

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

GOOGLE LLC  
Petitioner

v.

K.MIZRA LLC  
Patent Owner

---

Case No. IPR2025-01436  
Patent 8,234,705

---

**DECLARATION OF MARKUS JAKOBSSON IN SUPPORT OF PETITION  
FOR INTER PARTES REVIEW OF U.S. PATENT NO. 8,234,705**

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

**TABLE OF CONTENTS**

	<b>Page</b>
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 '705 Patent .....	10
VII. THE '705 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 .....	22
A. Claims 1-19 Are Obvious Over Freund (EX1005) in view of Ball (EX1006), Pujare (EX1009), and Lewis (EX1013) (Ground 1) .....	22
1. Claim 1 (Preamble): “A method for protecting a network, 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,” .....	24
b. [1.2]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,” .....	26
c. [1.3]: “receiving a response, and” .....	31
d. [1.4]: “determining whether the response includes a valid digitally signed attestation of cleanliness,” .....	32
e. [1.5]: “wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;” .....	34
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,” .....	38

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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,” .....	39
h.	[1.8]: “serving a quarantine notification page to the first host when the service request comprises a web server request, and” .....	40
i.	[1.9]: “in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and” .....	42
j.	[1.10]: “permitting the first host to communicate with the remediation host.” .....	50
2.	Claim 2: “A method as recited in claim 1, wherein detecting an insecure condition further includes at least one of the following: scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.” .....	51
3.	Claim 3: “A method as recited in claim 1, wherein detecting an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.” .....	53
4.	Claim 4: “A method as recited in claim 1, wherein detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.” .....	54
5.	Claim 5: “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	

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

	outbound communication if it is addressed to the remediation host.” .....	56
6.	Claim 6: “A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.” .....	61
7.	Claim 7: “A method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.” .....	62
8.	Claim 8: “A method as recited in claim 1, performed at an Internet service provider.” .....	63
9.	Claim 9: “A method as recited in claim 1, wherein the software component on the first host is an operating system.” .....	66
10.	Claim 10: “A method as recited in claim 1, wherein determining that the response does not include a valid digitally signed attestation of cleanliness includes determining that the software component on the first host is not sufficiently updated.” .....	67
11.	Claim 11: “A method as recited in claim 1, wherein determining that the software component on the first host is not sufficiently updated includes determining that a patch level associated with the software component on the first host is not sufficiently recent.” .....	69
12.	Claim 12 (Preamble): “A system for protecting a network, comprising:” .....	71
a.	[12.1]: “a processor configured to:” .....	72

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

- b. [12.2]: “detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,” .....72
- c. [12.3]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,” .....72
- d. [12.4]: “receiving a response, and” .....72
- e. [12.5]: “determining whether the response includes a valid digitally signed attestation of cleanliness,” .....73
- f. [12.6]: “wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host; ” .....73
- g. [12.7]: “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,” .....73
- h. [12.8]: “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,” .....73
- i. [12.9]: “serving a quarantine notification page to the first host when the service request comprises a web server request, and” .....74
- j. [12.10]: “in the event the service request comprises a DNS query, providing in response an IP address

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

	of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and” .....	74
k.	[12.11]: “permit the first host to communicate with the remediation host; and” .....	74
l.	[12.12]: “a memory coupled to the processor and configured to provide instructions to the processor.” .....	74
13.	Claim 13: “A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by performing one or more of the following: scanning for a vulnerability, scanning for malicious data, determining whether a security software is installed, and detecting anomalous network traffic.” .....	75
14.	Claim 14: “A system as recited in claim 12, wherein the processor is configured to detect an insecure condition at least in part by determining that an initial startup after installation of an operating system is being performed.” .....	75
15.	Claim 15: “A system as recited in claim 12, wherein the processor is configured to quarantine the first host at least in part by preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.” .....	75
16.	Claim 16: “A system as recited in claim 12, wherein the software component on the first host is an operating system.” .....	75
17.	Claim 17: “A system as recited in claim 12, wherein determining that the response does not include a valid digitally signed attestation of cleanliness includes determining that the software component on the first host is not sufficiently updated.” .....	76

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

- 18. Claim 18: “A system as recited in claim 17, wherein determining that the software component on the first host is not sufficiently updated includes determining that a patch level associated with the software component on the first host is not sufficiently recent.” .....76
  
- 19. Claim 19 (Preamble): “A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:” .....76
  - a. [19.1]: “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,” .....77
  
  - b. [19.2]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,” .....77
  
  - c. [19.3] receiving a response, and .....77
  
  - d. [19.4] determining whether the response includes a valid digitally signed attestation of cleanliness, .....77
  
  - e. [19.5] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host; .....78
  
  - f. [19.6] 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, .....78

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

- g. [19.7] 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,.....78
- h. [19.8] serving a quarantine notification page to the first host when the service request comprises a web server request, and .....78
- i. [19.9] in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and .....79
- j. [19.10] permitting the first host to communicate with the remediation host. ....79

XII. SECONDARY CONSIDERATIONS .....79

XIII. CONCLUSION.....80

APPENDIX 1

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

Exhibit No.	Description
1001	U.S. Patent No. 8,234,705, issued July 31, 2012
1002	File History of U.S. Patent Application No. 11/237,003
1003	Not Assigned
1004	U.S. Provisional Application 60/613,909
1005	U.S. Patent Publication No. 2003/0055962, published March 20, 2003 to G. Freund <i>et al.</i> (“Freund”)
1006	U.S. Patent Application Publication No. 2006/0005009, published January 5, 2006 to C. Ball <i>et al.</i> (“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 <i>et al.</i> (“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.)
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.)

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

Exhibit No.	Description
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>
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. 8,234,705

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 1-19 (“the Challenged Claims”) of U.S. Patent No. 8,234,705 (“the ’705 Patent”) (EX1001).

