

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GOOGLE LLC
Petitioner

v.

K.MIZRA LLC
Patent Owner

Case No. IPR2025-01437
Patent 9,516,048

**DECLARATION OF MARKUS JAKOBSSON IN SUPPORT OF PETITION
FOR INTER PARTES REVIEW OF U.S. PATENT NO. 9,516,048**

**GOOGLE EXHIBIT 1010
Google v. K.Mizra
IPR2025-01437**

TABLE OF CONTENTS

	Page
I. BACKGROUND AND QUALIFICATIONS	2
II. INFORMATION CONSIDERED	4
III. RELEVANT LEGAL STANDARDS	4
A. Claim Interpretation	4
B. Perspective of One of Ordinary Skill in the Art.....	5
C. Anticipation	6
D. Obviousness.....	6
IV. SUMMARY OF OPINIONS.....	9
V. TECHNOLOGY BACKGROUND.....	9
VI. THE CHALLENGED '048 PATENT	10
VII. THE '048 PATENT PROSECUTION HISTORY	10
VIII. LEVEL OF ORDINARY SKILL IN THE ART	11
IX. CLAIM CONSTRUCTION	12
X. OVERVIEW OF THE PRIOR ART REFERENCES	17
A. Freund (EX1005) and Freund '611 (EX1020).....	17
B. Ball (EX1006)	18
C. Kappes (EX1007).....	19
D. Pujare (EX1009).....	20
E. Lewis (EX1013)	20
F. Kouznetsov (EX1021).....	21

XI. DETAILED EXPLANATION OF THE UNPATENTABILITY GROUNDS	21
A. Claims 1-20 Are Obvious Over Freund (EX1005) in view of Ball (EX1006), and Pujare (EX1009) (Ground 1)	21
1. Claim 1 (Preamble): “A method, comprising:”	22
a. [1.1]: “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,”	23
b. [1.2]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,”	25
c. [1.3]: “receiving a response, and”	31
d. [1.4]: “determining whether the response includes a valid digitally signed attestation of cleanliness,”	31
e. [1.5]: “wherein the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;”	33
f. [1.6]: “when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,”	37
g. [1.7]: “wherein preventing the first host from sending data to one or more other hosts associated	

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

	with the protected network includes receiving a service request sent by the first host,”	38
h.	[1.8]: “determining whether the service request sent by the first host is associated with a remediation request, and”	39
i.	[1.9]: “when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request,”	43
j.	[1.10]: “wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and”	46
k.	[1.11]: “permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.”	48
2.	Claim 2: “A method as recited in claim 1, wherein detecting the insecure condition further includes at least one of the group consisting of scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.”	49
3.	Claim 3: “A method as recited in claim 1, wherein detecting the insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.”	52
4.	Claim 4: “A method as recited in claim 1, wherein permitting the first host to communicate with the	

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

remediation host includes: detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to the remediation host.”53

5. Claim 5: “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.”57

6. Claim 6: “A method as recited in claim 1, performed at an Internet service provider.”58

7. Claim 7: “A method as recited in claim 1, wherein the software component on the first host is an operating system.”61

8. Claim 8: “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.”62

9. Claim 9: “A method as recited in claim 8, 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.”64

10. Claim 10 (Preamble): “A system, comprising:”66

a. [10.1]: “a processor configured to:”67

b. [10.2]: “detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,”67

c. [10.3]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,”67

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

- d. [10.4]: “receiving a response, and”67
- e. [10.5]: “determining whether the response includes a valid digitally signed attestation of cleanliness,”68
- f. [10.6]: “wherein the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;”68
- g. [10.7]: “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,”68
- h. [10.8]: “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,”68
- i. [10.9]: “determining whether the service request sent by the first host is associated with a remediation request, and”69
- j. [10.10]: “when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request,”69
- k. [10.11]: “wherein serving the quarantine notification page to the first host includes re-

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

	routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and”	69
l.	[10.12]: “permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition; and”	69
m.	[10.13]: “a memory coupled to the processor and configured to provide instructions to the processor.”	70
11.	Claim 11: “A system as recited in claim 10, 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.”	70
12.	Claim 12: “A system as recited in claim 10, 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.”	70
13.	Claim 13: “A system as recited in claim 10, 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.”	71
14.	Claim 14: “A system as recited in claim 10, wherein the software component on the first host is an operating system.”	71
15.	Claim 15: “A system as recited in claim 10, 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.”	72

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

- 16. Claim 16: “A system as recited in claim 15, 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.”72

- 17. Claim 17 (Preamble): “A computer program product, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:”72
 - n. [17.1]: “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,”73

 - o. [17.2]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,”73

 - p. [17.3]: “receiving a response, and”73

 - q. [17.4]: “determining whether the response includes a valid digitally signed attestation of cleanliness,”73

 - r. [17.5]: “wherein the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;”74

 - s. [17.6]: “when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,”74

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

- t. [17.7]: “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,”74
- u. [17.8]: “determining whether the service request sent by the first host is associated with a remediation request, and”74
- v. [17.9]: “when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request,”75
- w. [17.10]: “wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and”75
- x. [17.11]: “permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.”75
- 18. Claim 18: “A computer program product as recited in claim 17, wherein the software component on the first host is an operating system.”75
- 19. Claim 19: “A computer program product as recited in claim 17, 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.”76
- 20. Claim 20: “A computer program product as recited in claim 19, wherein determining that the software

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

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

XII. SECONDARY CONSIDERATIONS76

XIII. CONCLUSION.....77

APPENDIX 1

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

Exhibit No.	Description
1001	U.S. Patent No. 9,516,048, issued December 6, 2016
1002	File History of U.S. Patent Application No. 15/206,227
1003	File History of U.S. Patent Application No. 11/237,004, filed on September 27, 2005
1004	U.S. Provisional Application 60/613,909
1005	U.S. Patent Publication No. 2003/0055962, published March 20, 2003 to G. Freund et al. (“Freund”)
1006	U.S. Patent Application Publication No. 2006/0005009, published January 5, 2006 to C. Ball et al. (“Ball”)
1007	U.S. Patent Application Publication No. 2005/0111466, published May 26, 2005 to M. Kappes and P. Krishnan (“Kappes”)
1008	TCG Specification Architecture Overview
1009	U.S. Patent Application Publication No. 2002/0083183, published June 27, 2002 to S. Pujare <i>et al.</i> (“Pujare”)
1011	<i>Curriculum Vitae</i> of Markus Jakobsson
1012	U.S. Provisional Patent Application No. 60/303,653 filed July 6, 2001 (“Freund Provisional”)
1013	U.S. Patent No. 7,533,407 issued May 12, 2009 to Lewis et al. (“Lewis”)
1014	Google’s Opening Claim Construction Brief filed on August 26, 2025 in <i>K.Mizra LLC v. Google LLC</i> , Civ. Action No. 1:25-cv-00236 (W.D. Tex.)

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

Exhibit No.	Description
1015	K.Mizra’s Responsive Claim Construction Brief filed on September 16, 2025 in <i>K.Mizra LLC v. Google LLC</i> , Civ. Action No. 1:25-cv-00236 (W.D. Tex.)
1016	Final Written Decision, <i>Cisco Systems, Inc. et al. v. K.Mizra LLC</i> , IPR2021-00593, Paper 41 (PTAB Sep. 19, 2022)
1017	Federal Circuit Decision vacating Final Written Decision issued in IPR2021-00593 and remanding to PTAB, <i>Cisco Systems, Inc. et al. v. K.Mizra LLC</i> , 2022-2290, 2023-1183 (Fed. Cir. Aug. 16, 2024)
1018	Order Terminating Due to Settlement After Institution of Trial, <i>Cisco Systems, Inc. et al. v. K.Mizra LLC</i> , IPR2021-00593, Paper 51 (PTAB Jan. 30, 2025)
1019	Claim Construction Order dated October 7, 2021, <i>K.Mizra LLC v. Cisco Systems, Inc.</i> , Civ. Action No. 6:20-cv-01031 (W.D. Tex.)
1020	U.S. Patent No. 5,987,611, issued November 16, 1999 to G. Freund
1021	U.S. Patent No. 6,782,527, issued August 24, 2004 to V. Kouznetsov <i>et al</i>
1022	Decision Denying Institution of Inter Partes Review, <i>Hewlett Packard Enterprise Company v. K.Mizra LLC</i> , IPR2022-00843, Paper 14 (PTAB Oct. 31, 2022)
1023	U.S. Patent No. 8,234,705, issued July 31, 2012
1024	Claim Construction Order filed November 21, 2023 in <i>K.Mizra LLC v. Hewlett Packard Enterprise Company et al.</i> , Civ. Action No. 2:21-cv-00305 (E.D. Tex.)

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

I, Markus Jakobsson, hereby state as follows:

1. I have been retained by GOOGLE LLC (“Petitioner”) as an independent expert consultant in this *inter partes* review (“IPR”) proceeding before the United States Patent and Trademark Office (“PTO”).

2. I have been asked by Counsel for Petitioner (“Counsel”) to consider whether certain references teach or suggest the features recited in Claims 1-20 (“the Challenged Claims”) of U.S. Patent No. 9,516,048 (“the ’048 Patent”) (EX1001).

My opinions and the bases for my opinions are set forth below.

3. I understand that the ’048 Patent is assigned to K.MIZRA LLC.

4. I have been asked to provide an independent analysis of the ’048 Patent in view of the asserted prior art publications cited in the Petition. This Declaration is limited to those issues.

5. I am not, and never have been, an employee of K.MIZRA LLC or Petitioner. I am not receiving compensation for this Declaration beyond my normal hourly fees based on my time actually spent analyzing and documenting my opinions herein on the ’048 Patent, the asserted prior art publications cited in this Declaration and in the Petition, and the issues related thereto. My compensation is not related to the outcome of this proceeding, and I will not receive any additional compensation based on the outcome of any IPR or other proceeding involving the ’048 Patent.

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

6. I am being compensated at my ordinary and customary consulting rate for my work, which is \$895 per hour. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of this or any other proceeding. I have no other financial interest in this proceeding.

7. I have personal knowledge of the facts and opinions stated herein and, if called as a witness, could and would testify competently to them under oath.

I. BACKGROUND AND QUALIFICATIONS

8. All of my opinions stated in this declaration are based on my own personal knowledge and professional judgment. In forming my opinions, I have relied on my knowledge and experience in the field of malware detection and remediation, attestation, and trusted computing.

9. I am an expert in the fields of fraud detection and defense, which includes malware detection and remediation; authentication methods, which includes attestation; and trusted computing.

10. I have published extensively in the field of fraud detection and defense, including several dozens of peer-reviewed articles; textbooks, such as “Crimeware: Understanding New Attacks and Defenses” (Symantec Press); “Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft” (Wiley); and “Understanding Social Engineering Scams” (Springer). I have

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

been awarded multiple patents related to this topic, and held key positions of relevance, including Chief Scientist at Agari and Chief Scientist at ByteDance.

11. I have also done significant work in the area of authentication methods, including my PhD thesis “Privacy vs. Authenticity” (UCSD, 1997); several dozens of peer-reviewed articles; books, such as “Mobile Authentication: Problems and Solutions” (Springer) and “Towards Trustworthy Elections: New Directions in Electronic Voting” (Springer); and have been awarded a large number of patents. One of my patents, introducing the notion of “implicit authentication” was licensed by my then-employer, Xerox PARC, to Samsung, and is widely used.

12. I have, furthermore, made significant contributions to the field of trusted computing, including my work on retroactive detection of malware infection using software-based attestation. This corresponds to multiple peer-reviewed articles, as well as a company (“FatSkunk Inc.”) that I co-founded, and which was acquired by Qualcomm in 2013. Other related work includes work on securely managing biometrics, which resulted in peer-reviewed publications and patents, some of which were licensed to Samsung.

13. For a more complete overview of my contributions to these fields, as well as other fields of computer security and network security, I refer to my curriculum vitae, provided in Exhibit 1011, my Google Scholar profile, and my LinkedIn profile.

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

14. I have also served as an expert in certain legal proceedings. A list of cases in which I have testified at trial, hearing, or by deposition is provided in Appendix 1. Over the years, I have been involved in a large number of IPRs, retained by both patent owners and petitioners, as well as a large number of district court cases, retained by both patent owners and defendants.

II. INFORMATION CONSIDERED

15. In preparation for this declaration, I have considered the materials discussed in this declaration, including, for example, the '048 Patent, the references cited by the '048 Patent, the prosecution histories of the '048 Patent and applications from which it derives (including the references cited therein), various background articles and materials referenced in this declaration, and the prior art references identified in this declaration. In addition, my opinions are further based on my education, training, experience, and knowledge in the relevant field.

III. RELEVANT LEGAL STANDARDS

16. I am not an attorney and offer no legal opinions. 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. Claim Interpretation

17. I have been informed that during an *inter partes* review proceeding, claims are to be construed in light of the specification as would be read by a person

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

of ordinary skill in the relevant art at the time the application was filed. I have been informed that claim terms are given their ordinary and customary meaning as would be understood by a person of ordinary skill in the relevant art in the context of the entire disclosure. A claim term, however, will not receive its ordinary meaning if the patentee acted as his own lexicographer and clearly set forth a definition of the claim term in the specification. In that case, the claim term will receive the definition set forth in the patent.

