120 comprises a list of domain names it is permitted to resolve”). This whitelisted set of specific domain names can include the remediation host. EX1009, 9:26-28 (“the list may comprise the domain name of... a service upgrade server”).

J. Claim 6

291. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

1. [6pre] A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes:

292. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

**2. [6a] detecting an outbound communication from the first host;
and**

293. In my opinion, Freund discloses this limitation. §V(I)(2) (limitation 5a).

3. [6b] 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.

294. In my opinion, the combination of Freund and Danforth discloses this limitation. Freund discloses redirecting requests from computers in the LAN to the sandbox server if the computer is not in compliance regardless of the type of request that is received. §V(E)(9) (limitation 1h). Freund-Danforth combination discloses exceptions to this redirect, such as if the outbound communication is addressed to a remediation host. §V(E)(10) (limitation 1i); EX1007, 9:23-24 (“SACS DNS server 120 comprises a list of domain names it is permitted to resolve”), 9:26-28 (“the list may comprise the domain name of an enforcement server, a validation server, a virus scan server, and a service upgrade server”). Accordingly, in my opinion, in the case where the request is for an approved service that is not one of the whitelisted domains, such as the service upgrade server, Freund-Danforth combination discloses redirecting this communication to the sandbox server.

K. Claim 7 - A method as recited in claim 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.**

295. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

296. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

297. In my opinion, Freund-Danforth combination discloses this limitation. Freund discloses redirecting requests from computers in the LAN to the sandbox server if the computer is not in compliance. §V(E)(9) (limitation 1h). Freund-Danforth combination discloses this redirect if the outbound communication is not addressed to a remediation host, i.e., not addressed to one of the whitelisted domains. §V(E)(10) (limitation 1i); EX1007, 9:23-24 (“SACS DNS server 120 comprises a list of domain names it is permitted to resolve”), 9:26-28 (“the list may comprise the domain name of an enforcement server, a validation server, a virus scan server, and a service upgrade server”). Accordingly, because the Freund-Danforth combination discloses only being able to access the sandbox server or a remediation server if the computer is not determined to be in compliance, in my opinion, the Freund-Danforth combination necessarily discloses preventing the computer on the LAN from receiving data not related to remediation of the determined insecure condition.

L. Claim 8 - A method as recited in claim 1, performed at an Internet service provider.

298. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

299. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

300. In my opinion, Freund discloses this limitation. In particular, Freund discloses that its computers connect to the Internet through the router. EX1007, ¶74 (“The three personal computers 320, 330 and 340 connect to the Internet through router 310 via DSL or cable modem or another method of transport), FIG. 3. In my opinion, a POSITA would have understood and found obvious that the combination of the router and DSL or cable modem constitutes an Internet service provider because the combination of elements selectively provides access to the network, which Freund describes is the Internet.

M. Claim 9 - A method as recited in claim 1, wherein the software component on the first host is an operating system.

301. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

302. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

303. In my opinion, Freund discloses this limitation. §V(G) (claim 3).

304. As I previously discussed in limitation 1e, Freund's router detects the presence or absence of security software installed on computers 320-340. EX1007, ¶75 ("Computers 320 and 340 have the client-side security module installed...computer 330 does not respond to the router challenge, as there is no client-side security module installed on this computer. Freund's router also detects the current version or patch level associated with the security software. §V(E)(6) (limitation 1e). In my opinion, POSITA would have understood and found obvious that Freund's techniques could easily be extended to software beyond security software, such as an operating system with a reasonable expectation of success. Namely, such a modification of Freund employs a simple substitution of one application type (e.g., security software) having one set of properties (e.g., versions, patch level) with another application (e.g., operating system) having the same set of properties (e.g., versions, patch level). EX1020 (showing an example security bulletin describing a security patch for Windows NT 4.0 operating system).

N. Claim 10 - A method as recited in claim 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.

305. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

306. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

307. In my opinion, Freund discloses this limitation. As I discussed in limitation 1e, one example of the response not including a valid digitally signed attestation of cleanliness is determining that the computer does not have the correct version of security software installed. EX1007, ¶¶71 ¶78 (“A computer may also be precluded from connecting to the Internet if it answered the router challenge with a response that indicated it was not in compliance...with one or more of the security policy requirements indicated in the router challenge” such as “a computer running an older version of the security software may respond in the negative to a router challenge requesting confirmation that the computer is running a current version of the software”), ¶85 (“the system administrator may establish a policy requiring that a specific version of the security solution or a specific virus protection program is operational on each of these computers”), ¶132; §V(E)(6) (limitation 1e).

O. Claim 11 - A method as recited in claim 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.

308. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

309. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] method as recited in claim 1. See §V(E) (claim 1).*

310. In my opinion, Freund discloses this limitation. As previously discussed, Freund's router issues an "anti-virus challenge" to the computer and receives a response to the challenge. EX1007, ¶132, ¶144. One of the fields in the "anti-virus challenge" and one of the fields in the response to the anti-virus challenge is related to an indication of whether the antivirus program installed on the computer is the correct version. EX1007, ¶78 ("a computer running an older version of the security software may respond in the negative to a router challenge requesting confirmation that the computer is running a current version of the software"), ¶132 ("Antivirus version...Optional: CMPVERS '7.0.0'"), ¶144 ("Antivirus wrong version"), ¶102 ("Field 404 shows an example that allows the router to enforce the requirement for the client computers to run a minimum version level of the security solution of the present invention"). In my opinion, a POSITA would have understood and found obvious that versions of a software product, such as an antivirus software, would include patches to address specific issues from the previous version of the antivirus software. Therefore, determining whether the quarantine a computer based on a response that the antivirus software on the computer is not the correct version of the security software involves a determination that the patch level associated with the software component on the first host is not sufficiently recent.