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

3. I understand that the ’705 Patent is assigned to K.MIZRA LLC.

4. I have been asked to provide an independent analysis of the ’705 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 ’705 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 ’705 Patent.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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. 8,234,705

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. 8,234,705

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 '705 Patent, the references cited by the '705 Patent, the prosecution histories of the '705 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. 8,234,705

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. 8,234,705

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. 8,234,705

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. 8,234,705

- 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. 8,234,705

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 1-19 of the '705 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), U.S. Patent Application Publication No. 2002/0083183 to Pujare <i>et al.</i> ("Pujare") (EX1009), and U.S. Patent No. 7,533,407 to Lewis <i>et al.</i> ("Lewis") (EX1013)	103	1-19

#### V. TECHNOLOGY BACKGROUND

27. The '705 Patent is directed to computer network-based contagion isolation and inoculation, to protect a private network from roaming "hosts" that connect to outside networks (e.g., the Internet) with attendant vulnerability to hosting a virus infestation. The Challenged Claims recite protecting a network by detecting an insecure condition on the host and quarantining the host from connecting to a network via, for example, domain name system (DNS) and web server service requests. A trusted computing base verifies the host's cleanliness. When an insecure condition is detected, trusted network security components

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

redirect the insecure host's service request to a "quarantine" server. The quarantine server serves a quarantine notification page to the insecure host. *See* EX1001, 3:8-23; 14:4-12; EX1002, p.21. The quarantine notification page provides notice and/or instructions to the quarantined host device to remedy the insecure condition (e.g., download an anti-virus software update from a remediation host). EX1001, 3:13-23; 16:11-43.

## **VI. THE CHALLENGED '705 PATENT**

28. The '705 Patent contains 19 claims. I have been asked to opine on the validity of Claims 1-19.

## **VII. THE '705 PATENT PROSECUTION HISTORY**

29. I have reviewed the file history of the '705 Patent.

30. In response to rejections made during prosecution, Applicant amended the claims to recite specifics of the digitally signed attestation of cleanliness, including "the presence of a patch or patch level associated with a software component". EX1002, pp.38-45. An Examiner's Amendment included "in the event the service request comprises a DNS query, providing in response an IP address to a quarantine server". *Id.*, pp.25-28. The Examiner stated that Liang and Yan fail to anticipate or render obvious "serving both the specific quarantine notification page with the DNS redirection when in combination with the remaining claim

limitations.” *Id.*, p.21. This Petition cites prior art which clearly discloses the allowable subject matter.

31. The ’705 Patent was previously challenged in IPR2021-00593 filed by Cisco that settled earlier this year. EX1016, EX1017, EX1018. While the Final Written Decision initially upheld the claims, 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 where Patent Owner settled. EX1017. Validity was therefore left unresolved.

#### **VIII. LEVEL OF ORDINARY SKILL IN THE ART**

32. 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.

33. 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.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

34. 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 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 ’705 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 ’705 Patent are actually entitled to that date.

**IX. CLAIM CONSTRUCTION**

35. For purposes of my analysis in this IPR proceeding, I have been informed that terms that appear in the claims of the ’705 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.

36. 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

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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 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.

37. I have reviewed the ’705 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 ’705 Patent are in dispute in a related litigation.

38. 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.

39. 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:

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

40. 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.

41. 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.2. PO 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* EX1015, p.4. EX1024, p.6..

42. 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).

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

43. 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.

44. I understand that in the Related Litigation, Petitioner proposes this phrase should be construed as:

**includes at least one of an . . . and at least one of an . . .**

*See* EX1014, p.11.

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

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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 40-56 and column 15, lines 36-50 of the ’705 Patent (i.e., “servers providing security patches or advisories, for example allowing connections to a vendor’s server, or providing virus and worm disinfecting tools, such as focused removal tools, or data updates for previously installed repair tools”; “vendor sites known to provide remediation assistance, such as to Microsoft's Windows Update service, where security patches may be obtained.”; “a security update site such as Microsoft Windows Update.”; and “a remediation site, such as a security update service such as Microsoft Windows Update”). Thus, for compliance with 37 C.F.R. §42.104(b)(3), a ‘remediation host’ encompasses, for example, a site from which remediation assistance is received.

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 Related Litigation, the prior art cited herein discloses the terms with at least the same level of detail including corresponding structure and claimed functions as described in the ’705 Patent.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

49. The prior art cited herein discloses the noted terms under Petitioner's and PO's proposed constructions and any other constructions, as demonstrated herein.

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

51. 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.

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

## **X. OVERVIEW OF THE PRIOR ART REFERENCES**

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

53. 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. 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].

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

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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.

58. 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].

59. 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. *Id.*, ¶[0006].

60. 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). *Id.*, ¶[0033].

61. 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. *Id.*, ¶¶[0030], [0033].

**C. Kappes (EX1007)**

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

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

64. The restoration services use “standard packet filtering techniques” to filter web server requests and DNS requests. *Id.*, ¶¶[0029], [0038].

**D. Pujare (EX1009)**

65. Pujare discloses a “versioning table” that makes clear that application patches are merely software upgrades. EX1009, ¶[0019].

66. Pujare’s versioning table contains a list of root file numbers and version numbers. *Id.* The root file numbers and version numbers are used to track the application patches and upgrades. *Id.*

67. 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)**

68. 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. *See also id.*, 14:4-24; Fig. 8B.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

69. 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. *See also id.*, 11:15-17, 14:4-24. This causes non-compliant devices to be routed to a fix-up page of the quarantine server. *Id.*

70. The earlier publication of Lewis (U.S. Patent Application Publication No. 2005/0131997) was cited in the examination history of the ’705 Patent. EX1002, p.187. The Examiner relied on Lewis to reject a portion of dependent claims. *See id.*, pp.68-69, 112-113, 187-189. Applicant never disputed the Examiner’s assertions regarding Lewis and its disclosure concerning Element [1.9] (*see* VII.A.1.i. below).

71. 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 the ’705’s purported novel features. Further, Lewis discloses an exemplary embodiment called out in the ’705 Patent.