18. I have been informed that certain patent claim terms may be interpreted as “means-plus-function” claim terms. I have been informed that terminology is part of the U.S. Patent Law in 35 USC §112, paragraph 6 (pre-AIA) / 35 USC §112(f) (post-AIA), which states the following: “An element in a claim for a combination may be expressed as a means or step for performing a specified function without the recital of structure, material, or acts in support thereof, and such claim shall be construed to cover the corresponding structure, material, or acts described in the specification and equivalents thereof.”

B. Perspective of One of Ordinary Skill in the Art

19. I have been informed that a patent is to be understood from the perspective of a hypothetical “person of ordinary skill in the art” (“POSITA”). Such an individual is considered to possess normal skills and knowledge in a particular technical field (as opposed to being a genius). I have been informed that in

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

considering what the claims of a patent require, what was known prior to that patent, what a prior art reference discloses, and whether an invention is obvious or not, one must use the perspective of such a POSITA.

C. Anticipation

20. I have been informed that a claim is not patentable if it is anticipated. I have been informed that anticipation of a claim requires that every element of a claim is disclosed expressly or inherently in a prior art reference, arranged as in the claim, when considered from the perspective of a person of ordinary skill in the relevant art. I have been informed that when the structure recited in a reference is substantially identical to that of the claims, claimed properties or functions are presumed to be inherent. I have been informed that extrinsic evidence may be used to explain but not expand the meaning of terms and phrases used in the reference relied upon as anticipatory of the claimed subject matter.

D. Obviousness

21. I have been informed that a patent claim is obvious under 35 U.S.C. §103, and therefore invalid, if the claimed subject matter, as a whole, would have been obvious to a POSITA as of the priority date of the patent based on one or more prior art references and/or the knowledge of a POSITA.

22. I have been informed that an obviousness analysis must consider (1) the scope and content of the prior art, (2) the differences between the claims and the

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

prior art, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations, if any, of non-obviousness (such as unexpected results, commercial success, long- felt but unmet need, failure of others, copying by others, and skepticism of experts).

23. I have been informed that a prior art reference may be combined with other references to disclose each element of the invention under 35 U.S.C. § 103. I have been informed that a reference may also be combined with the knowledge of a POSITA, and that this knowledge may be used to combine multiple references. I have been informed that a POSITA is presumed to know the relevant prior art. I have been informed that the obviousness analysis may take into account the inferences and creative steps that a POSITA would employ.

24. In determining whether a prior art reference would have been combined with other prior art or other information known to a POSITA, I have been informed that the following principles may be considered:

- whether the references to be combined involve non-analogous art;
- whether the references to be combined are in different fields of endeavor than the alleged invention in the Patent;
- whether the references to be combined are reasonably pertinent to the problems to which the inventions of the Patent are directed;
- whether the combination is of familiar elements according to known methods that yields predictable results;

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

- whether a combination involves the substitution of one known element for another that yields predictable results;
- whether the combination involves the use of a known technique to improve similar items or methods in the same way that yields predictable results;
- whether the combination involves the application of a known technique to a prior art reference that is ready for improvement, to yield predictable results;
- whether the combination is “obvious to try”;
- whether the combination involves the known work in one field of endeavor prompting variations of it for use in either the same field or a different one based on design incentives or other market forces, where the variations are predictable to a POSITA;
- whether there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention;
- whether the combination requires modifications that render the prior art unsatisfactory for its intended use;
- whether the combination requires modifications that change the principle of operation of the reference;
- whether the combination is reasonably expected to be a success; and
- whether the combination possesses the requisite degree of predictability at the time the invention was made.

25. I have been informed that in determining whether a combination of prior art references renders a claim obvious, it is helpful to consider whether there is some teaching, suggestion, or motivation to combine the references and a reasonable

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

expectation of success in doing so. I have been informed, however, that a teaching, suggestion, or motivation to combine is not required.

IV. SUMMARY OF OPINIONS

26. It is my opinion that Claims 1-20 of the '048 Patent are unpatentable under 35 U.S.C. §§102 and 103 on the following grounds:

Ground	Reference(s)	Basis	Claims
1	U.S. Patent Application Publication No. 2003/0055962 to G. Freund <i>et al.</i> ("Freund") (EX1005) in view of U.S. Patent Application Publication No. 2006/0005009 to C. Ball <i>et al.</i> ("Ball") (EX1006) and U.S. Patent Application Publication No. 2002/0083183 to Pujare <i>et al.</i> ("Pujare") (EX1009)	103	1-20

V. TECHNOLOGY BACKGROUND

27. The '048 Patent discloses receiving a request from a host to connect to a protected network and determining whether the host should be quarantined. If the host is quarantined, the host's requests are re-routed to a quarantine server configured to serve a quarantine notification page providing information to remedy an insecure condition that caused the quarantine. EX1001, Abs. *Id.*, 3:13-23. The '048 Patent discloses that a device can assert cleanliness to the network using a trusted code base. *Id.*, 14:22-51.

VI. THE CHALLENGED '048 PATENT

28. The '048 Patent contains 20 claims. I have been asked to opine on the validity of Claims 1-20.

VII. THE '048 PATENT PROSECUTION HISTORY

29. I have reviewed the file history of the '048 Patent.

30. The Examiner allowed all claims on a first action Allowance on October 12, 2016. EX1002, pp.120-124. The Examiner did not provide any reasons for allowance.

31. The '705 Patent (which is in the same family as the '048 Patent and claims similar subject matter) was previously challenged in IPR2021-00593 filed by Cisco that settled and terminated earlier this year. EX1018. The PTAB issued a final written decision and on appeal, the Federal Circuit “vacate[d] the Board’s motivation to combine analysis, which was rooted in legal error and a fact finding unsupported by substantial evidence”, “further vacate[d] the ultimate determination that Cisco failed to show” unpatentability, and remanded to the PTAB. EX1017. K.Mizra opted to settle the IPR rather than resolve validity, thus no final written decision issued on remand and patentability was left unresolved.

32. The Board denied institution in a previous IPR challenge to the '048 Patent. EX1022. The Board’s rationale (insufficient motivation to combine) for denying institution in that IPR was the same as that in the final written decision

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

issued in the prior '705 IPR. EX1016. As noted above, the Federal Circuit vacated the Board's motivation to combine analysis "which was rooted in legal error and a fact finding unsupported by substantial evidence", vacated the ultimate determination that Cisco failed to show unpatentability, and remanded, and the case subsequently settled. EX1017. Validity of the '048 Patent (along with the '705 Patent) therefore remains unsettled. Further, the grounds of this Petition rely on prior art that is different from the prior art cited in the grounds of the previous IPR challenge to the '048 Patent.

VIII. LEVEL OF ORDINARY SKILL IN THE ART

33. A POSITA would have had a bachelor's degree in electrical engineering, computer engineering, or a related discipline, knowledge of networking as of this time, and at least two years of experience working in a field involving networking and system security. A person with a different degree could still qualify if they have additional experience that compensates for the different educational backgrounds.

34. A person with less experience working in a field involving networking and system security could still qualify if the person has additional education that compensates for their lesser experience.

35. I have been informed that the "priority date" or "earliest effective filing date" of a patent is the date on which it is filed, or the date on which an earlier-filed

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

U.S. or international patent application was filed if the patentee claims the benefit of priority to that earlier-filed U.S. or international patent application. For purposes of this declaration, I have assumed that the '048 Patent is entitled to a priority date of September 27, 2004, and I have not evaluated or formed an opinion on whether the claims of the '048 Patent are actually entitled to that date.

IX. CLAIM CONSTRUCTION

36. For purposes of my analysis in this IPR proceeding, I have been informed that terms that appear in the claims of the '048 Patent should be interpreted according to their plain and ordinary meaning under the *Phillips* standard. In determining the ordinary and customary meaning, I have been informed that the words of a claim are first given their plain meaning that those words would have had to a POSITA at the time of the alleged invention. I also have been informed that the claims, specification, and file history may be used to better construe a claim insofar as the plain meaning of the claims cannot be understood. I have been informed that even treatises and dictionaries may be used under limited circumstances to determine the meaning attributed by a POSITA to a claim term at the time of filing.

37. I also understand that, for terms that evoke a means plus function construction, “the construction of the claim must identify the specific portions of the specification that describe the structure, material, or acts corresponding to each claimed function.” 37 C.F.R. §42.104(b)(3). I understand from counsel that

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

construing a means-plus-function claim term is a two-step process that includes (1) identifying the claimed function and (2) then determining what structure, if any, disclosed in the specification corresponds to the claimed function.

38. I have reviewed the '048 Patent and its prosecution history as well as additional documents to construe the claims for performing my validity analysis. It is my understanding that some terms of the '048 Patent are in dispute in a related litigation.

39. I understand that in the Related Litigation, the parties proposed that certain claim terms should be given their plain and ordinary meaning. *See* EX1014, pp. 2-17; EX1015, pp. 1-19.

40. I understand that in the Related Litigation, Google proposes constructions for “protected network”, “trusted computing base”, “trusted platform module”, “valid digitally signed attestation of cleanliness”, “includes at least one of an . . . and an . . .”, “quarantine” or “quarantining”, “quarantine server”, and “remediation host configured to provide data usable to remedy the insecure condition”. EX1014, pp.2-17. These constructions are presented below:

41. I understand that in the Related Litigation, Petitioner proposes “protected network” should be construed as:

private network, distinct from public networks like the Internet

See EX1014, p.2.

42. I understand that in the Related Litigation, Petitioner proposes “trusted computing base” should be construed as:

hardware or software within the first host that provides security to the host

See EX1014, p.4. Patent Owner proposes construing this term as “hardware or software that has been designed to be a part of the mechanism that provides security to a computer system.” See EX1014, p.4; EX1024, p.6.

43. I understand that in the Related Litigation, Petitioner proposes “trusted platform module” should be construed as:

a secure cryptoprocessor that can store cryptographic keys and that implements the Trusted Platform Module specification from the Trusted Computing Group

See EX1014, p.2. See also EX1015, p.1. EX1019, p.1 (WDTX Order). See also EX1024, p.6 (EDTX Order).

44. I understand that in the Related Litigation, Petitioner proposes “valid digitally signed attestation of cleanliness” should be construed to have its plain and ordinary meaning wherein the plain and ordinary meaning is that the “attestation of

cleanliness” is digitally signed by and received from the “trusted computing base”.

See EX1014, p.10; *see also* EX1024, p.7.

45. I understand that in the Related Litigation, Petitioner proposes “quarantine” or “quarantining” should be construed as:

isolating from the protected network

See EX1014, p.13.

46. I understand that in the Related Litigation, Petitioner proposes “quarantine server” should be construed as:

server to which a quarantined host’s network traffic is redirected

See EX1014, p.16.

47. I understand that in the Related Litigation, Petitioner asserts that “remediation host configured to provide data usable to remedy the insecure condition” should be construed as a means-plus-function term and is indefinite for lack of corresponding structure to perform the claimed function of “provide data usable to remedy the insecure condition”. EX1014, p.17. I also understand that Petitioner identifies the following purported corresponding structure disclosed at column 11, lines 61-66 of the ’048 Patent (i.e., “servers providing security patches or advisories, for example allowing connections to a vendor’s server, or providing

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools”).

48. Patent Owner asserted plain and ordinary meaning for the terms discussed in Sections A, D, E, F, G, and H above. *See* EX1015. To the extent any claim terms are construed as means plus function in this IPR or in the Related Litigation, the prior art cited in this Declaration discloses the terms with at least the same level of detail including corresponding structure and claimed functions as described in the '048 Patent. To the extent any more narrow claim constructions are proffered or adopted by the District Court in the Related Litigation, the prior art cited discloses the terms with at least the same level of detail as described in exemplary embodiments of the '048 Patent.

49. I apply the constructions proposed in Related Litigation for purposes of this Expert Declaration.

50. While the proper metes and bounds of the claims are disputed in the Related Litigation, the cited prior art falls within these bounds whatever they may be.

51. The Challenged Claims are unpatentable under all potential constructions.

X. OVERVIEW OF THE PRIOR ART REFERENCES

A. Freund (EX1005) and Freund '611 (EX1020)

52. Freund discloses protecting a computer network by quarantining a non-compliant, vulnerable roaming client (i.e., host) device using a “sandbox server” to perform quarantine functions.

53. Web server requests (e.g., HTTP) and/or DNS requests from a potentially vulnerable host device are redirected to the sandbox server, which provides a quarantine notification page to the vulnerable device and initiates remediation. EX1005, ¶¶[0148]-[150], Figs. 7-9.

54. Freund’s system seeks to protect private networks (e.g., LANs) from viruses or other infections that may be obtained via other networks (e.g., Internet malware). *Id.*, ¶¶[0014]-[0021]. Freund’s system includes a client-side security component/module, and an associated router-side security module to challenge the host device which is connected to or attempting to connect to the local LAN for ensuring compliance with network security policies. *Id.*, ¶¶[0039]-[0041].