P. Claim 12

311. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

1. [12pre] A system for protecting a network, comprising:

312. In my opinion, Freund discloses this limitation. Freund discloses *a system for protecting a network*. EX1007, ¶4 (“The present invention relates...to system and methods for regulating access and maintaining security of individual computer systems and Local Area Networks (LANs) connected to larger open networks (Wide Area Networks or WANs), including the Internet”). Freund’s system is “a simple, but effective solution...that can provide protection against...malicious code by denying it the ability to initiate a connection to a LAN or a Wide Area Network to transmit unauthorized code or data.” EX1007, ¶68, ¶¶147-151, FIG. 9.

2. [12a] a processor configured to:

313. In my opinion, Freund discloses this limitation. Freund discloses *a processor*. EX1007, ¶55 (“present invention may be implemented on a conventional or general-purpose computer system” which “comprises a central processing unit(s) (CPU) or processor(s) 101”):

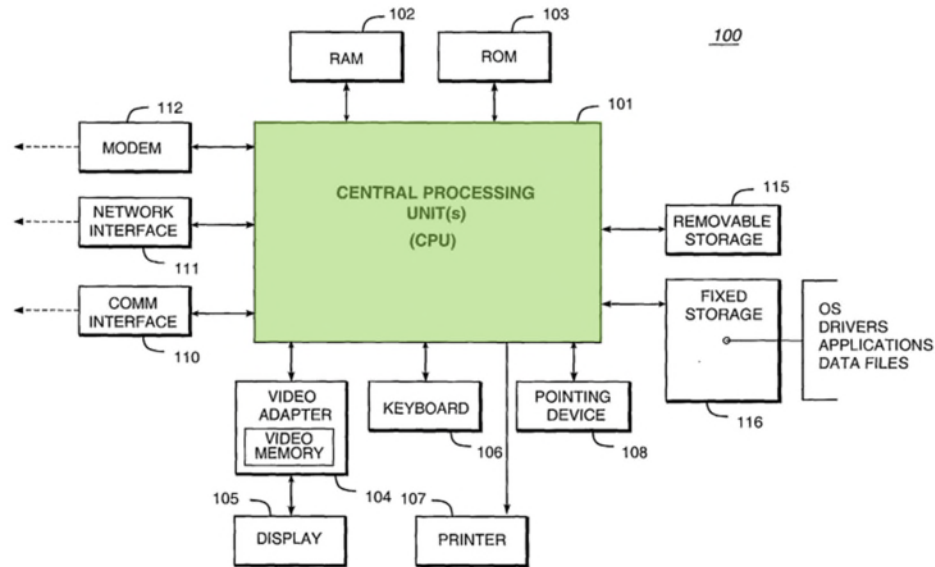


FIG. 1 (CPU 101 (green)), ¶55, ¶56. The router's processor is configured to perform operations, such as those recited in limitations 12b-12l and claims 13-18 below, by executing the program logic to implement the router-based policy enforcement techniques. EX1007, ¶58 ("program logic (including that which implements methodology of the present invention described below) is loaded from the storage device or mass storage 116 into the main (RAM) memory 102, for execution by the CPU 101"). To the extent it is argued the system 100 is not representative of router 310, in my opinion, a POSITA would have understood and found obvious that routers, such as router 310, include a processor configured to execute program logic loaded into main memory. *See, e.g.*, EX1021 (illustrating a generic router architecture that includes a routing processor).

- 3. [12b] detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,**

314. In my opinion, Freund discloses this limitation. §V(E)(2) (limitation 1a).

- 4. [12c] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,**

315. In my opinion, the combination of Freund and Ball discloses this limitation. §V(E)(3) (limitation 1b).

- 5. [12d] [wherein detecting the insecure condition includes ...] receiving a response, and**

316. In my opinion, Freund discloses this limitation. §V(E)(4) (limitation 1c).

- 6. [12e] [wherein detecting the insecure condition includes ...] determining whether the response includes a valid digitally signed attestation of cleanliness,**

317. In my opinion, Freund discloses this limitation. §V(E)(5) (limitation 1d).

- 7. [12f] 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;**

318. In my opinion, Freund discloses this limitation. §V(E)(6) (limitation 1e).

- 8. [12g] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantine the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,**

319. In my opinion, Freund discloses this limitation. §V(E)(7) (limitation 1f).

- 9. [12h] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,**

320. In my opinion, Freund discloses this limitation. §V(E)(8) (limitation 1g).

- 10.[12i] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and**

321. In my opinion, Freund discloses this limitation. §V(E)(9) (limitation 1h).

- 11.[12j] 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**

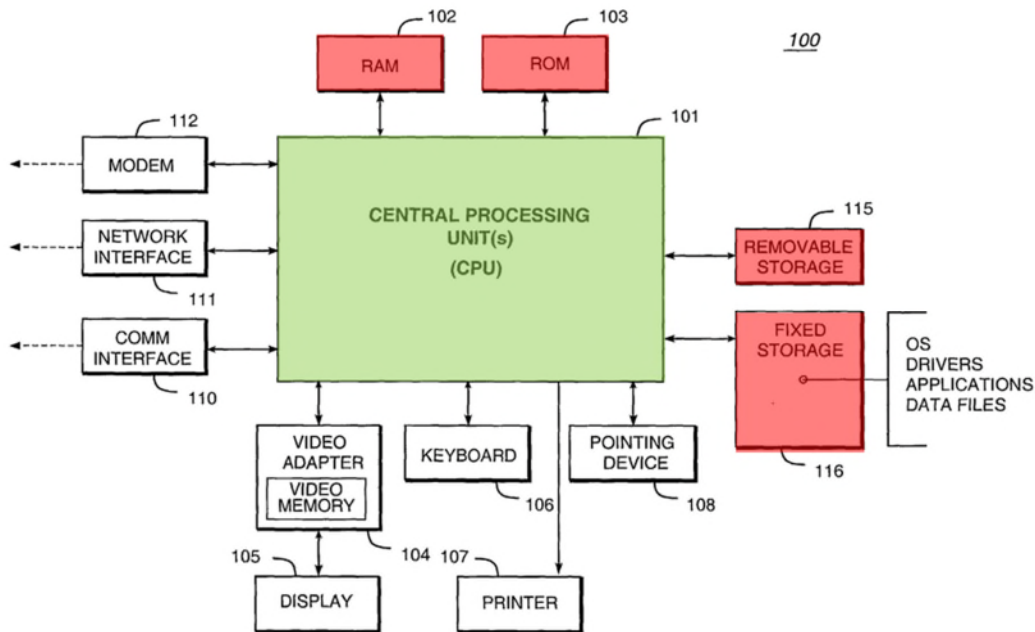
322. In my opinion, the combination of Freund and Danforth discloses this limitation. §V(E)(10) (limitation 1i).