**F. Kouznetsov (EX1021)**

72. Kouznetsov discusses software application management and discloses that maintenance of software applications (e.g., anti-virus software) includes

implementation of incremental improvements, such as patches, updates, and versions. EX1021, 1:39-3:33.

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

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

### **A. Claims 1-19 Are Obvious Over Freund (EX1005) in view of Ball (EX1006), Pujare (EX1009), and Lewis (EX1013) (Ground 1)**

74. The following sections reference where elements of Claims 1-19 are obvious over the prior art.

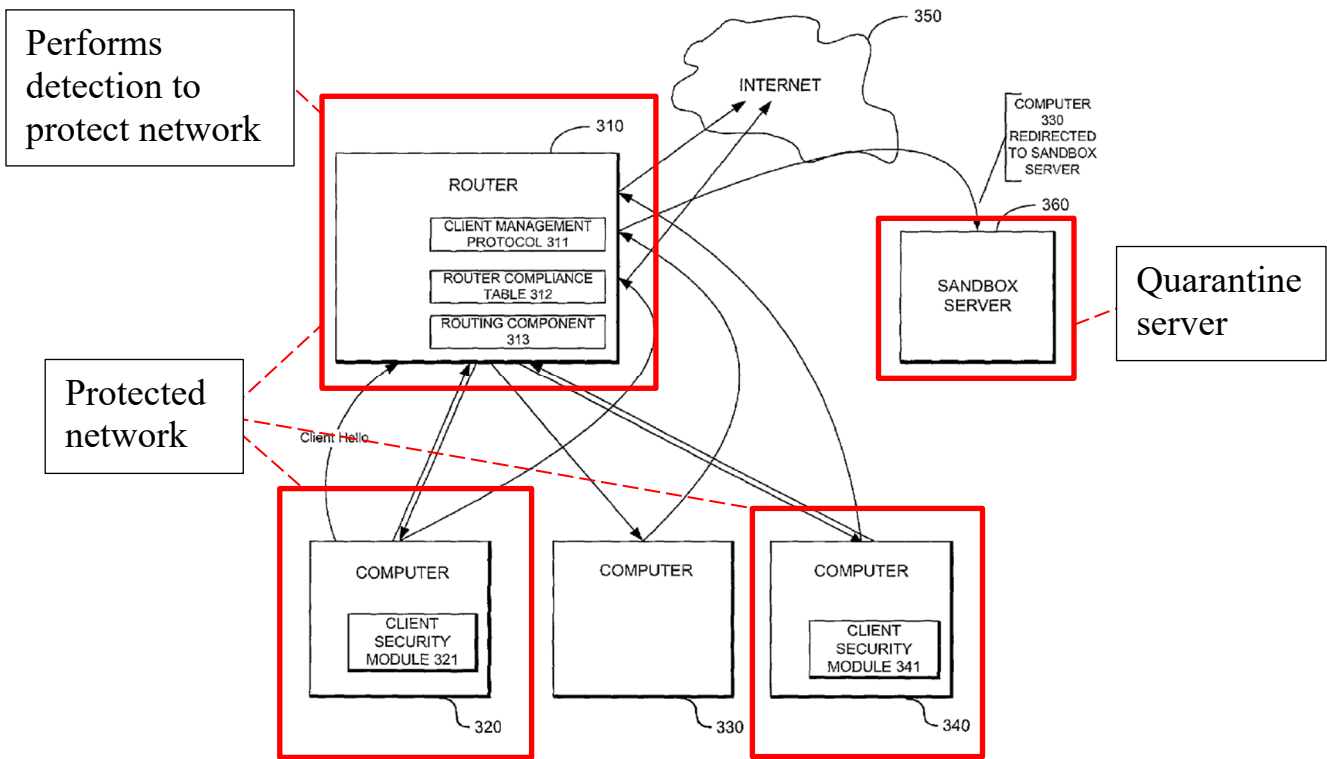
#### **1. Claim 1 (Preamble): “A method for protecting a network, comprising:”**

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

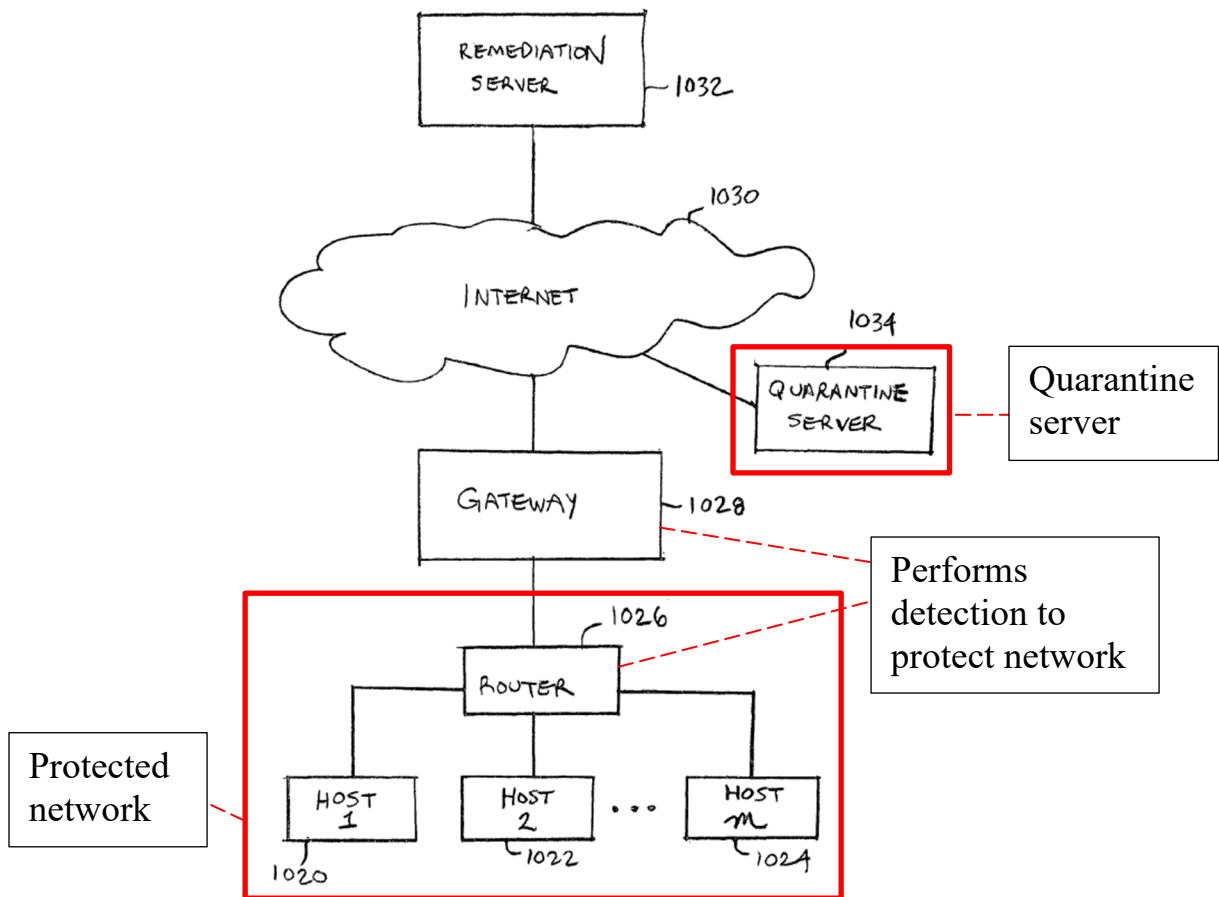
76. Freund discloses a method for protecting a network (e.g., a local area network (LAN)) from malicious code by denying connections to the network. EX1005, ¶¶[0004], [0068].