55. When Freund’s system detects a non-compliant device (e.g., a potentially infested host device), Freund’s system redirects communication from that device to the sandbox server to quarantine the device and serve a notification page to initiate remediation measures from a remediation host. *Id.*, ¶[0042].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

56. Freund '611, incorporated by reference in Freund (EX1005, ¶[0017]), discloses a “prior ZoneAlarm™ product” related to Freund’s disclosure. *Id.* Freund '611 similarly discloses “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.” EX1020, 1:27-30. Freund '611 discloses “client-based monitoring and filtering of access” (*id.*, 3:61) using filtering implemented, for example, at an Internet Service Provider (ISP). *See id.*, 21:47-22:41; 29:17-30:10.

B. Ball (EX1006)

57. Ball discloses host hardware can be configured with a “Trusted Platform Module” (TPM) conforming to an industry standard “Trusted Computing Group” (TCG) Specification that was well known and conventionally integrated in a vulnerable client-side host device as a client-side security component for providing security via cryptographic operations and securely stored encryption keys that securely convey attestations of the host device’s cleanliness. A “TPM 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.” EX1006, ¶[0006].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

58. Ball's solution verifies the attributes of a client-side host. EX1006, Abs. Attributes are measured using a TPM defined by the TCG Specification (EX1008) and integrated on the computing device. EX1006, ¶[0006].

59. The TPM can securely and accurately measure and communicate attributes about the computing device and digitally sign ("encrypt") the attributes using an attestation identity key (AIK). EX1006, ¶[0033].

60. AIKs encrypt device information and authenticate device information when it is transmitted to another device (e.g., in response to a security challenge). EX1006, ¶[0033]. AIKs ensure the device's identity can be trusted and the information attested to by the TPM is accurate. *Id.* Ball's TPM hardware ensures attestation accuracy. EX1006, ¶¶[0030], [0033].

C. Kappes (EX1007)

61. Kappes protects a network by authenticating client devices requesting access to the network. EX1007, Abs., ¶[0059].

62. Potentially vulnerable host devices are quarantined and permitted limited access to restoration services. EX1007, ¶¶[0036]-[0038], [0052], Fig. 3.

63. The restoration services use "standard packet filtering techniques" to filter web server requests and DNS requests. EX1007, ¶¶[0029], [0038].

D. Pujare (EX1009)

64. Pujare discloses a “versioning table” that makes clear that application patches are merely software upgrades. EX1009, ¶¶[0019]. Pujare’s versioning table contains a list of root file numbers and version numbers. EX1009. The root file numbers and version numbers are used to track the application patches and upgrades. *Id.* Pujare’s disclosure demonstrates that it was well known and conventional for software version numbers to correspond to patch levels. *Id.* A client receives the versioning table and compares it with the client’s application root file number/version number to find files required for a software patch or update. *Id.*

E. Lewis (EX1013)

65. Lewis discloses an alternate method of DNS redirection of insecure client devices to the IP address of a quarantine server. *See* EX1013, 12:11-18, 14:4-24; Fig. 8B.

66. A DNS destination address of a non-compliant host device is rerouted to a “hi-jack” DNS server that is configured to provide only the IP address of a quarantine server. EX1013, 14:20-24, 11:15-17, 14:4-24. This causes non-compliant devices to be routed to a fix-up page of the quarantine server. *Id.*

67. The earlier publication of Lewis (U.S. Patent Application Publication No. 2005/0131997) was cited and considered in an Information Disclosure Statement during examination. EX1002, p.125.

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

68. Petitioner merely relies on Lewis as an alternative technique to the technique disclosed by Freund for providing an IP address of a quarantine server in response to a DNS query by a non-compliant host device. Freund (EX1005) discloses and/or suggests providing an IP address of a quarantine server in response to a DNS query. As detailed in this Declaration, Freund discloses '048's purported novel features. Further, Lewis discloses an exemplary embodiment called out in the '048 Patent.

F. Kouznetsov (EX1021)

69. Kouznetsov discusses software application management and discloses that maintenance of software applications (such as anti-virus software) includes implementation of incremental improvements, such as patches, updates, and versions. *See* EX1021, 1:39-3:33.

**XI. DETAILED EXPLANATION OF THE UNPATENTABILITY
GROUNDS**

70. In my opinion, the Challenged Claims are unpatentable over the prior art.

A. Claims 1-20 Are Obvious Over Freund (EX1005) in view of Ball (EX1006), and Pujare (EX1009) (Ground 1)

71. The following sections detail how Claims 1-20 are obvious over the prior art.

1. Claim 1 (Preamble): “A method, comprising:”

72. To the extent the Preamble is limiting, Freund discloses and suggests the Preamble of claim 1.

73. Freund discloses a method for protecting a network (e.g., a local area network (LAN)) from malicious code by denying connections to the network. EX1005, ¶¶[0004], [0068].

74. Freund aims to “protect the overall security of the network.” *Id.*, ¶[0019]. *See also id.*, ¶[0066]. Figure 3 of Freund is compared to Fig. 10B of the ’048 Patent below:

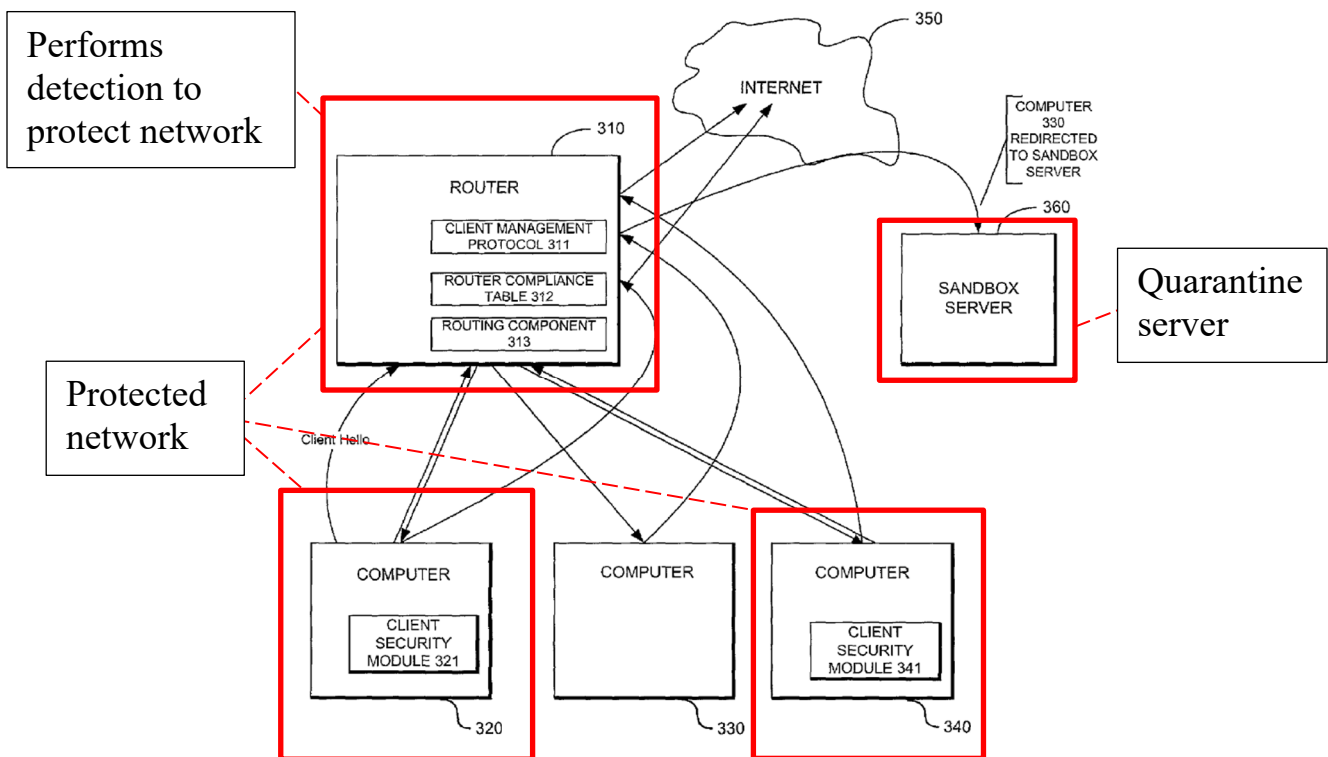


Figure 3 of Freund (Annotated)

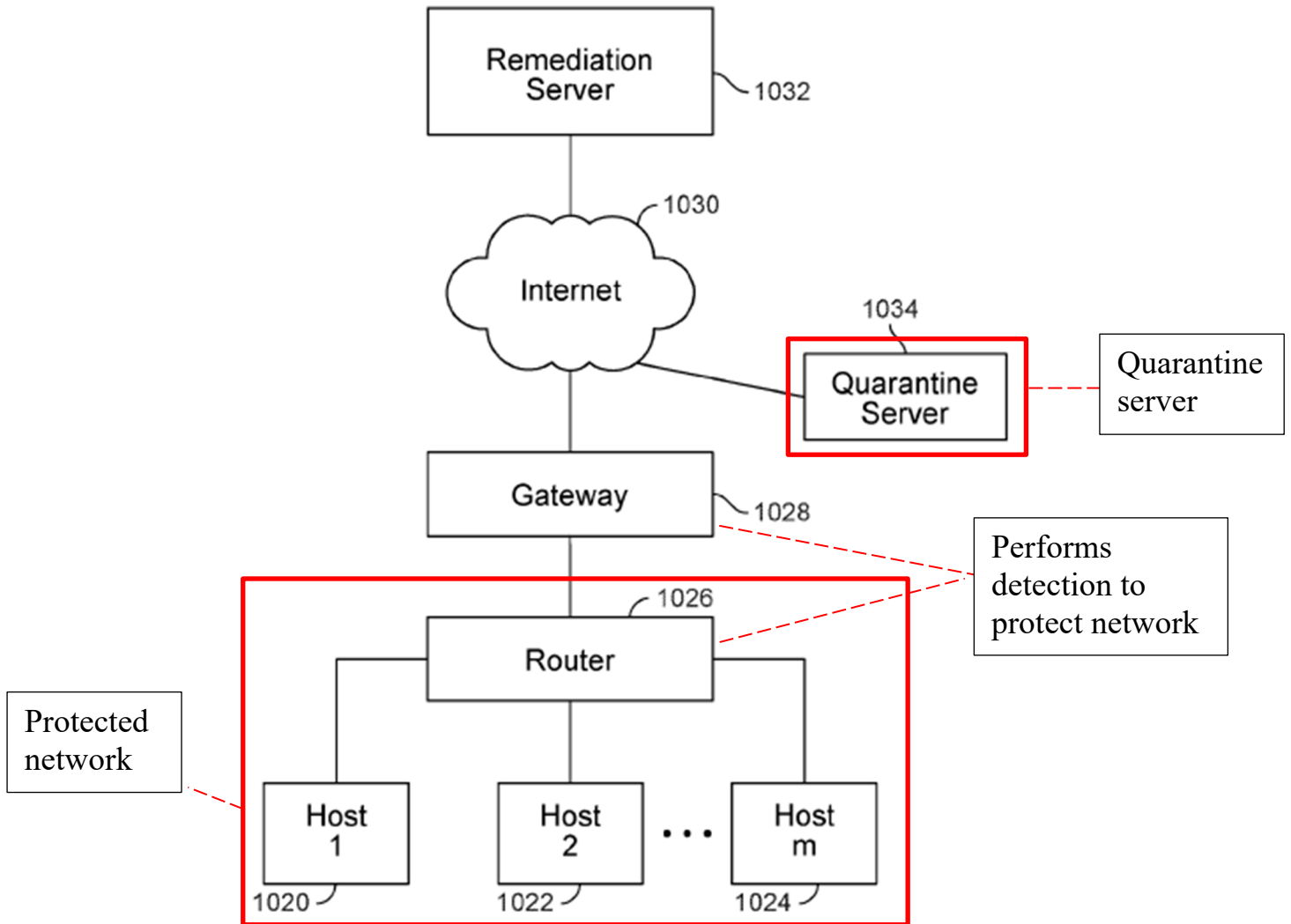


Figure 10B of '048 Patent (Annotated)

a. [1.1]: “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,”

75. Freund discloses and suggests Element [1.1].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

76. Freund discloses detecting an insecure condition on a vulnerable first host (i.e., client-side host) that has connected or is attempting to connect to a protected network.

77. A comparison of the above annotated Freund Figure with the annotated '048 Patent Figure 10B demonstrates that the hosts of both connect to a router device to access the network. All communication on the network passes through the router device, including communication to other hosts.

78. Freund's Figure 7 shows a notification page served by a quarantine server after an insecure condition was detected. EX1005, Fig. 7.

79. Freund discloses detecting a non-compliant device (e.g., running an older, outdated version of security software or having a virus) that has connected or is attempting to connect to a protected network (e.g., a LAN). EX1005, ¶¶[0071], [0078], [0088].