12.[12k] permit the first host to communicate with the remediation host; and

323. In my opinion, the combination of Freund and Danforth discloses this limitation. §V(E)(11) (limitation 1j).

13.[12l] a memory coupled to the processor and configured to provide instructions to the processor.

324. In my opinion, Freund discloses this limitation. Freund discloses *a memory (fixed storage 115, 116/RAM 102/ROM (all red)) coupled to the processor (CPU 101 (green)) and configured to provide instructions to the processor:*



EX1007, FIG. 1, ¶55 (“present invention may be implemented on a conventional or general-purpose computer system” which “comprises a central processing unit(s) (CPU) or processor(s) 101,” “memory 102,” “read-only memory (ROM) 103,” and

[m]ass storage devices 115 and 116”), ¶58 (“program logic (including that which implements methodology of the present invention described below) is loaded from the storage device or mass storage 116 into the main (RAM) memory 102, for execution by the CPU 101”). To the extent it is argued the system 100 is not representative of router 310, in my opinion, a POSITA would have understood and found obvious that routers, such as router 310, include a memory coupled to the processor and configured to provide instructions to the processor.

Q. Claim 13 - A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.

325. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

326. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] system as recited in claim 12. §V(P) (claim 12).*

327. In my opinion, Freund discloses this additional limitation. §V(F) (claim 2).

R. Claim 14 - A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by

determining that an initial startup after installation of an operating system is being performed.

328. In my opinion, the combination of Freund, Ball, and Danforth renders this claim obvious.

329. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] system as recited in claim 12. See §V(P) (claim 12).*

330. Furthermore, in my opinion, Freund renders obvious this additional limitation. *See §V(H) (claim 4).*

S. Claim 15 - A system as recited in claim 12, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.

331. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

332. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] system as recited in claim 12. §V(P) (claim 12).*

333. In my opinion, Freund-Danforth combination discloses this additional limitation. *§V(K) (claim 7).*

T. Claim 16 - A system as recited in claim 12, wherein the software component on the first host is an operating system.

334. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

335. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] system as recited in claim 12. §V(P) (claim 12).*

336. In my opinion, the combination of Freund and Danforth discloses this additional limitation. §V(M) (claim 9).

U. Claim 17 - A system as recited in claim 12, 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.

337. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

338. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] system as recited in claim 12. §V(P) (claim 12).*

339. In my opinion, Freund discloses this additional limitation. §V(N) (claim 10).

V. Claim 18 - A system as recited in claim 17, 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.

340. In my opinion, the combination of Freund, Ball, and Danforth discloses this claim.

341. As I explained above, the combination of Freund, Ball, and Danforth discloses *[a] system as recited in claim 17. §V(U) (claim 17).*

342. In my opinion, Freund discloses this additional limitation. §V(O)
(claim 11).

W. Claim 19

343. In my opinion, the combination of Freund, Ball, and Danforth renders
this claim obvious.

- 1. [19pre] 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:**

344. In my opinion, Freund discloses this limitation. EX1007, ¶58
("program logic (including that which implements methodology of the present
invention described below) is loaded from the storage device or mass storage 116
into the main (RAM) memory 102, for execution by the CPU 101").

- 2. [19a] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,**

345. In my opinion, Freund discloses this limitation. §V(E)(2) (limitation
1a).

- 3. [19b] wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,**

346. In my opinion, the combination of Freund and Ball discloses this
limitation. §V(E)(3) (limitation 1b).

**4. [19c] [wherein detecting the insecure condition includes...]
receiving a response, and**

347. In my opinion, Freund discloses this limitation. §V(E)(4) (limitation
1c).

**5. [19d] [wherein detecting the insecure condition includes...]
determining whether the response includes a valid digitally
signed attestation of cleanliness,**

348. In my opinion, Freund discloses this limitation. §V(E)(5) (limitation
1d).

**6. [19e] 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;**

349. In my opinion, Freund discloses this limitation. §V(E)(6) (limitation
1e).

**7. [19f] 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,**

350. In my opinion, Freund discloses this limitation. §V(E)(7) (limitation
1f).

8. [19g] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes receiving a service request sent by the first host,

351. In my opinion, Freund discloses this limitation. §V(E)(8) (limitation 1g).

9. [19h] [wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes...] serving a quarantine notification page to the first host when the service request comprises a web server request, and

352. In my opinion, Freund discloses this limitation. §V(E)(9) (limitation 1h).

10.[19i] 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

353. In my opinion, the combination of Freund and Danforth discloses this limitation. §V(E)(10) (limitation 1i).

11.[19j] permitting the first host to communicate with the remediation host.

354. In my opinion, the combination of Freund and Danforth discloses this limitation. §V(E)(11) (limitation 1j).

VI. SECONDARY CONSIDERATIONS

355. I am not aware of any relevant information related to secondary considerations. For example, I am not aware of any attempt to commercialize the

claimed technology in a product or through licensing. To the extent Patent Owner comes forward with any such information, I will consider it.

VII. RIGHT TO SUPPLEMENT

356. I reserve the right to supplement my opinions in the future to respond to any arguments that the Patent Owner raises. This declaration represents only those opinions that I have formed to date. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information that becomes available to me and only my continuing analysis of the materials already provided.