77. Freund aims to “protect the overall security of the network.” *Id.*, ¶[0019]. *See also id.*, ¶[0066]. Figure 3 of Freund is compared to Figure 10B of the ’705 Patent:

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705



**Figure 3 of Freund (Annotated)**



**Figure 10B of '705 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,”

78. Freund discloses and suggests Element [1.1].

79. 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.

80. A comparison of the above annotated Freund Figure with the annotated '705 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.

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

82. 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]. Freund's client monitoring protocol (CMP) evaluates responses from a host device to determine if the device is compliant or non-compliant. *Id.*, ¶¶[0084]-[0085], [0088]-[0089].

83. 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].

84. Freund's disclosure refers specifically to a protected network as a "private network" which can connect to the Internet. *Id.*, ¶[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,”**

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

86. 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.

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

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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]. 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].

89. 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].

90. 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.

91. 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 '705 Patent. While Freund discloses a CPU/processor as hardware for executing the TCB, Freund

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

does not expressly disclose that this CPU/processor hardware is a TCB associated with specialized “TPM” hardware. EX1005, ¶[0056].

92. 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.

93. 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.

94. 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.

95. 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].

96. Ball’s TPM and associated hardware satisfy the claimed TCB under Petitioner’s and PO’s constructions.

97. It therefore would have been obvious, predictable and beneficial to configure Freund’s TCB as a trusted platform module (TPM) based on Ball’s

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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].

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

99. 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].

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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

101. 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].

102. 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].

103. 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].

104. 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.

105. Employing a TPM in Freund's system would therefore have been obvious, predictable and beneficial for several reasons.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

106. 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.

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

108. 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.

109. 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 success.

110. 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"**

111. Freund discloses and suggests Element [1.3].

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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

113. 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,”**

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

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

116. Freund discloses determining whether the response includes a valid digitally signed attestation of cleanliness.

117. Freund’s CMP interprets the response from the device to determine whether the response is valid. *Id.*, ¶[0144].

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

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

120. 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].

121. Ball discloses the TPM transmitting a digitally signed attestation of cleanliness in the response.

122. 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).

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.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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

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

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

129. 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 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]).

130. 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

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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.”).

131. 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].

132. 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].

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

134. The ’705 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, 14:16-19.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

135. The '705 Patent discloses that “infestations”, “contagion”, and “viruses” are related concepts and anti-contagion software encompasses anti-virus software. EX1001, 11:20-22 (“Infestation herein refers to the current presence and/or execution of contagion”), 3:30-36 (“Examples of contagion include computer worms, viruses”), 3:36-45 (“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”).

136. 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 component on the first host.

138. 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].

139. 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. 8,234,705

confirmation that the computer is running a **current** version of the software”. EX1005, ¶[0078] (emphasis added).

140. 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].

141. 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 ’705 Patent describes patches in a similar manner. EX1001, 3:16-17 (“download a software patch, update, or definition”).

142. 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). *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...”).

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

143. 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,”**

144. Freund discloses and suggests Element [1.6].

145. 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].

146. Non-compliant devices in Freund are redirected to the “sandbox” quarantine server.

147. Freund’s “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.” *Id.*

148. 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].

149. 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,”**

150. Freund discloses and suggests Element [1.7].

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

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

153. Freund’s “router receives a request for connection”. *Id.* Freund discloses its “sandbox server to which non-compliant computers are re-directed when they attempt to connect”. *Id.*, ¶[0081].

154. 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].

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

155. 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.

156. Freund also discloses preventing the non-compliant host device from sending data on the network. 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]: “serving a quarantine notification page to the first host when the service request comprises a web server request, and”**

158. Freund discloses and suggests Element [1.8].

159. Freund discloses receiving a service request in a quarantine-capable network. *See* Element [1.7], *supra*.

160. 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].

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

161. Freund discloses serving a quarantine notification page to a device in response to a service request when the device is quarantined and/or deemed non-compliant. *Id.*, ¶[0149].

162. 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].

163. 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].

164. Freund’s quarantine notification page is served to the device when the service request comprises a web server request (e.g., an HTTP request).