80. Freund's client monitoring protocol (CMP) evaluates responses from a host device to determine if the device is compliant or non-compliant. EX1005, ¶¶[0084]-[0085], [0088]-[0089]. If Freund's CMP determines the device properly responded, then it is determined compliant. If a device did not properly respond, or did not respond at all, Freund's CMP determines the device has an insecure condition (e.g., insufficient anti-virus version, security module disabled, presence of virus, etc.). *Id.*, ¶[0088].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

81. Freund's disclosure refers specifically to a protected network as a "private network" which can connect to the Internet. EX1005, ¶[0028]. The protected network can be a Local Area Network (LAN) on a client's premises which can connect to "larger open networks (Wide Area Networks or WANs), including the Internet. *Id.*, ¶[0004]; [0069]-[0070].

b. [1.2]: "wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,"

82. Freund in view of Ball discloses and suggests Element [1.2].

83. Freund detects the insecure condition by contacting a trusted computing base (TCB) configured as Freund's "client monitoring protocol software" (CMP) and/or "client-side security component/module" associated with a TPM within the first host.

84. Freund's CMP contacts a client-side security module (i.e., the TCB) within the host device. EX1005, ¶¶[0084]-[0089].

85. Freund's CMP contacts the client-side security module of the host device by sending a router challenge. *Id.*, ¶[0084]. The client-side security module receives the router challenge and responds to the router challenge. *Id.*, ¶[0093]. *See also id.*, ¶¶[0077]-[0078], [0100].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

86. The CMP can challenge the client-side security module to determine a version level of security software and/or to verify appropriate anti-virus software is running on the device. *Id.*, ¶¶[0127]-[0132].

87. Freund's router-side CMP and client-side security module perform various security functions by handling router challenges and responding to security requirements issued by the router challenge (e.g., providing application status, anti-virus software version installation and status, and so forth). EX1005, ¶¶[0091]-[0093], [0118]-[0144]. Freund's router-side CMP and/or client-side security module are part of the mechanism providing security to Freund's hosts and network. Freund's router-side CMP and/or client-side security module satisfy the claimed TCB under Petitioner's and PO's constructions. *See* EX1014, p.4; EX1015, p.4; EX1024, p.6.

88. Freund discloses attestations involving digital signatures to avoid being forged, and stores a private key to generate the digital signature. *See* EX1005, ¶[0127].

89. Freund discloses CPUs or processors including "any other suitable microprocessor or microcomputer" where program logic (e.g., for the client-side security module) is executed. EX1005, ¶¶[0057]-[0058].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

90. Freund uses such CPUs or processors “within the first host”, i.e., they reside within the client computer. *Id.*, ¶¶[0043], [0065]. *See also id.*, ¶¶[0053]-[0061].

91. Freund’s disclosure of the client-side security module constitutes a TCB given that the client-side security module is hardware and/or software within the first host that provides security to the host.

92. Freund’s client-side security module for interfacing with a router-side security module to access a network is not expressly disclosed to be a “Trusted Platform Module (TPM)” conforming to the TCG as called out in the ‘048 Patent.

93. While Freund discloses a CPU/processor as hardware for executing the TCB, Freund does not expressly disclose that this CPU/processor hardware is a TCB associated with specialized “TPM” hardware. EX1005, ¶[0056].

94. A POSITA would have recognized that a hardware-based TPM conforming to the TCG specification would have been an obvious, well-known hardware choice for implementing Freund’s TCB security functions.

95. A POSITA would have recognized that such a substitution of known TPM hardware to implement enhanced functionality of Freund’s TCB would have achieved predictable results with a reasonable expectation of success. *See, e.g.*, EX1006. *See also* EX1007. This is true for several reasons discussed herein.

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

96. Ball expressly discloses a TPM according to the TCG Specification to be a well-known, conventional CPU/processor for executing the client-side security module and security-based functions disclosed by Freund.

97. Ball states that a “TPM 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.” EX1006, ¶[0006]. Ball’s TPM and associated hardware satisfy the claimed TCB under Petitioner’s and PO’s constructions.

98. It therefore would have been obvious, predictable and beneficial to configure Freund’s TCB as a trusted platform module (TPM) based on Ball’s teachings that a TPM conforming to a TCG specification was a well-known, desirable hardware option for securely implementing client-side security functions according to industry standards. This would have allowed Freund’s client-side host to verify its trustworthiness by securely communicating accurate information regarding anti-virus versions, anti-virus status, security compliance, and digitally signed applications using cryptographic data keys to generate digital signatures and encryption/decryption. *Id.* EX1005, ¶¶[0071], [0110], [0127].

99. It would have been obvious to a POSITA to use Ball’s TPM hardware to house and implement the client-side security module of Freund for securely

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

storing cryptographic keys, hash functions, and identity information. *See* EX1006, ¶[0006]; EX1005, ¶¶[0091]-[0093], [0110], [0127], [0144].

100. A POSITA would have had reason to substitute at least one of the processors disclosed in Freund to execute security functions of the client-side security module using Ball's disclosed TPM (e.g., either integrated or dedicated). Ball's TPM would have provided enhanced hardware-based security for Freund's client-side security module and associated router CMP challenge functions (*see* EX1006, ¶¶[0006], [0033]-[0034], [0046]), and provided enhanced trust in the security configuration of Freund's client-side device. *See, e.g.*, EX1007, ¶[0149]; EX1006, ¶¶[0006], [0033]-[0034].

101. A TPM would have provided enhanced hardware-based security features such as hardware root of trust. EX1005, ¶[0110].

102. Ball and Freund disclose similar goals of enhanced trust and security and similar mechanisms of a challenge/response protocol to determine the trustworthiness of a device. EX1005, ¶¶[0071], [0089]-[0089], [0110], [0122]-[0127]; EX1006, ¶¶[0004], [0031]-[0032].

103. A POSITA would have recognized that Ball's TPM would have been an appropriate hardware solution for implementing the security measures disclosed by Freund in a manner consistent with Freund's hardware/software configuration. *See* EX1006, ¶¶[0006], [0031].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

104. Ball, like Freund, discloses verifying attributes of a device, including security status of a device using a request/response protocol to determine whether a device can be trusted. EX1006, ¶¶[0002], [0030]-[0033].

105. Substituting Ball's TPM to provide the hardware support for Freund's security functions would have been entirely consistent with their shared goal of network security.

106. Employing a TPM in Freund's system would therefore have been obvious, predictable and beneficial for at least four reasons.

107. First, such a combination would have involved the simple substitution of Ball's known TPM implementing the TCG Specification for one of the processors disclosed in Freund to execute the client-side security module.

108. Second, such a combination would have constituted the obvious combination of prior art elements (the TPM according to the TCG Specification taught by Ball) to known methods (Freund's techniques) to yield predictable results.

109. Third, such a combination would have involved using a known security component (a TPM according to the TCG Specification as taught by Ball) as the hardware to improve the implementation of Freund's security functions thereby yielding beneficial results.

110. Fourth, it would have been obvious to try the TPM from among the finite number of identified, predictable hardware solutions for executing software

security modules of the type disclosed by Freund with a reasonable expectation of predictable success.

111. The combination of Freund and Ball disclose a TPM under any construction. *See* EX1014, p.2; EX1015, p.1. *See also* EX1006, ¶[0006]; EX1008 in its entirety.

c. [1.3]: “receiving a response, and”

112. Freund discloses and suggests Element [1.3].

113. Freund’s router-based CMP interrogates the host device and receives a response from the host device’s TCB. *See* Element [1.2], *supra*.

114. The CMP includes a router compliance table to determine whether the device is compliant. EX1005, ¶¶[0077]-[0078], [0084], [0086].

d. [1.4]: “determining whether the response includes a valid digitally signed attestation of cleanliness,”

115. Freund in view of Ball discloses and suggests Element [1.4].

116. As discussed, Freund discloses a CMP. EX1005, ¶¶[0121]-[0122]. *See* Elements [1.2], [1.3], *supra*.

117. Freund discloses determining whether the response includes a valid digitally signed attestation of cleanliness. Freund’s CMP interprets the response from the device to determine whether the response is valid. *Id.*, ¶[0144].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

118. The table in [0144] shows “client application incorrect or old”, “AVold version”, and “AV Real-Time Monitor not running on client.” *Id.*

119. Freund also discloses that applications (e.g., anti-virus software and versions) can be verified via digitally signed attestations using a cryptographic hash function, to attest that the application has not been tampered with. *Id.*, ¶[0110].

120. The digital signature would have been obvious to include in any attestation, as part of the CMP function discussed for example at [0121], [0122].

121. To the extent the digitally signed attestation is required to be performed by the TCB of a “TPM”, Freund and Ball in combination disclose Element [1.4].

122. Ball discloses the TPM transmitting a digitally signed attestation of cleanliness in the response. Freund’s system, with its security features, would have suggested to a POSITA to implement its TCB on a TPM as disclosed by Ball. *See* Element [1.2], *supra*.

123. Ball discloses that “[t]o ensure that the quoted value is not corrupted during communication” the TPM “can generate an attestation identity key (AIK) that is used to encrypt some or all of the quoted value.” EX1006, ¶[0033].

124. The TCG Specification, incorporated by reference in Ball (*id.*, ¶[0006]), confirms that “[a]ttestation by the TPM is an operation that provides proof of data known to the TPM. This is done by **digitally signing** specific internal TPM data using an attestation identity key (AIK).” EX1008, p.6 (emphasis added).

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

125. Freund's system would have implemented the TPM with its client-side security module (i.e., the TCB and/or part of the TCB) to provide digitally signed attestations from the TCB associated with the TPM in the response to the CMP that a device is not infested, is security compliant, or is running anti-virus software that is sufficiently updated.

126. Freund and Ball in combination disclose determining whether the response includes a valid digitally signed attestation of cleanliness.

127. Freund and Ball disclose a valid digitally signed attestation of cleanliness, signed by and received from a TCB of a TPM.

128. Freund and Ball disclose a valid digitally signed attestation of cleanliness under any construction. *See* EX1014, p.2; EX1015, p.6. *See also* EX1024, pp. 7-11..

- e. [1.5]: **“wherein the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;”**

129. The cited art discloses and suggests Element [1.5].

130. Freund discloses that the valid digitally signed attestation of cleanliness indicates that the first host is not infested (e.g., a router CMP challenge verifies that

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

the first host is running an anti-virus program, *see*, e.g., EX1005, ¶¶[0110]-[0117], [0132]-[0133], and receives an attestation of the presence of an anti-virus version update – i.e., patch or a patch level associated with a software component of the first host (*see*, e.g., EX1005, ¶¶[0078], [0085]).

131. Freund discloses an “‘anti-virus challenge’ option” in which “the router-side security module looks for the appropriate code to verify if the anti-virus program is running on the client machine and if both the anti-virus program and the associated data file are up to date.” EX1005, ¶¶ [0132]-[0133]. *See also id.*, ¶ [0117] (“Anti-virus Real-Time monitoring not enabled. Informs user to activate Real-Time monitoring.”).

132. Freund’s valid digitally signed attestation of cleanliness (e.g., a hashed, signed application preventing substitution of applications) ensures that client-side applications (including anti-virus applications) cannot be tampered with, thereby creating a level of trust in a client’s response to the router’s CMP anti-virus challenge. EX1005, ¶[0110].

133. Freund’s valid digitally signed attestation of cleanliness attests that the first host is not infested by attesting that the anti-virus software is running and/or that anti-virus real-time monitoring is enabled. EX1005, ¶¶[0110]-[0117].

134. Moreover, “performing a virus scan” was a well-known and conventional technique used in security and authentication processes, and it would

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

have been obvious to perform such a virus scan and attest to same given that the purpose of such virus scan is to “ensure or restore the integrity of the content of the device”. EX1007, ¶¶[0052]-[0054], ¶[0047].

135. The '048 Patent discloses that a first host that is “not infested” (i.e., cleanliness) includes “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, 14:37-44.

136. The '048 Patent discloses that “infestations”, “contagion”, and “viruses” are related concepts and anti-contagion software encompasses anti-virus software. EX1001, 11:40-42 (“Infestation herein refers to the current presence and/or execution of contagion”), 3:44-45 (“Examples of contagion include computer worms, viruses”), 3:45-49 (“Anti-contagion software refers herein to software that prevents, impedes, or remediates contagion, such as Norton Antivirus from Symantec, or VirusScan from McAfee, which identifies and/or removes contagion from a user’s computer”). Thus, Freund’s device transmits a digitally signed attestation of cleanliness by asserting whether the anti-virus software is currently running and/or performing real-time monitoring of the client device to Freund’s CMP. EX1005, ¶¶[0110], [0144].

137. Freund also discloses that the attestation validates the presence of an anti-virus version update level as a patch or a patch level associated with a software

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

component on the first host. Freund's attestation of cleanliness confirms that anti-virus software is updated with any recent updates represented by patch or patch level updates to the anti-virus software. EX1005, ¶¶[0078], [0085].

138. Freund discloses that "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". EX1005, ¶[0078] (emphasis added).

139. Freund's Figure 4 shows a patch or patch level for the TRENDMICRO anti-virus software PC-Cillin and ZAP with a "version" that Freund's router inspects and enforces via the digitally signed attestation of cleanliness. EX1005, Fig. 4, ¶¶[0098]-[0099], [0132].