VIII. CONCLUSION

357. I may utilize the documents cited and/or listed herein, or portions of those documents, as exhibits at any hearing or trial in this proceeding. I may further prepare and use exhibits that summarize portions of my testimony or key terms or concepts presented therein, or other demonstrative exhibits, at any hearing or trial in this proceeding.

358. I reserve the right to supplement my testimony and this report in response to any judicial determinations, in response to the arguments expressed by the Patent Owner or the opinions of the Patent Owner's experts in this proceeding, and/or in light of additional evidence or testimony brought forth at trial or otherwise brought to my attention after the date of my signature on the cover page.

EXHIBIT A

CLAY SHIELDS

CONTACT

WORK:	Department of Computer Science Georgetown University Washington, DC, 20057	HOME:	10505 MacArthur Blvd Potomac, MD, 20854
PHONE:	(202) 687-2004	CELL:	(202) 468-4335 [15in]
WEB:	http://www.cs.georgetown.edu/~clay		
EMAIL:	clay@georgetown.edu		

ACADEMIC EXPERIENCE

CURRENT	Professor, Georgetown University
2005 - 2011	Associate Professor, Georgetown University
2001 - 2005	Assistant Professor, Georgetown University One of the top teachers in the Computer Science department as rated by students. Awarded Dean's Teaching Award, 2025. Teaching classes in programming, networks, computer systems, and computer and network security. Conducting research in computer and network security, digital forensics, and on anonymous communication. PI for \$5M NSF Scholarship for Service grant that will train students in cybersecurity.
2002 - 2015	Director, Georgetown Institute for Information Assurance Initiated and led the effort that resulted in Georgetown University being declared an NSA Center of Excellence in Information Assurance. Demonstrated that Georgetown's Information Assurance curriculum met the Information Assurance Courseware Evaluation standards, then completed an accreditation process requiring coordination between information assurance faculty across schools within Georgetown. Also formed a partnership with the National Defense University to bring externally-supported graduate students into the Computer Science Master's degree program.
1999 - 2001	Assistant Professor, Purdue University Assistant professor in computer science, and associated with CERIAS, the Center for Education and Research in Information Assurance and Security. Conducted research into network forensics and anonymity. Taught courses in network security, information assurance and operating systems.
1992 - 1993	Instructor, Central Texas College Instructed fourteen distance-learning college level courses covering a variety of subjects in the Arts and Sciences for U.S. Army soldiers stationed in the Sinai. Rated as "excellent" on student evaluations.

EDUCATION

1996 - 1999	PhD in Computer Engineering, University of California at Santa Cruz Advisor: J.J. Garcia-Luna-Aceves. Dissertation: Secure Hierarchical Multicast Routing and Multicast Internet Anonymity.
1994 - 1996	Master's in Computer Engineering, University of California at Santa Cruz Master's Thesis: Ordered Core Based Trees.
1993 - 1994	University of Maryland Graduate-level course work in Computer Science.
1984 - 1989	Bachelor of Science, Electrical Engineering, University of Virginia

PROFESSIONAL EXPERIENCE

2005 - 2010	<p>Principal, Computer Litigation Resources, LLC</p> <p>Principal of consulting business for conducting forensic computer examinations and providing expert testimony on the results. Prepared and delivered forensic courses for Ernst & Young, LLP, internal training. Qualified by the 19th Judicial Circuit of Virginia as an expert witness on computer forensics.</p>
2000	<p>Staff Scientist, Cenus Technologies</p> <p>Summer Consulting on network security issues for Internet start-up.</p>
1997 - 1998	<p>Security Coordinator, University of California at Santa Cruz</p> <p>Responsible for conducting vulnerability testing, for monitoring of campus networks, and for response to security breaches. Conducted short and long-term planning for campus security systems, including investigation and testing of firewall and one-time password systems, and testing of campus certificate server system.</p>
1990 - 1993	<p>Infantry Platoon Leader, 101st Airborne Division, U.S. Army</p> <p>Platoon Leader of Rifle and Anti-Armor Infantry Platoons. Responsible for leadership of a 40 soldier platoon during tactical employment; planning and execution of safe, effective training; and accountability and maintenance of over one million dollars of equipment. Led platoon during six month deployment to the Sinai as part of the MFO peace-keeping force, and received Army Achievement medal for exceptional performance in that position.</p>

EXPERT WITNESS EXPERIENCE

INTELLECTUAL PROPERTY SECURITY, NETWORKING, COMPUTER SYSTEMS	Testifying Witness, Defendant Maxell, LTD. v. Samsung Electronics CO., LTD, Case No. 5:23-CV-00092-RWS (Eastern District of Texas) Deposed. 2024
	Testifying Witness, Defendant CUPP Cybersecurity, LLC, et al. v. Trend Micro, Inc., Case Nos. 3:18-cv-01251 and 3:20-cv-03206 (Northern District of Texas) Deposed. 2021.
	Testifying Witness, Respondent Certain Communications or Computing Devices, and Components Thereof, Case No. 337-TA-925, ITC. Deposed. 2015
	Testifying Witness, Plaintiff Before the Federal Trade Commission, In the Matter of LabMD, Inc., a corporation, Docket 9357. Deposed and testified at trial. 2014
	Consulting Witness, Plaintiff Intellectual Ventures I LLC and Intellectual Ventures II LLC v. Capital One Financial Corporation, Capital One Bank (USA) and Capital One, N.A., Civil Action No. 1:13cv740-AJT/TRJ, Eastern District of Virginia. 2013
	Consulting Witness, Defendant Droplets, Inc. v. Facebook, Inc., Civil Action No. 2:11-CV-392, Eastern District of Texas. 2012
	Testifying Witness, Plaintiff Creative Kingdoms, LLC. v. Nintendo Co., Ltd., Case No. 337-TA-770, ITC. Respondent chose not to depose or cross examine. 2011
	Consulting Witness, Plaintiff Juniper Networks Inc. v. GraphOn Corp., Case No. 1:09-cv-00287, Eastern District of Virginia, 2009
COMPUTER FORENSICS	Written report Cause No F-2569-B, 93rd Judicial District Court, Hidalgo County, TX, May 2013
	Testifying Witness, Plaintiff Facility Solutions Group v. ISM Services, Inc. Fairfax County, VA, June, 2005
	Consulting Witness, Plaintiff FTC v. D Squared Solutions, AMD 03 CV3108, 2003. (pro bono)