165. 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].

166. 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.

167. When Freund determines the service request is a web server request, Freund responds by replacing the destination Internet Protocol (“IP”) address with

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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.*

168. Freund discloses serving a quarantine notification page to the device when the service request comprises a web server request.

- i. **[1.9]: “in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and”**

169. Freund discloses and suggests Element [1.9].

170. Element [1.9] was the stated basis for allowance during prosecution because the prior art considered at that time did not disclose providing, in response to a DNS query, an IP address of a quarantine server for serving a quarantine notification page to remedy an insecure condition. *See* EX1002, pp.19-21.

171. In Freund, where a service request comprises a DNS query, Freund discloses providing in response an IP address of the “sandbox” quarantine server

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

configured to serve the notification page of Figure 7 or 8. This response is provided when the DNS query is not associated with a remediation host.

172. Freund therefore provides rerouting of an insecure client device to the IP address of the sandbox server for quarantining and remediation. EX1005, Figs. 7-9, ¶¶[0049]-[0050], [0114]-[0117], [0147]-[0151].

173. Freund discloses a service request including a DNS query transmitted to a DNS server. EX1005, ¶[0150].

174. However, Freund's system prevents the host device from contacting the subject of the DNS query by providing, in response, the IP address of the "sandbox" quarantine server if the host name that is the subject of the DNS query is not associated with a remediation host. *Id.*, ¶[0149].

175. Freund replaces the destination IP address from the DNS query with the IP address of the sandbox server to redirect the request to the sandbox server. *Id. See also id.*, ¶[0150].

176. Freund's providing of the sandbox server's IP address satisfies limitation [1.9] at least because the '705 Patent acknowledges that the redirect to the quarantine server "may be accomplished in numerous ways". *See* EX1001, 15:1-12; 15:57-16:31.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

177. The Examiner's reasons for allowance focused on the claim language of serving a quarantine notification page following a DNS query not associated with remediation. EX1002, pp.17-21.

178. Freund squarely addresses this by providing, in response to a DNS query, the IP address of the sandbox quarantine server to serve the quarantine notification page and effect remediation. Freund discloses the stated reasons for allowance.

179. Freund discloses using a router to provide the IP address of the sandbox server in response to a DNS query (EX1005, ¶¶[0149]-[0150]).

180. Freund's providing of an IP address of a quarantine server in response to a DNS query involves a rerouting of the client device that transmitted the DNS query to the sandbox server via the DNS server as per exemplary embodiments of the '705 Patent specification. EX1005, ¶[0150] ("the re-routing manager proceeds to step 960 to evaluate whether or not the destination port was DNS or DHCP and the destination IP address that of the DNS/DHCP server.").

181. Non-compliant client devices are permitted to access the DNS server, otherwise "the browser would fail prior to being redirected to the sandbox server because it could not lookup the IP address of the sandbox server." *Id.*

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

182. Freund's system therefore permits a non-complaint device to access the DNS server as part of the process for providing the IP address of the sandbox server in response to a DNS query.

183. The DNS query and an HTTP request are used to access a web server and/or a website including a quarantine server.

184. The IP address of the sandbox server is replaced in an HTTP request when the IP address that was the original subject of the DNS query is not associated with a remediation host.

185. Although Freund satisfies limitation [1.9], should it be argued that the claim is somehow limited to the non-limiting exemplary embodiments disclosed in the '705 specification, Freund's combination with Lewis satisfies any asserted construction of the claim language. Lewis discloses that, for a non-compliant device accessing a DNS server as per Freund, an alternate process to that disclosed by Freund for providing the IP address of a quarantine server at a router is to provide the IP address of the quarantine server at the DNS server. Lewis discloses that "[w]henver the client performs name resolution on any address [*i.e., a DNS query*], it will receive the IP of QS [*i.e., a quarantine server*]." EX1013, 14:22-23.

186. Lewis' clients are redirected to a fix-up page [*i.e., a quarantine notification page*] on the quarantine server. *Id.*, 15:24. *See also id.*, 9:1-13. Lewis

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

thus discloses an alternate technique of DNS redirection to a quarantine server by providing the IP address of a quarantine server at a DNS server rather than at a router.

187. It would have been obvious to provide the IP address of Freund's sandbox quarantine server in response to Freund's DNS query by a DNS server as disclosed by Lewis, rather than at a router as disclosed by Freund. Such a substitution of an IP address at a DNS server rather than at a router would have been an obvious and predictable substitution for Freund's expressly disclosed providing of the sandbox server IP address. Each of Freund, Lewis, and the '705 Patent are concerned with achieving the goal of DNS redirection of a non-compliant client device to a quarantine server.

188. Freund recognizes that non-compliant client devices must be permitted to access DNS to retrieve an IP address prior to being redirected to the sandbox server. EX1005, ¶[0150].

189. Freund discloses replacing an IP address from the DNS server with the IP address of the sandbox server when the IP address is not associated with remediation. *Id.*, ¶[0149].

190. Lewis teaches that the IP address of the sandbox server in Freund could be provided at the DNS server itself, rather than at the router.

191. Substituting Lewis's DNS server to provide the IP address of the sandbox server in Freund would have been an obvious substitution of one known

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

alternative for another to obtain predictable results of redirecting the non-compliant device to the IP address of the quarantine server. Lewis teaches one example of substituting the IP address of the quarantine server at the DNS server in a manner as described in an exemplary embodiment of the '705 Patent (*see* EX1001, 15:1-5), while Freund discloses another example of replacing the IP address at a router as one of the “numerous ways” referenced by the '705 Patent (*see* EX1001, 15:1-3; 16:1-3).

192. To provide the redirect to the sandbox server, Freund’s system determines whether the service request is associated with a remediation request by filtering the request based on a destination address. EX1005, Fig. 9 (step 920). Freund’s router keeps a list of destination addresses that are used for remediation in order to filter requests that are directed to remediation. *See also*, Freund’s U.S. Provisional Application No. 60/303,653. *See* EX1012, p.27. “If a computer is not in compliance, then the computer’s access to the Internet is restricted to those activities necessary to get the computer back into compliance.