140. If the correct update (i.e., patch) level for these software components is not confirmed, Freund's router will quarantine the client device and redirect its communications to the sandbox server to remediate and update the anti-virus software. EX1005, ¶¶[0114]-[0117]. *See also* EX1021, 2:34-37. *See also id.*, 2:49-52 ("many applications provide downloadable access to updates and patches"). The '048 Patent describes patches in a similar manner. *See* EX1001, 14:52-15:38 ("a security patch update provider").

141. Freund discloses that "a computer running an *older version* of the security software may respond in the negative to a router challenge requesting

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

confirmation that the computer is running a *current* version of the software”. EX1005, ¶[0078] (emphasis added). *See also* EX1009, ¶[0019] (“A versioning table contains a list of root file numbers and version numbers. This information is used to track application patches and upgrades. Each entry in the versioning table corresponds to one patch level...”).

142. Freund discloses both (1) an attestation that the TCB has ascertained that the first host is not infested, and (2) an attestation that the TCB has ascertained the presence of software updates via a patch or a patch level associated with a software component on the first host. Freund therefore discloses limitation [1.5] under any construction. *See* EX1014.

- f. [1.6]: “when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,”

143. Freund discloses and suggests Element [1.6].

144. Freund discloses detecting an insecure condition such as outdated anti-virus software (*see* Element [1.2], *supra*) on a host by using a router-based CMP challenge/response protocol. EX1005, ¶[0041].

145. Non-compliant devices in Freund are redirected to the “sandbox” quarantine server. Freund’s “security module only allows the non-compliant

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

computer to access the sandbox server to perform a defined set of tasks to address the non-compliance.” *Id.*

146. Freund prevents the quarantined device from sending any data to any devices (including one or more other hosts associated with Freund’s network) other than the sandbox server or to a server providing updates to the out-of-date anti-virus software. *Id.*, ¶¶[0042], [0071].

147. Freund’s quarantining includes isolating a vulnerable host device from a protected network. Freund discloses quarantining a device under any construction. *See* EX1014, p.2.

g. [1.7]: “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,”

148. Freund discloses and suggests Element [1.7].

149. Freund discloses receiving a service request from a host device, and preventing the device from sending data to one or more other hosts.

150. Freund discloses using service requests to request services from a network. EX1005, ¶¶[0042], [0147].

151. Freund’s “router receives a request for connection”. *Id.*

152. Freund discloses its “sandbox server to which non-compliant computers are re-directed when they attempt to connect”. *Id.*, ¶[0081].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

153. If a device is non-compliant, Freund “operates to redirect the local computer to the sandbox server instead of the address originally requested.” *Id.*, ¶[0089].

154. Freund prevents the device from sending data to one or more other hosts associated with the protected network upon receiving and redirecting the service request to the sandbox server.

155. Freund also discloses preventing the non-compliant device from sending data on the network.

156. Freund discloses a network connection being “denied in the event that the destination address is determined at step 960 not to be the DNS or DHCP server.” EX1005, ¶[0151].

157. Freund also denies a network connection where the service request is redirected to the sandbox server. *See id.*, Fig. 9, step 970.

h. [1.8]: “determining whether the service request sent by the first host is associated with a remediation request, and”

158. Freund discloses and suggests Element [1.8].

159. Freund discloses determining whether the service request sent by the first host is associated with a remediation request. EX1005, ¶[0042], [0078].

160. Freund’s Figure 9 decision block 920 determines whether a destination address for a service request is “exempt” per the process of rerouting service requests

to the sandbox server (i.e., quarantine server). *See* Element [1.10], *infra*. *See* EX1005, Fig. 9.

161. Figure 9 illustrates how a service request is permitted to pass to a remediation host providing updates and/or patches for TRENDMICRO's PC-Cillin shown in Figures 7, 8. *See* EX1005, ¶¶[0114]-[0117], [0132].

162. Decision block 920 determines whether a service request for a destination host should be permitted (e.g., exempt) or redirected (e.g., not exempt). EX1005, ¶¶[0042], [0071], [0078], Fig. 9.

163. A remediation request accessing a download page of Freund's Figures 7, 8 is transmitted via the router upon determining the destination address (e.g., remediation host) is exempt from being redirected. EX1005, Figs. 7-9.

164. A POSITA would have understood that decision block 920 is a branching point to determine whether a destination address is exempt. *Id.*

165. A POSITA would have understood that Freund filters service requests (e.g., destination addresses) to permit remediation. EX1005, ¶[0110] ("For example, rules can also be established on the basis of including and/or excluding access to particular Internet sites.").

166. Freund allows a non-compliant device to access an anti-virus software update, such as via another server and/or host on the Internet (e.g., as downloadable

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

software). *See, e.g., id.*, Fig. 7. All other communications from a non-compliant device are redirected to the quarantine sandbox server. *Id.*, ¶¶[0148]-[0150].

167. Freund’s system “enables the user to take the steps necessary to bring his or her computer back into compliance” (*id.*, ¶[0095]) with a service request prompt (e.g., “Update Now” and “Download Now” in Figures 7, 8) for accessing virus protection software updates or new versions; i.e., the service request is “associated with a remediation request”. *See id.*, Figure 7, ¶[0114] (“The message displayed in panel 702 . . . informs the user that he or she needs to update the virus protection software installed on the computer.”); Figure 8 (“Download Now!” prompt for remediation), ¶[0116] (“error message panel 802 . . . indicating that a new version of the security software available”). *See also* EX1012, pp.26-94.

168. The ’048 Patent works in precisely the same way. *See, e.g.,* EX1001, 16:29-37 (“An example of a quarantine notification page is a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain.”).

169. Freund’s “Update Now” and “Download Now” prompts permit access for the purpose of addressing non-compliance.

170. Following the prompt, Freund’s client will generate a new outbound communication service request which Freund’s router and CMP monitor as a request

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

for remediation (e.g., to download and/or update anti-virus software). *See* EX1005, Fig. 7 and 8, ¶¶[0042], [0071], [0114]-[0116].

171. The '048 Patent's process is the same as Freund's process. *See* EX1001, Fig. 14, 15:8-38.

172. The '048 Patent tests outbound traffic to determine whether the traffic is associated with remediation such as "contact with a verified remediation site". *Id.*, 15:16. If the traffic is associated with a remediation request, then the traffic is forwarded to the destination. *Id.*, 15:17-20. Otherwise, the traffic is rerouted to the quarantine server. *Id.*, 15:20-31. Freund determines whether a service request is associated with a remediation request to the same extent as the '048 Patent.

173. Determining whether Freund's service request or prompt is associated with a remediation request is accomplished in various ways (e.g., via request filtering or other policy rules). *Id.*, ¶[0110].

174. Freund's "Update Now" and "Download Now" prompts are service requests that Freund's system determines are associated with remediation requests because they allow for anti-virus updates of a quarantined client, *i.e.*, the first host.

- i. **[1.9]: “when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request,”**

175. Freund discloses and suggests Element [1.9].

176. Freund discloses receiving a service request in a quarantine-capable network. *See* Elements [1.7] and [1.8], *supra*.

177. Freund discloses that a service request is redirected to the sandbox server so the sandbox server can transmit a quarantine notification page to the device when the service request is a web server request. *See* EX1005, Fig. 7, Fig. 8, ¶¶[0049]-[0050], [0114]-[0117], [0148]-[0151].

178. When Freund determines that a service request is not addressed to a remediation host destination, Freund’s router assesses the service request to replace the IP address with an address for the sandbox server (i.e., quarantine server). EX1005, ¶¶[0147]-[0150].

179. Freund’s Figure 9 discloses that a service request from a client device is evaluated to determine whether: (a) the HTTP destination address is an exempt request (e.g., remediation), (b) the source is permitted to connect to a network (e.g., whether the source is exempt per (a) or must be evaluated by the router’s CMP), (c) the destination is a DNS server so that an IP address will be returned from the DNS

server, or (d) if the request is an HTTP request (i.e., web server request), in which case the original IP address is replaced with an IP address for the sandbox server (i.e., quarantine server) if the original HTTP destination address is not exempt per (a). EX1005, ¶¶[0147]-[0151], Fig. 9. See Element [1.8], *supra*. See also EX1012, pp.10-27.

180. In all cases for a non-compliant device, once the service request is authorized by the router, Freund replaces the client's source IP address through the NAT table (e.g., as a client alias to protect the private network); the service request is then passed to the destination address of either the sandbox server (i.e., quarantine server) or the remediation host. EX1005, ¶¶[0145]-[0151]. See also EX1012, pp.10-27.

181. A service request is rerouted to the sandbox server which serves a notification page to the client device. EX1005, ¶[0149].

182. Freund “*denies any other access* to the Internet by the non-compliant computer” that is not associated with the remediation request. EX1005, ¶[0071] (emphasis added). When the non-compliant computer submits a service request that is not for the purpose of addressing the non-compliance (i.e., is not associated with the remediation request), that service request is *denied*. *Id.* Freund's system therefore determines whether the non-compliant computer's service request is associated with a remediation request or is not associated with a service request given that Freund's

system expressly distinguishes between remediation-associated requests (which are permitted access) and all other requests (which are denied access). *Id.*

183. It would have been obvious for Freund's system to make such a determination (e.g., as shown in decision block 920 in Figure 9) for precisely the same reason—to allow Freund's system to distinguish between permitted and non-permitted service requests received from the non-compliant computer. *See also id.*, [0141]-[0151], Fig. 9.

184. Freund serves a quarantine notification page in response to a service request when the device is quarantined and/or deemed non-compliant. *Id.*, ¶[0149]. Freund discloses serving “an error message window 700 that is displayed to a non-compliant client computer that is redirected to the sandbox server.” *Id.*, ¶[0114]. Freund's quarantine notification page “informs the user that he or she needs to update the virus protection software installed on the computer.” *Id.*, ¶[0114].

185. Freund's quarantine notification page is served to the device when the service request comprises a web server request (e.g., an HTTP request). Freund's routing component monitors the service request and “determines whether or not the destination port is HTTP (port 80 TCP). If the destination port is HTTP, then the re-routing manager proceeds in step 951 to manipulate the destination IP address and port.” EX1005, ¶[0148].

186. A POSITA would have understood that a service request having a destination port of HTTP would include a web server request because it is well known that HTTP is a standard protocol for web server requests. Freund discloses serving a quarantine notification page to the device when the service request comprises a web server request.

187. When Freund determines the service request is a web server request, Freund responds by replacing the destination Internet Protocol (“IP”) address with the IP address of the sandbox server which then serves the quarantine notification page to the device. EX1005, ¶[0149]. “Using this information, the sandbox server then displays a page with information enabling the client to address the specific problem that was detected.” *Id.* “In this manner, the connection request from a non-compliant client computer is patched and manipulated to reroute this packet to the sandbox server.” *Id.* Freund discloses serving a quarantine notification page to the device when the service request comprises a web server request.

j. [1.10]: “wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and”

188. Freund discloses and suggests Element [1.10].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

189. Freund discloses that other requests (e.g., HTTP requests to other services that are not remediation) are rerouted to the sandbox server for a non-compliant device. *See* EX1005, ¶¶[0042], [0078], [0147]-[0150].

190. Freund's routing component monitors the service request and "determines whether or not the destination port is HTTP (port 80 TCP). If the destination port is HTTP, then the re-routing manager proceeds in step 951 to manipulate the destination IP address and port." EX1005, ¶[0148]. Requests to connect to other services are "redirected to the sandbox server." *Id.*, ¶¶[0040], [0042], [0071].

191. Freund discloses that serving the quarantine notification page includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page. EX1005, ¶¶[0042], [0078], [0147]-[0150]. *See* Element [1.8], *supra*.

192. Freund causes a browser on the first host to be directed to the sandbox server when it replaces the IP address provided by the browser with the IP address of the sandbox server. Freund's quarantine notification page then provides quarantine information and remediation information such as is shown in Freund's Figures 7 and 8. *Id. See id.*, Figs. 7, 8. *See* Element [1.8], *supra*.

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

193. Lewis discloses an alternative means of re-routing service requests sent by hosts with a redirect that causes a browser on the hosts to be directed to a quarantine server configured to serve the quarantine notification page. Lewis discloses “a hijack DNS component 421 for intercepting DNS queries from quarantined clients.” EX1013, 11:15-17.

194. When Lewis’ client, via a DNS query, “performs name resolution on any address, it will receive the IP of QS. This way any client will be redirected to fix-up page on QS [*quarantine server*].” EX1013, 14:22-24. Lewis discloses a specific embodiment described in the ’048 Patent for redirecting a browser on a host to a quarantine server. *See* EX1001, 15:27-38.

k. [1.11]: “permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.”

195. Freund in view of Ball discloses and suggests Element [1.11].

196. Freund discloses permitting the device to communicate with a remediation host when the device is quarantined.

197. Freund discloses that a non-compliant device redirected to the sandbox server is only permitted “to perform a defined set of tasks to address the non-compliance. All other Internet access by the non-compliant computer is disabled.” EX1005, ¶[0042], Fig. 9, ¶¶[0148]-[0151].