SCHOLARSHIP

BOOK CHAPTERS	<p>B. Levine, J. Pasquarelli, and C. Shields. "REFERENCE GUIDE ON COMPUTER SCIENCE". The Reference Manual on Scientific Evidence, 4th Edition. National Academy of Sciences. 2024. To appear.</p> <p>C. Shields. "AN INTRODUCTION TO INFORMATION ASSURANCE." Machine Learning and Data Mining for Computer Security. Ed. Marcus A. Maloof. London: Springer, 2005.</p>
JOURNAL ARTICLES	<p>A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach. "ACCOUNTABLE WIRETAPPING -OR- I KNOW THEY CAN HEAR YOU NOW.", Journal of Computer Security, 23:167-195, 2015.</p> <p>M. Liberatore, B. N. Levine, C. Shields and B. Lynn. "EFFICIENT TAGGING OF REMOTE PEERS DURING CHILD PORNOGRAPHY INVESTIGATIONS", Transactions on Dependable and Secure Computing, January, 2014.</p> <p>S. Cabuk, C. Brodley, and C. Shields. "IP COVERT CHANNEL DETECTION", ACM Transactions on Information and System Security (TISSEC) Vol. 12, Num. 22, April 2009.</p> <p>M. Wright, M. Adler, B.N. Levine, and C. Shields. "PASSIVE-LOGGING ATTACKS AGAINST ANONYMOUS COMMUNICATIONS SYSTEMS", ACM Transactions on Information and System Security (TISSEC) Vol. 11, Num. 2, March 2008.</p> <p>K. Sanzgiri, B. Dahill, D. LaFlamme, B. N. Levine, C. Shields, and E. Belding-Royer, "AN AUTHENTICATED ROUTING PROTOCOL FOR SECURE AD HOC NETWORKS", IEEE Journal on Selected Areas in Communications: Special Issue on Wireless Ad Hoc Networks. Vol. 23, Num. 3, March, 2005.</p> <p>B. Carrier and C. Shields, "THE SESSION TOKEN PROTOCOL FOR FORENSICS AND TRACEBACK", ACM Transactions on Information and System Security (TISSEC). Vol. 7 , Num. 3, August 2004.</p> <p>F. Buchholz and C. Shields, "PROVIDING PROCESS ORIGIN INFORMATION TO AID IN COMPUTER FORENSIC INVESTIGATIONS", Journal of Computer Security, Vol. 12, Num 5., 2004</p> <p>M. Wright, M. Adler, B. N. Levine, and C. Shields, "THE PREDECESSOR ATTACK: AN ANALYSIS OF A THREAT TO ANONYMOUS COMMUNICATION SYSTEMS", ACM Transactions on Information and System Security (TISSEC). Vol. 7 , Num. 4, November 2004.</p> <p>B.N. Levine and C. Shields. "HORDES - A MULTICAST BASED PROTOCOL FOR ANONYMITY", Journal of Computer Security, Vol. 10, Num. 3, 2002, pp. 213-240, by invitation.</p> <p>C. Shields and J.J. Garcia-Luna-Aceves, "A PROTOCOL FOR HIERARCHICAL MULTICAST ROUTING", Computer Communications, Vol:23. Issue: 7, March 13, 2000, pages 628-641.</p>

CONFERENCE
PAPERS

- C. Shields, "SLOWKEYS: TOWARDS SECURE DELAY AS A SYSTEMS SECURITY GOAL", in preparation.
- H. Demoulin, T. Vaidya, I. Pedisich, B. DiMaiolo, J. Qian, C. Shah, Y. Zhang, A. Chen, A. Haeberlen, B. T. Loo, L. T X. Phan, M. Sherr, C. Shields, and W. Zhou. "DEDoS: DEFUSING DoS WITH DISPERSION ORIENTED SOFTWARE". In Annual Computer Security Applications Conference (ACSAC), December 2018.
- H. Demoulin, T. Vaidya, I. Pedisich, N. Sultana, Y. Zhang, A. Chen, A. Haeberlen, B. T. Loo, L. T X. Phan, M. Sherr, C. Shields, and W. Zhou. "A DEMONSTRATION OF THE DeDoS PLATFORM FOR DEFUSING ASYMMETRIC DDOS ATTACKS IN DATA CENTERS (DEMO)". In Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM), August 2017.
- N. Carlini, P. Mishra, T. Vaidya, Y. Zhang, M. Sherr, C. Shields, D. Wagner, and W. Zhou. "HIDDEN VOICE COMMANDS". In USENIX Security Symposium (Security), August 2016.
- A. Bates, K. Butler, M. Sherr, C. Shields, P. Traynor, and D. Wallach. 'ACCOUNTABLE WIRETAPPING -OR- I KNOW THEY CAN HEAR YOU NOW'. Network and Distributed System Security Symposium (NDSS), February 2012
- C. Shields, O. Frieder, M. Maloof. "A SYSTEM FOR THE PROACTIVE, CONTINUOUS, AND EFFICIENT COLLECTION OF DIGITAL FORENSIC EVIDENCE", Proceedings of the Digital Forensics Research Conference (DFRWS), August, 2011
- M. Libertore, B.N. Levine, C. Shields. "STRENGTHENING FORENSIC INVESTIGATIONS OF CHILD PORNOGRAPHY ON P2P NETWORKS", Proceedings of the 6th International Conference on emerging Networking EXperiments and Technologies (CoNEXT), November, 2010
- M. Liberatore, R. Erdely, T. Kerle B. Levine and C. Shields. "FORENSIC INVESTIGATION OF PEER-TO-PEER FILE SHARING NETWORKS", Proceedings of the Digital Forensics Research Conference (DFRWS), August, 2010
- C. Shields. "TOWARDS PROACTIVE FORENSIC EVIDENTIARY COLLECTION", Proceedings of the Hawaii International Conference on System Sciences (HICSS), January, 2010
- C. Piro, C. Shields. B. N. Levine. "DETECTING THE SYBIL ATTACK IN MOBILE AD HOC NETWORKS", Proceedings of the Second International Conference on Security and Privacy in Communication Networks (SecureComm), Baltimore, MD, 2006
- S. Cabuk, R. M. Forte, C. Brodley, and C. Shields, "IP COVERT TIMING CHANNELS: AN INITIAL EXPLORATION", Proceedings of the ACM Computer and Communications Security Conference (CCS), October, 2004
- M. Wright, M. Adler, B. N. Levine, an C. Shields, "DEFENDING ANONYMOUS COMMUNICATION AGAINST PASSIVE LOGGING ATTACKS", in Proceedings of the 2003 IEEE Symposium on Security and Privacy (IEEE S&P), Oakland, CA, May, 2003
- B. Dahill, K. Sanzgiri, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A SECURE ROUTING PROTOCOL FOR AD HOC NETWORKS", in Proceedings of the 2002 IEEE International Conference on Network Protocols (ICNP), Paris, France, November, 2002
- B. Carrier and C. Shields, "A RECURSIVE SESSION TOKEN PROTOCOL FOR USE IN COMPUTER FORENSICS AND TCP TRACEBACK", in Proceedings of the 2002 IEEE Conference on Computer Communications (Infocom), New York, NY, June, 2002