193. 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].

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

194. Freund's sandbox server is configured to serve the quarantine notification page. Freund discloses a separate remediation host that is accessed by non-compliant devices via links provided on the quarantine notification page. EX1005, Figs. 7-8, ¶¶[0114]-[0117].

195. A non-compliant device accesses the download link to a remediation host by transmitting a new HTTP request that is permitted by Freund's router as an exempt request from quarantined communication. EX1005, Fig. 9, 920.

196. Freund's Figure 4 confirms that updates are provided via separate remediation hosts at least because the router and sandbox server require checking for specific versions of anti-virus software. *See* EX1005, Fig. 4.

197. If Freund's sandbox server provided remediation updates, Freund's software and router would not require the illustrated tracking of licenses and specific anti-virus versions on the client devices.

198. Thus, Freund discloses a third-party host (e.g., TRENDMICRO) from which to download anti-virus remediation updates.

199. The anti-virus product "TRENDMICRO" illustrated in Freund is a separate product. Downloading updates for the TRENDMICRO antivirus product would involve contacting a TRENDMICRO host.

200. Freund's client devices would have accessed the "download" link using the "Update Now!" or "Download Now!" buttons on the notification page.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

201. Freund's sandbox server would have retrieved the anti-virus update from a data file, database, or server (e.g., via TCP). *See* EX1005, ¶¶[0035]-[0036].

202. The '705 Patent discloses links provided through the quarantine notification page to the same extent as Freund's sandbox server. *See* EX1001, 16:2-9 ("provides links to remediation sites appropriate to the quarantine"; "The links on the quarantine notification page may be examples of HTTP addresses that are for use in remediation.").

203. To the extent this limitation is interpreted under §112(f)/¶6, Freund discloses corresponding structure at least to the same extent as the '705 Patent. Freund discloses a quarantine server and remediation host under any construction. *See* EX1014

204. Element [1.9] served as basis for allowance during prosecution. *See* EX1002, pp.19-21.

205. The Examiner's reasons for allowance explained "[t]he closest prior art, Liang (US 7287278 B2) and Yan et al. (US 2005/0033987 A1) disclose detecting abnormal events on host, and redirecting to quarantine **serve[r]** to get remediated; however, they fail to anticipate or render serving both the specific quarantine notification page with the DNS redirection when in combination with the remaining claim limitations."

206. Freund, alone and/or in combination with Lewis, discloses this exact function under any construction.

**j. [1.10]: “permitting the first host to communicate with the remediation host.”**

207. Freund in view of Ball discloses and suggests Element [1.10].

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

209. 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.” *Id.*, ¶[0071].

210. Freund allows a non-compliant computer to download appropriate corrective software from a remediation host or through the sandbox server itself acting as a remediation host. *See also id.*, ¶¶[0078], [0095].

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

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

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

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

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

216. 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.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

217. 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].

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

219. 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 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”).

220. 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].

221. 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. *Id.*, ¶¶[0147]-[0150].

222. 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.

223. 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 an insecure condition includes determining that the first host should be quarantined until an update to an operating system has been installed.”**

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

225. 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].

226. Freund recognizes network security vulnerabilities associated with devices running “older software”. *See id.*, ¶¶[0088]-[0089].

227. 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”).

228. 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 detecting an insecure condition includes configuring an operating system to quarantine the first host upon initial startup after installation of the operating system.”**

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

230. Freund discloses detecting an insecure condition including configuring an operating system to quarantine the first host upon initial startup after installation of the operating system. Freund specifically warns against operating system “security holes”. EX1005, ¶¶[0015], [0019].

231. Freund contemplates that operating systems can result in security vulnerabilities or security non-compliance such that the operating system must be up-to-date to avoid such vulnerabilities. *See Claim 3, supra.*

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

232. Freund expressly recognizes that a “user may inadvertently disable previously installed security software in the process of upgrading his or her operating system.” EX1005, ¶[0019].

233. Freund recognizes that security software can be disabled when installing and/or upgrading an operating system.

234. A POSITA would have been motivated to use Freund’s security compliance system to configure an operating system on the client-side device to quarantine a device upon initial startup installation to solve this problem recognized by Freund and to check for disabled or altered security software upon initial startup to ensure a device remains compliant after installation of a new operating system. *See also*, EX1006, ¶[0031].

235. Freund also discloses quarantine of a device upon initial startup. *See* EX1005, ¶[0125].

236. Freund recognizes out-of-date operating systems posing security threats, problems associated with disabling security software upon installation of an operating system, and Freund contemplates quarantine upon initial startup of a device.

237. It would have been obvious to a POSITA that Freund discloses configuring an operating system to quarantine a device upon initial startup to ensure

the device's operating system is up-to-date and in compliance with Freund's security policies after installation.

238. A POSITA would have had a reasonable expectation of success given that Freund informs a POSITA that installation and/or upgrade of operating systems can pose a threat to a device's security compliance, and Freund is directed to ensuring networked devices remain in compliance with established security policies.

*See id.*, ¶[0071].

5. **Claim 5: “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.”**

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

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

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

242. 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

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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].

243. 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 Figure 4, available from TRENDMICRO referenced in EX1005, ¶[0132]. *See*, EX1005, ¶[0147]-[0151]; [0104]-[0105].

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

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

246. 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].

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

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

248. 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].

249. 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].

250. Freund's system "enables the user to take the steps necessary to bring his or her computer back into compliance." EX1005, ¶[0095].

251. 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. *See 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"). The '705 Patent works this same way. *See, e.g.,* EX1001, 16:2-7 ("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.”).

252. 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].

253. For example, when the 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.

254. 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].

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

255. 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.