198. Freund discloses that the non-compliant computer's "access to the Internet is restricted to those activities necessary to get the computer back into compliance. This is accomplished by redirecting the attempted connection by a non-compliant computer to a designated 'sandbox' server that can facilitate appropriate corrective action, including the download of appropriate software to correct the non-compliance." EX1005, ¶[0071].

199. Freund allows a non-compliant computer to download appropriate corrective software from a remediation host through the sandbox server itself acting as a remediation host. *See* EX1005, ¶¶[0019]-[0020], [0078], [0095]. Figures 7-9 of Freund also show and describe the notification page providing update and download links to remediation hosts to retrieve data to remedy the non-compliant devices. *See id.*, Figs. 7-9; ¶¶[0114]-[0115].

2. **Claim 2: "A method as recited in claim 1, wherein detecting the insecure condition further includes at least one of the group consisting of scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic."**

200. Freund in view of Ball discloses and suggests claim 2.

201. Freund discloses detecting an insecure condition at least by "scanning for a vulnerability", "determining whether a security software is installed", and "detecting anomalous network traffic" as claimed. Freund discloses a component

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

that “checks to ensure that appropriate end point security software is in place on all of the computers on the LAN.” EX1005, ¶[0071].

202. Freund discloses verifying “that the computer has installed and is running appropriate security software, and is in compliance with other established security policies.” *Id.*

203. A POSITA would have understood that a device that is not in compliance with security policies exhibits a vulnerability.

204. Thus, Freund discloses and suggests scanning (e.g., checking) for a vulnerability by determining whether a device is running appropriate security software and complies with established security policies. Freund also discloses determining whether security software is installed by determining that the device has installed and is running appropriate security software. EX1005, ¶¶[0019], [0071].

205. A POSITA would have understood that an outdated application (e.g., including an OS) and/or security software would be a vulnerability. EX1005, ¶[0110].

206. Freund also discloses that “detecting an insecure condition” includes “scanning for malicious data”. Freund discloses an “anti-virus challenge” that “allows the administrator to use the router for anti-virus enforcement and distribution. The router-side security module looks for the appropriate code *to verify if the anti-virus program is running* on the client machine and if both the anti-virus

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

program and the associated data file are up to date.” EX1005, ¶[0132] (emphasis added). *See also id.*, ¶[0068] (implementing security policies that serve to avoid or reduce the impact of “attacks from malicious code”).

207. Indeed, it was well known to “perform[] a virus scan” to detect whether an insecure condition exists, and it would have been obvious to perform such a virus scan for this purpose. EX1007, ¶[0047], ¶¶[0052]-[0054].

208. Freund also discloses “detecting anomalous network traffic” as claimed at least because Freund discloses checking network requests for compliance by evaluating responses in a router compliance table and determining whether network traffic includes HTTP requests and/or DNS requests. EX1005, ¶¶[0147]-[0150].

209. By determining a network request and therefore a device is non-compliant with the router compliance table, Freund discloses and suggests “detecting anomalous network traffic” as claimed.

210. Freund contemplates using “one or more of the security policy requirements indicated in the router challenge” and thus teaches use of any combination of the security policy requirements described above. EX1005, ¶[0078]. *See also id.*, ¶[0093] (“any optional security requirements”).

3. Claim 3: “A method as recited in claim 1, wherein detecting the insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.”

211. Freund in view of Ball discloses and suggests claim 3.

212. Freund discloses detecting an insecure condition including determining that the first host should be quarantined until an update to an operating system has been installed. Freund discloses that a device is quarantined until software on the device has been sufficiently updated to correct non-compliance. EX1005, ¶¶[0071], ¶¶[0117]-[0118].

213. Freund recognizes network security vulnerabilities associated with devices running “older software”. EX1005, ¶¶[0088]-[0089].

214. It was well-known and conventional to verify the version of an operating system for security and attestation purposes. *See, e.g.*, EX1006, ¶[0031] (“verifies” the “type and/or version” of an “operating system” for purposes of “attestation”).

215. Given the above, a POSITA would have understood that Freund’s teachings concerning the insecure condition associated with out-of-date software is not limited to anti-virus software but also applies to out-of-date operating systems—indeed, Freund specifically warns against operating system “security holes”. EX1005, ¶¶[0015], [0019].

- 4. Claim 4: “A method as recited in claim 1, wherein permitting the first host to communicate with the remediation host includes: detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to the remediation host.”**

216. Freund in view of Ball discloses and suggests claim 4.

217. Freund discloses receiving a service request from a device. *See* Element [1.7], *supra*.

218. Freund discloses detecting an outbound communication from the device (i.e., as a service request). *See* Element [1.7], *supra*.

219. Freund discloses forwarding the outbound communication if it is addressed to the remediation host to permit the device to communicate with the remediation host at least because Freund discloses that a device’s activities are restricted to activities necessary to get the device back into compliance with security policies when the device is redirected to the sandbox server. EX1005, ¶[0071].

220. Figure 9 of Freund discloses a process for forwarding an exempt address referenced in block 920 via block 980 (e.g., the exempt address of a remediation host such as the PC-Cillan anti-virus software referenced in Freund’s Fig. 4, available from TRENDMICRO referenced in EX1005, ¶[0132]. *See*, EX1005, ¶[0147]-[0151]; [0104]-[0105].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

221. Freund redirects communication to the sandbox server or permits communication if it is addressed to remediation “to address the specific problem that was detected.” EX1005, ¶[0149]. *See id.*, ¶¶[0071], [0149], Fig. 9.

222. Freund discloses that requests (e.g., HTTP requests to other services) are redirected to the sandbox server for a non-compliant device. EX1005, ¶¶[0042], [0078], [00147]-[0150].

223. Freund’s routing component monitors the service request and “determines whether or not the destination port is HTTP (port 80 TCP). If the destination port is HTTP, then the re-routing manager proceeds in step 951 to manipulate the destination IP address and port.” EX1005, ¶[0148].

224. Freund discloses that such requests to connect to other services are “redirected to the sandbox server.” *Id.*, ¶¶[0040], [0042], [0071].

225. Freund discloses allowing the non-compliant device to access the sandbox server to perform a defined set of tasks to address non-compliance, such as downloading appropriate software to correct non-compliance. *Id.*, ¶¶[0071], [0078].

226. Freund allows a non-compliant device to access remediation services. *See, e.g., id.*, Fig. 7. Any other communications from a non-compliant device are redirected to the sandbox server (i.e., quarantine server). *Id.*, ¶¶[0148]-[0150].

227. Freund’s system “enables the user to take the steps necessary to bring his or her computer back into compliance.” EX1005, ¶[0095].

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

228. Prompts such as “Update Now” in Figure 7 and “Download Now” in Figure 8, when selected, constitute service requests for accessing virus protection software updates “associated with a remediation request” as claimed. *Id.*, Fig. 7 (prompting user to select “Update Now!” button for remediation), ¶[0114] (“The message displayed in panel 702, as shown in FIG. 7, informs the user that he or she needs to update the virus protection software installed on the computer.”); Fig. 8 (prompting user to select “Download Now!” button for remediation), ¶[0116] (“error message panel 802 is displayed to the user indicating that there is a new version of the security software available and prompting the user to download the new version”).

229. The '048 Patent works this same way. *See, e.g.*, EX1001, 16:29-35 (“An example of a quarantine notification page is a web page that provides notification that the computer is quarantined, and/or provides links to remediation sites appropriate to the quarantine, such as a link to a site that provides anti-contagion software for removing a virus that the quarantined computer is believed to contain.”).

230. A non-compliant computer is “permitted *only* a limited Internet connection to the sandbox server” where “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. All other Internet access by the non-compliant computer is disabled.* [Emphasis added.]” EX1005, ¶[0042]. For example, when the

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

user selects the “Update Now” and “Download Now” prompts described above, Freund’s system forwards requests made by the non-compliant device to download updates (e.g., anti-virus software updates) given that such system-generated prompts are for the purpose of addressing the non-compliance.

231. Freund’s sandbox server provides a notification page including a link to a remediation service (e.g., “Update Now” and “Download Now” prompts). When a device attempts to download an anti-virus software update using the prompts, Freund’s client will generate a new outbound communication request. Freund’s router and CMP determine that the new outbound communication is an exempt request for remediation, thus forwarding the outbound communication to a remediation host providing the download and/or update for remediation. *See* EX1005, Figs. 7 and 8, ¶¶[0042], [0071], [0114]-[0116].

232. Freund filters a remediation request based on a destination address. EX1005, Fig. 9 (step 920). *See also*, Freund’s U.S. Provisional Application No. 60/303,653; EX1012, p.27. Freund discloses determining whether a destination address (e.g., to a remediation host) is exempt. EX1005; Fig. 7, ¶¶[0042], [0071], [0114].

233. A POSITA would have understood that Freund filters service requests (e.g., based on destination addresses) and forwards requests for remediation by establishing policy rules for permitting service requests to specific sites for

remediation. EX1005, ¶[0110] (“For example, rules can also be established on the basis of including and/or excluding access to particular Internet sites.”).

234. The ’048 Patent describes the same process as disclosed by Freund. *See* EX1001, Fig. 14, 15:8-15:38.

235. The ’048 Patent describes testing outbound traffic to determine whether the traffic is associated with remediation such as “contact with a verified remediation site”. *Id.*, 15:11-17. If the traffic is associated with a remediation request, then the traffic is forwarded to the destination. *Id.*, 15:17-20. Otherwise, the traffic is rerouted to the quarantine server. *Id.*, 15:17-31.

236. Freund discloses detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to the remediation host.

5. Claim 5: “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.”

237. Freund in view of Ball discloses and suggests claim 5.

238. Freund discloses that quarantining the device at the sandbox server includes preventing the device from receiving via the network data not related to remediation. Freund discloses that a non-compliant device “is redirected and permitted only a limited Internet connection to the sandbox server. In this situation,

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. All other Internet access by the non-compliant computer is disabled.” EX1005, ¶[0042] (emphasis added). *See also id.*, ¶[0095]; claim 6, *supra*.

239. By only permitting non-compliant devices to access the sandbox server and to perform defined tasks to address non-compliance, and disabling all other Internet access, Freund discloses and/or suggests preventing the device from receiving data not related to remediation of the insecure condition.

6. Claim 6: “A method as recited in claim 1, performed at an Internet service provider.”

240. Freund in view of Ball discloses and suggests claim 6.

241. Freund discloses “computers are now connected to the Internet, either directly (e.g., over a dial-up or broadband connection with an Internet Service Provider or ‘ISP’) or through a gateway between a LAN and the Internet”. EX1005, ¶[0008].

242. Freund’s Figure 3 shows router 310 as connecting a client computer 320 to the Internet 350 and therefore would have suggested to a POSITA that Freund’s method which is implemented with a router connection and a quarantine sandbox server 360, constitutes implementation of that method at Internet connection equipment of an ISP. EX1005, Fig. 3.

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

243. The '048 Patent contemplates an “ISP web server” as the “special quarantine server” referenced in claim 1. EX 1001,15:25-15:27; Fig. 14.

244. Freund’s system for network access management addresses common problems for ISPs such as attacks from malicious devices, unauthorized access, viruses, employee abuse of network systems, and network bandwidth.

245. U.S. Patent No. 5,987,611 (EX1020) (“Freund ’611”), incorporated by reference in Freund (EX1005, ¶[0017]), discloses an “ISP-based embodiment” that is “implemented for establishing a monitoring and filtering system” for ISPs. EX1020, 21:47-52. *See also id.*, Fig. 3B.

246. Both Freund ’611 and Freund are aimed at “maintaining security of individual computer systems and local area networks (LANs) connected to larger open networks (Wide Area Networks or WANs), including the Internet.” EX1020, 1:25-30. EX1005, ¶[0004].

247. Freund expressly incorporates Freund ’611 with reference to a “prior ZoneAlarm™ product” (EX1005, ¶[0017]). Freund is also directed to a ZoneAlarm product. *Id.*, ¶¶[0018]-[0021]. *See also id.*, Figs. 4-8.

248. Freund ’611 discloses that client devices can have “Internet access restricted to the ISP ‘Sandbox’ Server.” EX1020, 28:65-67, 27:51-30:10.

249. Freund ’611 expressly performs Freund’s methods at an ISP with an ISP sandbox server. It would have been obvious to implement Freund’s router and

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

sandbox server at an ISP to redirect service requests of non-compliant devices at least because Freund '611 explains that ISPs can “offer their users a tamper-proof, safe, and managed access to the Internet and protect[] the users from many security threats.” *Id.*, 21:53-55, 21:47-22:41.

250. Implementing Freund’s router and sandbox server at an ISP would have been a simple implementation taught and/or suggested by Freund '611 that would have led to predictable results of providing managed network access from an ISP for the types of networks Freund seeks to protect. EX1005, ¶¶[0019]-[0020].

251. A POSITA would have had a reasonable expectation of success given that Freund '611 describes a successful implementation of the ZoneAlarm 1.0 product. *Id.*, ¶[0017]. *See* EX1020 in its entirety.

252. Freund also discloses using “an independent piece of equipment (such as a router or DSL modem)” and a quarantine server to implement its network access method. EX1005, ¶[0039].