CONFERENCE PAPERS	<p>F. Buchholz and C. Shields, "PROVIDING PROCESS ORIGIN INFORMATION TO AID IN NETWORK TRACEBACK", in Proceedings of the 2002 USENIX Annual Technical Conference, Monterey, CA, June, 2002</p> <p>M. Wright, M. Adler, B.N. Levine, and C. Shields, "AN ANALYSIS OF THE DEGRADATION OF ANONYMOUS PROTOCOLS", Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), San Diego, CA., February 2002, RECEIVED THE OUTSTANDING PAPER AWARD</p> <p>V. Scarlata, B.N. Levine, and C. Shields, "RESPONDER ANONYMITY AND ANONYMOUS PEER-TO-PEER FILE SHARING", in Proceedings of the. IEEE International Conference on Network Protocols (ICNP), 2001, Riverside, CA., November 2001</p> <p>C. Shields and B.N. Levine, "A PROTOCOL FOR ANONYMOUS COMMUNICATION OVER THE INTERNET", Proceedings of the 7th Annual ACM Conference on Computer and Communications Security (CCS), Athens, Greece, November, 2000</p> <p>C. Shields and J.J. Garcia-Luna-Aceves, "KHIP -A SCALABLE, EFFICIENT PROTOCOL FOR SECURE MULTICAST ROUTING". In Proceedings of ACM Special Interest Group on Data Communications (SIGCOMM), Boston, MA, August, 1999</p> <p>C. Shields and J.J. Garcia-Luna-Aceves, "THE HIP PROTOCOL FOR HIERARCHICAL MULTICAST ROUTING", In Proceedings of the Seventeenth Annual ACM Symposium on Principles of Distributed Computing (PODC), Puerto Vallarta, Mexico, June, 1998</p> <p>C. Shields and J.J. Garcia-Luna-Aceves, "THE ORDERED CORE BASED TREE PROTOCOL", In Proceedings of the IEEE Conference on Computer Communications (Infocom), Kobe, Japan, April, 1997</p>
WORKSHOP PAPERS	<p>T. Vaidya, E. Burger, M. Sherr, and C. Shields. "WHERE ART THOU, EVE EXPERIENCES LAYING TRAPS FOR INTERNET EAVESDROPPERS". In USENIX Workshop on Cyber Security Experimentation and Test (CSET), August 2017.</p> <p>A. Chen, A. Sriraman, T. Vaidya, Y. Zhang, A. Haeberlen, B. T. Loo, L. T. X. Phan, M. Sherr, C. Shields, and W. Zhou. "DISPERSING ASYMMETRIC DDoS ATTACKS WITH SPLITSTACK." In ACM Workshop on Hot Topics in Networks (HotNets), November 2016.</p> <p>T. Vaidya, Y. Zhang, M. Sherr, and C. Shields. "COCAINE NOODLES: EXPLOITING THE GAP BETWEEN HUMAN AND MACHINE SPEECH RECOGNITION", in USENIX Workshop on Offensive Technologies (WOOT), August 2015.</p> <p>R. Walls, B.N. Levine, M. Libertore, C. Shields "EFFECTIVE DIGITAL FORENSICS RESEARCH IS INVESTIGATOR-CENTRIC", 6th USENIX Workshop on Hot Topics in Security (HotSec), August, 2011</p> <p>C. Shields, "WHAT DO WE MEAN BY NETWORK DENIAL OF SERVICE?", Proceedings of the 2002 IEEE Workshop on Information Assurance and Security, West Point, N.Y., June, 2002</p> <p>S. Lee and C. Shields, "TRACING THE SOURCE OF NETWORK ATTACKS: A TECHNICAL, LEGAL AND SOCIAL PROBLEM", in Proceedings of the Second Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, West Point, NY., June 2001</p> <p>S. Mandujano and C. Shields, "CONFIDENTIALITY AND ANONYMITY ANALYSIS OF ON-LINE PAYMENT PROTOCOLS", Computer Security Congress, November 2000, Mexico City, Mexico</p>