256. Freund discloses determining whether a destination address (e.g., to a remediation host) is exempt. EX1005, Fig. 7, ¶¶[0042], [0071], [0114].

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

258. The '705 Patent describes the same process as disclosed by Freund. *See* EX1001, Fig. 14, 14:50-15:12.

259. The '705 Patent describes testing outbound traffic to determine whether the traffic is associated with remediation such as “contact with a verified remediation site”. *Id.*, 14:53-59. If the traffic is associated with a remediation request, then the traffic is forwarded to the destination. *Id.*, 14:59-61.

260. Otherwise, the traffic is rerouted to the quarantine server. *Id.*, 14:59-15:5. Freund discloses detecting an outbound communication from the first host; and forwarding the outbound communication if it is addressed to the remediation host.

6. **Claim 6: “A method as recited in claim 1, wherein preventing the first host from sending data to the one or more other hosts includes: detecting an outbound communication from the first host; and redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to a remediation host.”**

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

262. Freund discloses detecting an outbound communication from the device. *See* Claim 5, *supra*. Freund discloses redirecting the outbound communication to a sandbox server (i.e., quarantine server) if it comprises a request for an approved service and is not addressed to a remediation server.

263. Freund discloses that outbound communication from 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.” EX1005, ¶[0042].

264. Freund detects the outbound communication and determines whether the destination address for the communication is exempt (e.g., for remediation). EX1005, Fig. 9. Any other outbound communications (i.e., sending data to the one or more other hosts of Freund’s network) are redirected to the sandbox server at least because the communication are not detected as exempt.

265. “The re-routing manager operates to redirect the local computer to the sandbox server instead of the address originally requested.” *Id.*, ¶[0089]. *See also id.*, ¶¶[0071], [0078], [0149].

266. Freund discloses detecting an outbound communication from the device and redirecting the outbound communication to a quarantine server if it comprises a request for an approved service and is not addressed to remediation.

**7. Claim 7: “A method as recited in claim 1, wherein quarantining the first host further includes preventing the first host from receiving via the protected network data not related to remediation of the insecure condition.”**

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

268. Freund discloses that quarantining the device at the sandbox server includes preventing the device from receiving via the network data not related to remediation.

269. 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*.

270. 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.

**8. Claim 8: “A method as recited in claim 1, performed at an Internet service provider.”**

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

272. 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].

273. 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. *Id.*, Fig. 3.

274. The ’705 Patent contemplates an “ISP web server” as the “special quarantine server” referenced in claim 1. EX1001,14:65-15:1; Fig. 14.

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

275. 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.

276. 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. 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.” *Id.*, 1:25-30. EX1005, ¶[0004].

277. 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.

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

279. 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 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,

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

safe, and managed access to the Internet and protect[] the users from many security threats.” *Id.*, 21:53-55. *See id.*, 21:47-22:41.

280. 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].

281. 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.

282. 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. *Id.*, ¶[0039].

283. 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.

284. 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.

285. 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.

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

**9. Claim 9: “A method as recited in claim 1, wherein the software component on the first host is an operating system.”**

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

288. 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.

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

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

291. 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. *Id.*, ¶¶[0103], [0110].

292. 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 id.*, ¶¶[0068], [0071]-[0072], [0078], [0085]-[0089]; *see also*, EX1006, ¶[0031].

**10. Claim 10: “A method as recited in claim 1, wherein determining that the response does not include a valid digitally signed attestation of cleanliness includes determining that the software component on the first host is not sufficiently updated.”**

293. Freund in view of Ball discloses and suggests claim 10.

294. 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.

295. Kappes demonstrates that those skilled in the art would have understood Freund in view of Ball to disclose storing a content authentication token

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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.

296. 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.

297. 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.

298. 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. *Id.*

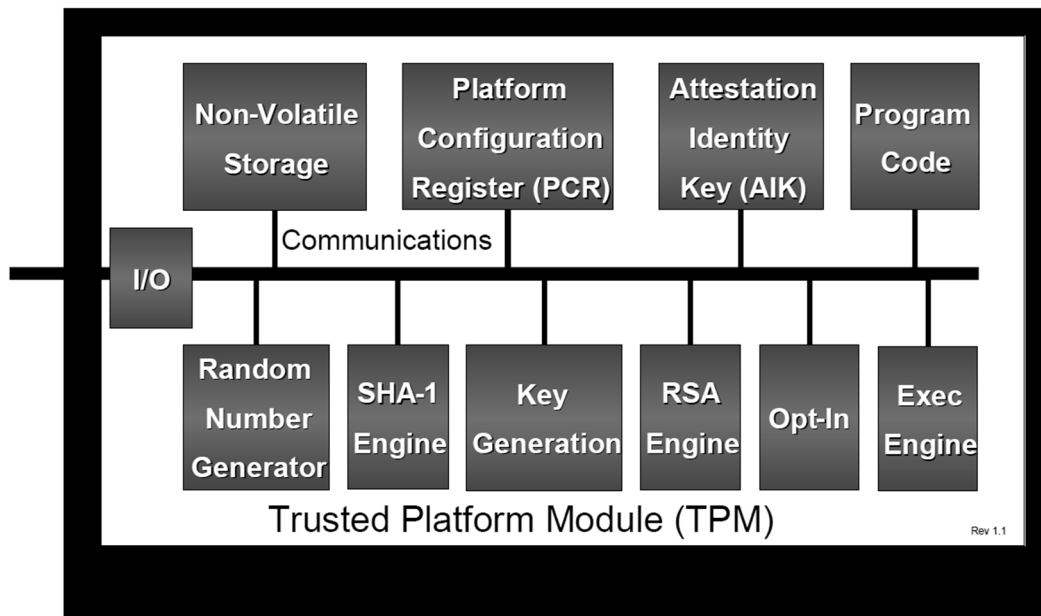


Figure 4:g – TPM Component Architecture

See also, EX1008, pp.19-26.

299. 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].