253. A POSITA would have understood that DSL modems and/or routers and/or servers connect networks (e.g., private networks) to receive Internet access. *See* EX1020, 21:59-22:6.

254. Freund’s techniques for access management are performed at an ISP device, such as a DSL modem or an ISP router with a quarantine server to provide security policies and quarantine services to private networks.

255. Freund therefore discloses and/or renders obvious performing the disclosed method at an ISP at least because devices within a protected network disclosed by Freund will attempt to connect to the Internet via an ISP service and related equipment.

256. Freund discloses performing the method of claim 1 at an ISP interface to the Internet.

7. Claim 7: “A method as recited in claim 1, wherein the software component on the first host is an operating system.”

257. Freund in view of Ball discloses and suggests claim 7.

258. Freund discloses the software component on the first host is an operating system. Freund discloses that its devices “include[] a kernel or operating system (OS) 210.” EX1005, ¶[0063]. *See id.*, Fig. 2.

259. Freund also discloses various security issues that can arise with operating systems. *See* EX1005, ¶¶[0015], [0019]. *See also* Claim 4, *supra*.

260. Freund specifically warns against operating system “security holes”. EX1005, ¶¶[0015], [0019].

261. Freund discloses detecting devices having out-of-date software components, and Freund teaches that the software component can include an operating system at least because operating systems being out-of-date can pose a well-known security threat and will cause a device to be out of compliance with

established security policies. Freund also teaches that other security policies can be used for enforcement. EX1005, ¶¶[0103], [0110].

262. A POSITA would have understood that a device having an out-of-date operating system would be non-compliant with Freund's disclosed security policies and other possible security policies. *See* EX1005, ¶¶[0068], [0071]-[0072], [0078], [0085]-[0089]; *see also*, EX1006, ¶[0031].

8. Claim 8: “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.”

263. Freund in view of Ball discloses and suggests claim 8.

264. Freund discloses determining an insecure condition by determining a software component on the first host is not sufficiently updated (i.e., anti-virus software out-of-date). Freund discloses determining that a device is not clean when the CMP and/or router-side security module “looks for the appropriate code to verify if the anti-virus program is running on the client machine and if both the anti-virus program and the associated data file are up to date.” EX1005, ¶[0132]. *See also id.*, ¶¶[0114], [0117], [0144] (“ZAP version outdated 33 Client application incorrect or old.”), Figs. 7 and 8. Freund discloses determining that the response does not include a valid digitally signed attestation of cleanliness, where cleanliness includes that a software component (i.e., anti-virus software) on the device is sufficiently updated.

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

265. Kappes demonstrates that those skilled in the art would have understood Freund in view of Ball to disclose storing a content authentication token within the first host. “The content authentication token framework can and the token scheme be implemented with a trusted program (or a set of trusted programs) running on the client device 110.” EX1007, ¶[0049]. “This secure program can participate in the challenge/response protocol for content authentication.” *Id.* Kappes’ demonstrates that a POSITA would have understood Freund’s router challenge/response to access a digitally signed content authentication token to detect the insecure condition. According to Kappes, “[t]he trusted program can be provided, for example, on a Smart Card, driver or run inside a secure portion of the device 110.” EX1007, ¶[0049]. *See also* EX1008, pp.3-21.

266. The TCG Specification, incorporated by reference in Ball, also supports the attestation of Freund, as the TCG Specification expressly discloses a TPM and components thereof, stating that “[i]mplementations of TPMs may be done in hardware or software.” EX1008, p.19. TCG Specification also notes that a TPM is “a building block of a trusted platform”. *Id.* A diagram and a component architecture of a TPM are also presented.

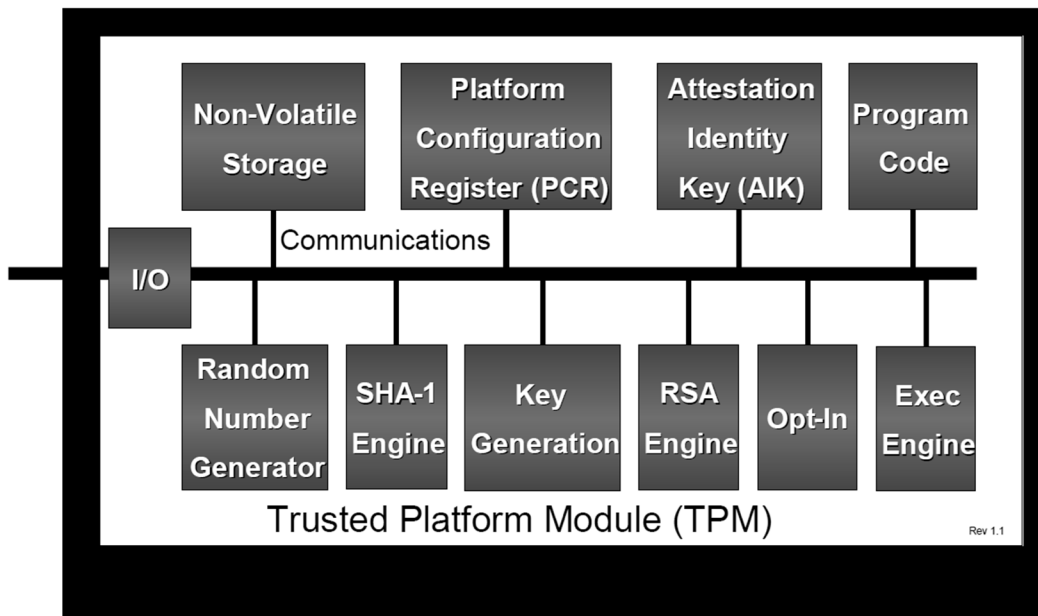


Figure 4:g – TPM Component Architecture

See also, EX1008, pp.19-26.

267. Implementing Ball’s TPM with its TCG Specification to provide the security features of Freund with a content authentication process and trusted program would have been a straightforward combination of known elements according to known methods to yield predictable results. EX1007, ¶[0049].

9. Claim 9: “A method as recited in claim 8, 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.”

268. Freund in view of Ball discloses and suggests claim 9.

269. Freund discloses determining that a software component on the device (e.g., anti-virus software) is not sufficiently updated. See Claim 8, *supra*.

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

270. Freund discloses that “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”. EX1005, ¶[0078] (emphasis added).

271. Freund’s failed router challenge due to “running an older version” of the security software constitutes a disclosure and suggestion that “a patch level ... is not sufficiently recent.” *See also* EX1009, ¶[0019] (“A versioning table contains a list of root file numbers and version numbers. This information is used to track application patches and upgrades. Each entry in the versioning table corresponds to one patch level...”).

272. Freund discloses the software components of the first host include an operating system. EX1005, ¶[0063] (devices “include[] a kernel or operating system (OS) 210.”), Fig. 2. *See* Claims 3/4, *supra*.

273. Freund discloses that operating systems can have “well-known security holes.” EX1005, ¶[0015]. *See also* Claim 4, *supra*.

274. A POSITA would have understood that out-of-date anti-virus software and/or operating systems including well-known security holes would violate security policies and that these software components would include a patch or patch level that is not sufficiently recent.

275. Freund's disclosure of updates to anti-virus software or operating systems would encompass patches or patch levels.

10. Claim 10 (Preamble): "A system, comprising:"

276. To the extent the Preamble is limiting, Freund discloses and suggests the Preamble.

277. Freund discloses a system for protecting a network. *See* Claim 1 (Preamble), *supra*. *See also* Fig. 3.

278. Freund "provides a security system that delegates enforcement of certain security policies to software that is not running on a local computer but instead running on another piece of equipment" on the same LAN. EX1005, ¶[0068].

279. Freund's Fig. 3 discloses a system including a router for monitoring client requests within the private network. EX1005, ¶¶[0073]-[0074], Fig.3.

280. Freund's system includes a router executing the CMP connected to and serving multiple devices (e.g., personal computers) having the client-side security module stored thereon (where computer 330 is not running the client-side security module). *Id.* Freund's system also includes the sandbox server residing somewhere on the Internet. *Id.* Freund's system using the client-side security modules, the router and the CMP to monitor network traffic is configured to protect the devices on the private network from transmitting or receiving malicious or unauthorized data. EX1005, ¶¶[0068]-[0072].

a. [10.1]: “a processor configured to:”

281. Freund discloses and suggests Element [10.1].

282. Freund’s system can be “implemented on a conventional or general-purpose computer system” including “a central processing unit(s) (CPU) or processor (s)” where “any other suitable microprocessor or microcomputer may be utilized for implementing the present invention.” EX1005, ¶¶[0055]-[0056].

283. Freund discloses a system including a processor.

b. [10.2]: “detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,”

284. Freund discloses and suggests Element [10.2]. *See* Element [1.1], *supra*.

c. [10.3]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,”

285. Freund in view of Ball discloses and suggests Element [10.3]. *See* Element [1.2], *supra*.

d. [10.4]: “receiving a response, and”

286. Freund discloses and suggests Element [10.4]. *See* Element [1.3], *supra*.

- e. **[10.5]: “determining whether the response includes a valid digitally signed attestation of cleanliness,”**

287. Freund in view of Ball discloses and suggests Element [10.5]. *See* Element [1.4], *supra*.

- f. **[10.6]: “wherein the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;”**

288. Freund discloses and suggests Element [10.6]. *See* Element [1.5], *supra*.

- g. **[10.7]: “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,”**

289. Freund discloses and suggests Element [10.7]. *See* Element [1.6], *supra*.

- h. **[10.8]: “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,”**

290. Freund discloses and suggests Element [10.8]. *See* Element [1.7], *supra*.

- i. **[10.9]: “determining whether the service request sent by the first host is associated with a remediation request, and”**

291. Freund discloses and suggests Element [10.9]. *See* Element [1.8],
supra.

- j. **[10.10]: “when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request,”**

292. Freund discloses and suggests Element [10.10]. *See* Element [1.9],
supra.

- k. **[10.11]: “wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and”**

293. Freund discloses and suggests Element [10.11]. *See* Element [1.10],
supra.

- l. **[10.12]: “permit the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition; and”**

294. Freund discloses and suggests Element [10.12]. *See* Element [1.11],
supra.

m. [10.13]: “a memory coupled to the processor and configured to provide instructions to the processor.”

295. Freund discloses and suggests Element [10.13].

296. Freund discloses the system including a memory coupled to the processor and configured to provide instructions to the processor. EX1005, ¶¶[0055]-[0058].

11. Claim 11: “A system as recited in claim 10, 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.”

297. Freund in view of Ball discloses and suggests claim 11. *See* claim 2, *supra*.

12. Claim 12: “A system as recited in claim 10, 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.”

298. Freund in view of Ball discloses and suggests claim 12. *See* claim 10, *supra*, regarding the system processor. Freund discloses a processor 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. Freund specifically warns against OS “security holes” (EX1005, ¶¶[0015], [0019]), such as security vulnerabilities or security non-compliance. *See* Claim 3, *supra*. Freund recognizes that a “user may inadvertently disable previously installed security software in the

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

process of upgrading his or her operating system” (EX1005, ¶[0019]) and recognizes that security software can be disabled at OS installation/upgrade. A POSITA would have been motivated to use Freund’s security compliance system to ensure a device remains compliant after OS installation. *See also*, EX1006, ¶[0031]. A POSITA would have had a reasonable expectation of success given Freund’s disclosed OS installation/upgrade security compliance procedure and security policies. *Id.*, ¶[0071].

- 13. Claim 13: “A system as recited in claim 10, 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.”**

299. Freund in view of Ball discloses and suggests claim 13. *See* claim 5, *supra*.

- 14. Claim 14: “A system as recited in claim 10, wherein the software component on the first host is an operating system.”**

300. Freund in view of Ball discloses and suggests claim 14. *See* claim 7, *supra*.

- 15. Claim 15: “A system as recited in claim 10, 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.”**

301. Freund in view of Ball discloses and suggests claim 15. *See* claim 8, *supra*.

- 16. Claim 16: “A system as recited in claim 15, 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.”**

302. Freund in view of Ball discloses and suggests claim 16. *See* claim 9, *supra*.

- 17. Claim 17 (Preamble): “A computer program product, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:”**

303. To the extent the Preamble is limiting, Freund discloses and suggests the Preamble.

304. Freund discloses a computer program product for protecting a network where the computer program product is embodied in a non-transitory computer readable medium and comprising computer instructions.

305. Freund discloses that “program logic” for its network protection system “is loaded from the storage device or mass storage 116 into the main (RAM) memory 102, for execution by the CPU 101.” EX1005, ¶[0058].

306. Freund's storage device or mass storage storing program logic constitutes the computer program product embodied in a non-transitory computer readable medium.

n. [17.1]: “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,”

307. Freund discloses and suggests Element [17.1]. *See* Element [1.1], *supra*.

o. [17.2]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,”

308. Freund in view of Ball discloses and suggests Element [17.2]. *See* Element [1.2], *supra*.

p. [17.3]: “receiving a response, and”

309. Freund in view of Ball discloses and suggests Element [17.3]. *See* Element [1.3], *supra*.

q. [17.4]: “determining whether the response includes a valid digitally signed attestation of cleanliness,”

310. Freund in view of Ball discloses and suggests Element [17.4]. *See* Element [1.4], *supra*.

- r. [17.5]: “wherein the valid digitally signed attestation of cleanliness includes at least one attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;”

311. Freund discloses and suggests Element [17.5]. *See* Element [1.5],

supra.