U.S. PATENTS	<p>SYSTEM AND METHOD FOR DETERRING MALICIOUS NETWORK ATTACKS, US Patent US 10,482,037, C. Shields. Awarded November 19, 2019.</p> <p>SYSTEM AND METHOD FOR DETERRING MALICIOUS NETWORK ATTACKS, US Patent US 10,146,705, C. Shields. Awarded December 4th, 2018.</p> <p>SYSTEM AND METHOD FOR DETERRING MALICIOUS NETWORK ATTACKS, US Patent US 9,483,640, C. Shields. Awarded June 11, 2016.</p> <p>AUTOMATED FORENSIC DOCUMENT SIGNATURES, US Patent US 8,438,174 C. Shields, M. Maloof, and O. Frieder. Awarded May 13, 2013</p> <p>AUTOMATED FORENSIC DOCUMENT SIGNATURES, US Patent 8,312,023. C. Shields, M. Maloof, and O. Frieder. Awarded Nov 13, 2012.</p> <p>AUTOMATED FORENSIC DOCUMENT SIGNATURES, US Patent 8,280,905. C. Shields, M. Maloof, and O. Frieder. Awarded Oct 2, 2012.</p>
OTHER ARTICLES	<p>C. Shields, “ASK THE EXPERTS - HOW CAN DELETED COMPUTER FILES BE RETRIEVED AT A LATER DATE?”. Scientific American, March, 2004.</p> <p>C. Shields, “ASK THE EXPERTS - WHY DO COMPUTERS CRASH?”. Scientific American, May, 2003.</p> <p>S. C. Lee and C. Shields, “TECHNICAL, LEGAL, AND SOCIETAL CHALLENGES TO AUTOMATED ATTACK TRACEBACK”, IT Professional, May/June, 2002. pp. 12-18.</p>
SOFTWARE	<p>M. Libertore, B.N. Levine and C. Shields, ROUNDUP.</p> <p>RoundUp is a modified Gnutella client in use by various police forces to locate and create warrants for arrest for individuals sharing child pornography online. In August of 2010, RoundUp was declared part of the US National Strategy for Child Exploitation Prevention and Interdiction. In addition, as of August 2010, RoundUp was being used by over 1,224 individual investigators and 58 Internet Crimes Against Children Task Forces. As of that date, they had used RoundUp to serve 1,258 search warrants that had resulted in 567 arrests. These numbers are a lower bound based on self-reporting.</p> <p>C. Shields, E. Bloomberg, and L. Neubauer, sdttext.</p> <p>Creates portable text-based similarity digests that can identify similar files despite differences in format.</p>
TUTORIALS	<p>C. Shields and B.N. Levine, “AN OVERVIEW OF NETWORK FORENSICS INVESTIGATION WITH A FOCUS ON PEER-TO-PEER NETWORKS”. The First Annual ACM Northeast Digital Forensics Exchange. New York, NY. July 2009.</p> <p>C. Shields and B.N. Levine, “INTERNET PRIVACY AND ANONYMITY”. ACM Conference on Computer Communications Security (CCS). October 2004.</p> <p>C. Shields and B.N. Levine “INTERNET PRIVACY AND ANONYMITY”. ACM International Conference on Measurements and Modeling of Computer Systems (SIGMETRICS). June 2002.</p>

GRANTS AND
FUNDING

RENEWAL: RENEWING THE SCHOLARSHIP FOR SERVICE PROGRAM AT GEORGETOWN UNIVERSITY, National Science Foundation. Awarded 2022. \$5,440,064

SATC: CORE: SMALL: PRACTICAL AND ROBUST HIDDEN VOICE COMMANDS, National Science Foundation. Awarded 2017. \$506,313

CYBERSECURITY FELLOWS: THE SCHOLARSHIP FOR SERVICE PROGRAM AT GEORGETOWN UNIVERSITY, National Science Foundation. Awarded 2017. \$4,999,563

DEDOS: DECLARATIVE DISPERSION-ORIENTED SOFTWARE, Defense Advanced Research Projects Agency. Awarded 2016. \$1,191,113

SENIOR FACULTY RESEARCH FELLOWSHIP, Georgetown University, Washington, D.C. Awarded Spring 2016.

CC-NIE NETWORK INFRASTRUCTURE: NWIRED - NETWORK INNOVATION FOR RESEARCH AND EDUCATION AT GEORGETOWN: SCIENCE DMZ AND CLOUD SERVICES, National Science Foundation. Awarded 2014. \$452,373.

IMPROVING PARTIAL TEXT MATCHING WITH SPACE-EFFICIENT PROBABILISTIC TOKEN STORAGE, Naval Postgraduate School. Awarded 2013. \$331,985.

CC-NIE NETWORK INFRASTRUCTURE: ENABLING BIG-DATA SCIENCE COLLABORATION AT GEORGETOWN, National Science Foundation. Awarded 2013, \$379,018.

II-NEW: INFRASTRUCTURE FOR CHANGE: FROM A TEACHING DEPARTMENT TO NATIONAL PROMINENCE, National Science Foundation. Awarded 2012. \$460,000.

IMPROVING FORENSIC TRIAGE WITH RAPID TEXT DOCUMENT SIMILARITY MATCHING, Naval Postgraduate School. Award for 2010-2013. \$383,444,.

SELECTABLE ANONYMITY FOR ENABLING SAFER TELECOMMUNICATIONS (SAFEST), Defense Advanced Research Projects Agency. Award for 2010-2014 \$1,191,113.

A SYSTEM FOR IDENTIFYING AND GATHERING EVIDENCE OF P2P TRAFFICKING, U.S. Department of Justice, Washington, D.C. Awarded for \$227,502 in FY10 and \$221,104 in FY11.

INFORMATION ASSURANCE SCHOLARSHIP PROGRAM ANNEX I AND ANNEX II, National Security Agency, Fort Meade, MD. Awarded 2009. \$19,716.

PEERLESS: A SYSTEM FOR IDENTIFYING AND GATHERING EVIDENCE OF P2P TRACKING, U.S. Department of Justice, Washington, D.C. Awarded 2009. \$237,834.