**11. Claim 11: “A method as recited in claim 1, wherein determining that the software component on the first host is not sufficiently updated includes determining that a patch level associated with the software component on the first host is not sufficiently recent.”**

300. Freund in view of Ball discloses and suggests claim 11.

301. Freund discloses determining that a software component on the device (e.g., anti-virus software) is not sufficiently updated. See Claim 10, *supra*. Freund

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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). 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...”).

302. 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*.

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

304. 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.

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

**12. Claim 12 (Preamble): “A system for protecting a network, comprising:”**

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

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

308. 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. *Id.*, ¶[0068].

309. Freund’s Fig. 3 discloses a system including a router for monitoring client requests within the private network. *Id.*, ¶¶[0073]-[0074], Fig.3.

310. 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.*

311. 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. *Id.*, ¶¶[0068]-[0072].

**a. [12.1]: “a processor configured to:”**

312. Freund discloses and suggests Element [12.1].

313. 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].

314. Freund discloses a system including a processor.

**b. [12.2]: “detect an insecure condition on a first host that has connected or is attempting to connect to a protected network,”**

315. Freund discloses and suggests Element [12.2]. *See* Element [1.1], *supra*.

**c. [12.3]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,”**

316. Freund in view of Ball discloses and suggests Element [12.3]. *See* Element [1.2], *supra*.

**d. [12.4]: “receiving a response, and”**

317. Freund discloses and suggests Element [12.4]. *See* Element [1.3], *supra*.

- e. **[12.5]: “determining whether the response includes a valid digitally signed attestation of cleanliness,”**

318. Freund in view of Ball discloses and suggests Element [12.5]. *See* Element [1.4], *supra*.

- f. **[12.6]: “wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host; ”**

319. Freund discloses and suggests Element [12.6]. *See* Element [1.5], *supra*.

- g. **[12.7]: “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,”**

320. Freund discloses and suggests Element [12.7]. *See* Element [1.6], *supra*.

- h. **[12.8]: “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,”**

321. Freund discloses and suggests Element [12.8]. *See* Element [1.7], *supra*.

- i. **[12.9]: “serving a quarantine notification page to the first host when the service request comprises a web server request, and”**

322. Freund discloses and suggests Element [12.9]. *See* Element [1.8], *supra*.

- j. **[12.10]: “in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and”**

323. Freund discloses and suggests Element [12.10]. *See* Element [1.9], *supra*.

- k. **[12.11]: “permit the first host to communicate with the remediation host; and”**

324. Freund discloses and suggests Element [12.11]. *See* Element [1.10], *supra*.

- l. **[12.12]: “a memory coupled to the processor and configured to provide instructions to the processor.”**

325. Freund discloses and suggests Element [12.12].

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

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

327. Freund in view of Ball discloses and suggests claim 13. *See* claim 2, *supra*.

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

328. Freund in view of Ball discloses and suggests claim 14. *See* claim 4, *supra*.

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

329. Freund in view of Ball discloses and suggests claim 15. *See* claim 7, *supra*.

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

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

- 17. Claim 17: “A system as recited in claim 12, wherein determining that the response does not include a valid digitally signed attestation of cleanliness includes determining that the software component on the first host is not sufficiently updated.”**

331. Freund in view of Ball discloses and suggests claim 17. *See* claim 10, *supra*.

- 18. Claim 18: “A system as recited in claim 17, wherein determining that the software component on the first host is not sufficiently updated includes determining that a patch level associated with the software component on the first host is not sufficiently recent.”**

332. Freund in view of Ball discloses and suggests claim 18. *See* claim 11, *supra*.

- 19. Claim 19 (Preamble): “A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising computer instructions for:”**

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

334. 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.

335. 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].

Declaration of Markus Jakobsson in Support of  
Petition for *Inter Partes* Review of U.S. Patent No. 8,234,705

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

- a. **[19.1]: “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,”**

337. Freund discloses and suggests Element [19.1]. *See* Element [1.1], *supra*.

- b. **[19.2]: “wherein detecting the insecure condition includes contacting a trusted computing base associated with a trusted platform module within the first host,”**

338. Freund in view of Ball discloses and suggests Element [19.2]. *See* Element [1.2], *supra*.

- c. **[19.3] receiving a response, and**

339. Freund in view of Ball discloses and suggests Element [19.3]. *See* Element [1.3], *supra*.

- d. **[19.4] determining whether the response includes a valid digitally signed attestation of cleanliness,**

340. Freund in view of Ball discloses and suggests Element [19.4]. *See* Element [1.4], *supra*.

- e. **[19.5] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;**

341. Freund discloses and suggests Element [19.5]. *See* Element [1.5],  
*supra*.

- f. **[19.6] 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,**

342. Freund discloses and suggests Element [19.6]. *See* Element [1.6],  
*supra*.

- g. **[19.7] 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,**

343. Freund discloses and suggests Element [19.7]. *See* Element [1.7],  
*supra*.

- h. **[19.8] serving a quarantine notification page to the first host when the service request comprises a web server request, and**

344. Freund discloses and suggests Element [19.8]. *See* Element [1.8],  
*supra*.

- i. **[19.9] in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and**

345. Freund discloses and suggests Element [19.9]. *See* Element [1.9], *supra*.

- j. **[19.10] permitting the first host to communicate with the remediation host.**

346. Freund discloses and suggests Element [19.10]. *See* Element [1.10], *supra*.

## **XII. SECONDARY CONSIDERATIONS**

347. 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.

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

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

### **XIII. CONCLUSION**

350. For the reasons set forth above, it is my opinion that all elements of the Challenged Claims of the '705 Patent are disclosed or suggested by the prior art. In my opinion, the Challenged Claims of the '705 Patent are anticipated by and/or would have been obvious over the prior art.

351. 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.

352. 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. 8,234,705

**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. 8,234,705

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. Dhama & Bal (Sandeep Singh Dhama 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. 8,234,705

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. 8,234,705

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. 8,234,705

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. 8,234,705

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)	