- s. [17.6]: “when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,”

312. Freund discloses and suggests Element [17.6]. *See* Element [1.6],

supra.

- t. [17.7]: “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,”

313. Freund discloses and suggests Element [17.7]. *See* Element [1.7],

supra.

- u. [17.8]: “determining whether the service request sent by the first host is associated with a remediation request, and”

314. Freund discloses and suggests Element [17.8]. *See* Element [1.8],

supra.

- v. [17.9]: “when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request,”

315. Freund discloses and suggests Element [17.9]. *See* Element [1.9],
supra.

- w. [17.10]: “wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and”

316. Freund discloses and suggests Element [17.10]. *See* Element [1.10],
supra.

- x. [17.11]: “permitting the first host to communicate with a remediation host configured to provide data usable to remedy the insecure condition.”

317. Freund discloses and suggests Element [17.11]. *See* Element [1.11],
supra.

- 18. **Claim 18:** “A computer program product as recited in claim 17, wherein the software component on the first host is an operating system.”

318. Freund discloses and suggests claim 18. *See* claims 7, 14, and 17,
supra.

19. Claim 19: “A computer program product as recited in claim 17, 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.”

319. Freund discloses and suggests claim 19. *See* claims 8, 15, and 17, *supra*.

20. Claim 20: “A computer program product as recited in claim 19, 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.”

320. Freund discloses and suggests claim 20. *See* claims 9, 16, and 17, *supra*.

XII. SECONDARY CONSIDERATIONS

321. As discussed herein, all elements of the Challenged Claims were known in the art, and any differences would have been obvious to a POSITA based on the disclosures of the applied references and the knowledge in the art.

322. I am not aware of any secondary considerations that would alter my opinion.

323. Any secondary considerations evidence Patent Owner may offer in this proceeding would be insufficient to overcome the strong evidence that the Challenged Claims are obvious.

XIII. CONCLUSION

324. For the reasons set forth above, it is my opinion that all elements of the Challenged Claims of the '048 Patent are disclosed or suggested by the prior art. In my opinion, the Challenged Claims of the '048 Patent are anticipated by and/or would have been obvious over the prior art.

325. In signing this Declaration, I understand that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I acknowledge that I may be subject to cross-examination in the case and that cross-examination will take place within the United States. If cross-examination is required of me, I will appear for cross-examination within the United States during the time allotted for cross-examination.

326. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Date: September 18, 2025



Markus Jakobsson

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

APPENDIX 1

I have previously testified and/or been consulted as an expert in the following matters:

Case	Number if known	Jurisdiction
Govt v House		Ohio
Govt v Blackwell		Ohio
PacId v Apple	6:09cv143-LED-JDL (Filed 3/30/2009 USDC E.D. TX)	E Texas (Tyler)
Datatreasury Corp v Royal Bank of Canada	T-1661-07 (Filed 9/13/2007 Federal Court, Canada; Toronto)	Federal Court, Canada
Quantumworld v Dell	11-cv-00688 (Filed 6/3/2010 USDC W.D. Texas)	E Texas (Marshall), moved to W Texas
RootZoo v Facebook	C 09-03043 (Filed 7/7/2009 USDC N.D. CA)	N California (San Jose)
Cloakworks Inc v Cloakware Inc	CV08-020244 PJH	N California
Farr v St Francis		Indiana
Sobel patent re-examination	patent 7,366,919 (Filed 4/25/2003, USPTO)	N/A
Yahoo! v Facebook	12-cv-01212 (Filed 3/12/2012 USDC N.D. CA)	N California
Prism v. Adobe	10-cv-00220 (Filed 6/8/2010 USDC Nebraska)	Nebraska
Symantec Finjan Inc. v. McAfee Inc. et al (including Symantec)	patent 6,480,962 (Filed 7/12/2010 USDC Delaware)	N/A
	patent 7,506,155	N/A
Patent reexam, by Symantec against IV	patent 7,506,155	N/A
Symantec Intellectual Ventures LLC v. Check Point Software Technologies, et al (including Symantec)	patent 6,460,050 (Filed 12/8/2010 USDC Delaware)	N/A
RMAIL Limited v. Amazon et al	2:10-cv-258-JRG (Filed 7/21/2010 USDC E.D. Texas)	ED Texas
Comcast Cable et al v. BT Americas Inc et al	3:12-cv-01712-B	N Texas

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

Case	Number if known	Jurisdiction
Geotag, Inc v. Frontier Communications Corp, et al.	Civil Action No. 2:10-cv-00265 (consolidated), Civil Action No. 2:12-cv-00471, Case No. 2:12-cv-00525-JRG, Case No. 2:12-cv-00465, 2:10-CV-265-JRG	E TX (Marshall)
Adobe Systems Inc adv Computer Software Protection LLC	USDC-DE-C.A. No 12-451-SLR	DE
THE TRUSTEES OF COLUMBIA UNIVERSITY IN THE CITY OF NEW YORK v. Symantec	Civil Action No. 3:13-cv-00808-JRS	E Virginia (Richmond)
Intertrust v. Apple	CASE NO. C13-1235 YGR	N California
PARZIVAND ENTERPRISES, INC . d/b/a WORLDWIDE DISTRIBUTORS, JONATHAN PARZIVAND, AND AZITA SHALOM v. eBay INC . and PAYPAL, INC .,	Claim No. AAA No . 01-1 4-0000 - 4837	California
MUSIC GROUP MACAO COMMERCIAL OFFSHORE LIMITED, a Macao entity, vs. DAVID FOOTE	3:14-cv-03078 JSC	N California
Alcatel-Lucent USA v. Fortinet litigation	<u>Civil Action No. 1:14-cv-00574-UNA</u>	Delaware
SOPHOS LIMITED and SOPHOS INC., v. FORTINET, INC.,	C.A. No. 14-100 (GMS)	Delaware
Yozons v. Docusign	3:15-cv-05041	N California
Sandhu v. Dhami & Bal (Sandeep Singh Dhami and Brinda Kaur Bal)		
Intellectual Ventures II LLC v. Bitco General Insurance Corp., f/k/a, § Bituminous Casualty Corp.; and § Bitco National Insurance Co., f/k/a § Bituminous Fire and Marine Insurance Co.,	6:15-CV-59-JRG	E Texas (Tyler)

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

Case	Number if known	Jurisdiction
Intellectual Ventures I LLC and Intellectual Ventures II LLC, v. Sally Beauty Holdings, Inc., and Sally Beauty Supply LLC	CIVIL ACTION NO. 2:15-CV-1414-JRG	ED Texas
Trend Micro c. RPOST	Case No. 3:13-cv-5227-VC	N California
BlackBerry Limited, et al. v. Avaya, Inc.,	Case No. 3:16-cv-2185-M (N.D. Tex.)	N Texas
Zscaler v Symantec	2:16-cv-1176-SLR (Delaware)	Delaware
UNIVERSAL SECURE REGISTRY v APPLE VISA INC., and VISA U.S.A., INC.,	1:99-mc-09999	Delaware
SEVEN Networks, LLC v. Google Inc. et al., Case No. 2:17-cv-00442-JRG (EDTX) and Google Inc. v. SEVEN Networks, LLC, Case No. 3:17-cv-04600-WHO (NDCA)		NDCA
Google v. Confident Technologies		
RPOST Holdings et al v. Adobe Systems Inc et al	Case 2:11-cv-325	ED TX
Class (Elisabeth Borchers) v. Xceligent		Missouri Western District Court
Bohannon v. Innovak		Alabama
Zscaler v Symantec	U.S. Patent No. 8,316,429 (two petitions)	
BlackBerry Limited, et al. v. Facebook, Inc.,	Case No. 2:18-cv-01844	(C.D. Cal.)
Blue Spike, LLC v. VIZIO, Inc	8:17-cv-01172-DOC-KES	CD Cal
Zscaler IPR 8316429, 8402540, 9525696	IPR2018-00912, IPR2018-00913, IPR2018-00930, IPR2018-00920	
CUPP Cybersecurity, LLC v. Trend Micro, Inc	3:18-cv-01251	N. Texas
Philips v. ASUS and Acer	Case No. 18-cv-01885-HSG	
Facebook, Inc. et al. v. Blackberry Limited	IPR Case No. IPR2019-00923	

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

Case	Number if known	Jurisdiction
Intertrust v. Cinemark, 2:19-cv-00266-JRG (E.D. Tex. 2019) Intertrust v. AMC, 2:19-cv-00265-JRG (E.D. Tex. 2019) Intertrust v. Regal, 2:19-cv-00267-JRG (E.D. Tex. 2019) Dolby v. Intertrust, 3:19-cv-03371-EMC (N.D. Cal. 2019)		ED Tex
UNILOC 2017, LLC et al. v Google LLC	Case No. 2-18-cv-00504-JRG-RSP	ED Tex
UNILOC 2017, LLC et al. v Google LLC	Case No. 2:18-CV-00493-JRG-RSP Case No. 2:18-CV-00499-JRG-RSP Case No. 2:18-CV-00502-JRG-RSP	ED Tex
DeCurtis LLC v. Carnival Corp.,	Case No. 6:20-cv-00607 (M.D. Fla) and/or Carnival Corp. v. DeCurtis Corp., et al., Case No. 1:20-cv-21547 (S.D. Fla).	MD FL + SD FL
MobileIron v. Blackberry	Case No. 3:20-cv-02877-JCS	ND Cal
Rafael and Rafi Nehushtan adverse to Samsung	Pre-trial, no case number	
CUPP Cybersecurity, LLC v. Trend Micro, Inc		
Daedalus Blue, LLC v. Microsoft Corp.,	Case No. 6:20-cv-1152	WDTX
Koninklijke KPN N.V. v Ericsson		
MOBILE EQUITY CORP., v. WALMART INC.,	Case No. 2:21-cv-00126-JRG-RSP	ED TX
Palantir v. Abramowitz et al.	Case No. 5:19-cv-06879-BLF	
DivX v Hulu	2-19-cv-01606-CDCA	
Pre-IPR: F5 Networks, Inc., et al., v. Sunstone Information Defense, Inc.		
Zoho Corp v. Liberty PeakVentures LLC	case 1:22-cv-00037	WDTX
Finjan LLC v. Palo Alto Networks, Inc.	Case No. 4:14-cv-04908-JD	NDCA
Ant (pre-litigation work)	TBD	
R.N Nehushtan Trust Ltd. v. Apple Inc. -	3:22-cv-01832-WHO	NDCA

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

Case	Number if known	Jurisdiction
Webroot, Inc. and Open Text, Inc. v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc	IPR - U.S. Patent Nos. 8,201,243 (IPR2023-01052), 8,719,932 (IPR2023-01051), 8,763,123 (IPR2023-01050), and 11,409,869 (IPR2023-01053)	
Webroot, Inc. and Open Text, Inc. v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc	IPR -- U.S. Patent Nos. 8,856,505 (IPR2023-01159) and 8,181,244 (IPR2023-01158)	
Security First Innovations, LLC v. Google LLC		
T-Mobile SIM Swap Arbitration: Christian Nielsen v. T-Mobile USA, Inc. (AAA Case No. 01-22-0002-5108)		
Hamilcar Barca v. Western Digital	pre-lit	
Taasera Licensing LLC v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.;	Civil Action No. 2:22-cv-00498-JRG (E.D. Tex.); Civil Action No. 2:22-md-03042- JRG (E.D. Tex.); Civil Action No. 6:22-cv-01094-ADA (W.D. Tex.)	
Inter Partes Review Regarding U.S. Patent No. 9,071,518		
<i>IBM v. Zynga, C.A. No. 22-590-GBW (D. Del.)</i>		
SQWIN SA v Walmart, Inc.	4:22-cv-01040-SDJ	EDTX
Giesecke & Devrient GmbH v. United States	17-cv-01812 (RTH)	
Klein v Meta	3:20-cv-08570-JD	NDCA
Telefonaktiebolaget ML Ericsson v. Lenovo	<i>ITC Inv. No. 337-TA-1375, Inv. No. 337-TA-1376, 5:23-cv-569, 5:23-cv-570</i>	ITC, EDNC
<i>GoSecure, Inc. v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.</i>	IPR 9,106,697 (IPR2025-00067, IPR2025-00069) and 9,954,872 (IPR2025-00068, IPR2025-00070)	
Commure, Inc. v. Canopy Works, Inc., et al.	3:24-cv-02592-AMO	(N.D. Cal.)
QOMPLX v. Microsoft Corporation and Palo Alto Networks, Inc		

Declaration of Markus Jakobsson in Support of
Petition for *Inter Partes* Review of U.S. Patent No. 9,516,048

Case	Number if known	Jurisdiction
Mobile Equity Corp. ("MEC")	litigation and/or IPR proceedings involving U.S Patent Nos. 8,589,236 (IPR2022-00380) and 10,535,058 (IPR2022-00379)	