RESEARCH OPPORTUNITIES FOR UNDERGRADUATES, National Science Foundation, Arlington, VA. Awarded 2005. \$5,625.

GEORGETOWN UNIVERSITY RESEARCH OPPORTUNITIES PROGRAM SUMMER RESEARCH FELLOWSHIP. Awarded Spring 2005, \$4,000.

MATCHING NETWORK DATA FLOWS. Georgetown University Research Opportunities Program, Washington, D.C. Awarded Spring 2004, \$400.

JUNIOR FACULTY RESEARCH FELLOWSHIP, Georgetown University, Washington, D.C. Awarded Fall 2003.

DETECTING THE SYBIL ATTACK IN AD HOC WIRELESS NETWORKS, Georgetown University Research Opportunities Program Awarded Fall 2003, \$400.

COLLABORATIVE RESEARCH: ANONYMOUS PROTOCOLS, National Science Foundation, Arlington, VA. \$140,000 Awarded 2001.

SERVICE

PROFESSIONAL

EDITOR

Special Issue of Computer Communications, Volume 29, Number 3, 1 February 2006

PROGRAM CHAIR

DFRWS 2012, 2013

PROGRAM COMMITTEES

ACM CCS 2013; ACSAC 2014; CNFR 2005; DFRWS 2009,2010,2011, 2014, 2015;
HICSS Forensics Minitrack Co-Chair 2011; IPCCC 2002; NDSS 2001,2002; NeFX
2009, 2010 (Workshop Chair); NGC 2001, 2002, 2003; SADFE 2009,2010,2011;
Security and Assurance in Ad hoc Networks Workshop 2003;

REVIEWER

ACM TON, SPE, IEEE Networks, IEEE Security and Privacy, Journal of Parallel
and Distributed Computing, IEEE TISSEC, IEEE TPDS, IEEE TDSC, Mobile In-
formation Systems:An International Journal, ACM SIGCOMM, IEEE INFOCOM,
Communciations of the ACM, National Science Foundation

UNIVERSITY	
2024-2025	UIS CIO Selection Committee, Promotion Committee Chair, Departmental Undergraduate Committee
2023-2024	Promotion Committee Chair, Departmental Undergraduate Committee
2022-2023	College Rank and Tenure Committee, Departmental Undergraduate Committee
2021-2022	College Rank and Tenure Committee, Departmental Undergraduate Committee
2020-2021	College Rank and Tenure Committee, MCEF Merit Policy Committee, Special Advisor to President, Departmental Undergraduate Committee
2019-2020	On sabbatical
2018-2019	First Vice Chair of Main Campus Executive Faculty, MCEF Merit Policy Committee, Chair Main Campus Executive Faculty Constitution Committee, Faculty Senate Member, Chair Departmental Hiring Committee
2017-2018	Interim Department Chair of Computer Science, First Vice Chair of Main Campus Executive Faculty, MCEF Merit Policy Committee, MCEF Constitution Committee
2016-2017	Chair of Main Campus Executive Faculty, University Budget Committee, MCEF Intellectual Life Committee, MCEF Constitution Committee
2015-2016	Chair of Main Campus Executive Faculty, University Budget Committee, Faculty Salary Plan Committee, Faculty IT Advisory Committee
2014-2015	Faculty IT Advisory Committee, Main Campus Executive Faculty
2013-2014	Director of Graduate Studies, Faculty IT Advisory Committee
2012-2013	Chair of Search Committee
2011-2012	Chair of Search Committee, Science in the Public Interest Advisory Committee
2010-2011	Chair of Search Committee, Science in the Public Interest Advisory Committee
2009-2010	ACM Chapter Advisor, Chair of Search Committee, University Research Integrity Committee, Science in the Public Interest Advisory Committee
2008-2009	On parental leave fall semester, Tenure Committee, University Research Integrity Committee
2007-2008	On sabbatical, University Research Integrity Committee
2006-2007	Curriculum Committee, University Executive Faculty, Executive Faculty Steering Committee, Search Committee, Web Committee
2005-2006	University Executive Faculty, Executive Faculty Steering Committee, University Admissions Committee, Chair of Merit Review Committee
2004-2005	University Executive Faculty, Chair of Merit Review Committee
2003-2004	Chair of Colloquim Committee, Chair of Curriculum Committee, Merit Review Committee
2002-2003	Freshman advising
PUBLIC	Puppy Raiser for Guiding Eyes for the Blind 2001-2003, 2005-2007 Media Appearances CNN 2002, Weird US 2005

TEACHING

AWARDS	Winner of Dean's Teaching Award, 2025. Awarded to top three out of about eight hundred faculty in the Georgetown College of Arts and Sciences.
GRADUATE COURSES	Doctoral Seminar in Computer Security, Blockchain: Fall 2017 Topics in Computer Security: Fall 2014, Spring 2013 Network Security: Spring 2009; Fall 1999 (Purdue) Operating Systems: Spring 2000 (Purdue)
UNDERGRAD COURSES	Introduction to Network Security: Spring 2025 Systems Programming: Fall 2024, Fall 2023, Fall 2022 Information Assurance: Fall 2024, 2015, 2012, 2010, 2009, 2000 (Purdue); Spring 2023, 2021, 2019, 2018, 2007, 2006, 2004, 2003, 2002 Operating Systems: Spring 2022, 2017, 2012, 2010, 2007, 2005, 2003, 2002, 2001 (Purdue) Computer Networks and Data Communication: Fall 2005, 2004; Spring 2010 Computer Science 1: Fall 2021, 2020, 2017, 2013, 2012, 2010, 2006, 2005, 2004, 2002, 2001; Spring 2021, 2014; Unix for Non-believers: Fall 2010, 2009 (with Mark Maloof)

CERTIFICATION

2005	ENCASE CERTIFIED EXAMINER (ENCE) Completed 64 hours of computer forensic training and the EnCase Certified Examiner program.
------	---