UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.
Petitioner

v.

TAASERA LICENSING LLC,
Patent Owner

Case IPR2024-00038
Patent No. 8,955,038

DECLARATION OF DR. MARKUS JAKOBSSON

CROWDSTRIKE 1003

TABLE OF CONTENTS

I. Introduction 5

II. Background and Qualifications 6

III. Level of Ordinary Skill in the Art 15

IV. Materials Considered and Relied Upon 15

V. Legal Standards 16

VI. Overview of the ’038 Patent 24

A. Brief Description of the ’038 Patent 24

B. File History of the ’038 Patent 27

C. Interpretation of the ’038 Patent Claims at Issue 29

VII. Overview of the Cited References 31

A. Couillard (EX1004) 31

B. Freund (EX1005) 33

C. An Obvious Combination of Couillard and Freund 37

VIII. Overview of Unpatentability Grounds 39

IX. Ground 1: Couillard and Freund REnder Obvious Claims 1, 23, 25, 31, 33 40

A. Claim 1 40

1. [1pre] A method for controlling the operation of an endpoint, comprising: 40

2. [1a] providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; 42

3. [1b] maintaining the plurality of policies in a data store on the computing system; 46

4. [1c] identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor; 48

5. [1d] configuring one or more software agents on the endpoint to monitor the plurality of operating conditions; 52

6. [1e] receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents; 57

7. [1f] determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and 58

8. 1[g] initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint 61

B. Claim 23 66

1. 23[pre] A system for controlling the operation of an endpoint, comprising: 66

1. 23[a] a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies; 67

2. 23[b] a data store, at the computing system, that contains the plurality of policies; 67

3. 23[c] one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and 68

4. 23[d] one or more hardware processors at the computing system configured to: 68

5. 23[d.i] receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents, ...69

6. 23[d.ii] determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and 69

7. 23[d.iii] initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint.....69

C. Claim 25 69

D. Claim 31 72

E. Claim 33 73

X. Additional Remarks 77

I. INTRODUCTION

1. My name is Dr. Markus Jakobsson, and I have been retained by counsel for Petitioner CrowdStrike, Inc. ("CrowdStrike" or "Petitioner") as an expert witness to provide assistance regarding U.S. Patent No. 8,955,038 ("the '038 Patent"). Specifically, I have been asked to consider the patentability of claims 1, 23, 25, 31, 33 of the '038 Patent ("Challenged Claims") in view of prior art, anticipation and obviousness considerations, and the understanding of a person of ordinary skill in the art at the time of the invention ("POSITA") as it relates to the '038 Patent.

2. I am being compensated for my time at my standard consulting rate. I am also being reimbursed for expenses that I incur during the course of this work. My compensation is not contingent upon the results of my study, the substance of my opinions, or the outcome of any proceeding involving the Challenged Claims. I have no financial interest in the outcome of this matter or on the pending litigation between Petitioner and Patent Owner.

3. My analysis here is based on my years of education, research and experience, as well as my investigation and study of relevant materials, including those cited herein.

4. I may rely upon these materials, my knowledge and experience, and/or additional materials to rebut arguments raised by the Patent Owner. Further, I may

also consider additional documents and information in forming any necessary opinions, including documents that may not yet have been provided to me.

5. My analysis of the materials produced in this proceeding is ongoing and I will continue to review any new material as it is provided. This declaration represents only those opinions I have formed to date. I reserve the right to revise, supplement, and/or amend my opinions stated herein based on new information and on my continuing analysis of the materials already provided.

II. BACKGROUND AND QUALIFICATIONS

6. I have summarized in this section my educational background, career history, and other qualifications relevant to this matter. I have also included a current version of my curriculum vitae, which is attached as Appendix A.

7. I received a Master of Science degree in Computer Engineering from the Lund Institute of Technology in Sweden in 1993, a Master of Science degree in Computer Science from the University of California at San Diego in 1994, and a Ph.D. in Computer Science from the University of California at San Diego in 1997, specializing in Cryptography. During and after my Ph.D. studies, I was also a researcher at the San Diego Supercomputer Center and General Atomics, where I did research on authentication, privacy, and security. Much of my work was on distributed protocols to enable security and privacy, and my Ph.D. thesis described a distributed electronic payment system. Whereas the term “cloud computing” had

not been popularized at this point, many of the principles I studied later became critical aspects of cloud computing and virtualization.

8. Since earning my doctorate degree over twenty-six years ago, I have been an employee, entrepreneur, and consultant in the computer systems, security, and cloud computing industry. I have worked extensively with technologies related to computer security, mobile security, malware detection, quantitative and qualitative fraud analysis, and disruptive security. I have worked as an engineer or technical advisor at a number of leading companies in the computer industry, including PayPal, Qualcomm, Bell Labs, and LifeLock. I have also taught and performed research at several prestigious universities, including New York University (NYU) and Indiana University (IU). Further, I have been materially involved in designing, developing, testing, and assessing technologies for computer and network security, digital rights management, trust establishment, randomness, cryptography, socio-technical fraud, malware detection, detection of malicious emails, user interfaces, authentication, and fraud detection for over twenty years.

9. From 1997 to 2001, I was a Member of Technical Staff at Bell Labs, where I did research on authentication, privacy, multi-party computation, contract exchange, digital commerce including crypto payments, and fraud detection and prevention. Example publications of mine from this time period include "Secure distributed computation in cryptographic applications" (U.S. Patent No. 6,950,937,

2001 priority date) and "Secure server-aided signature generation" (International Workshop on Public Key Cryptography PKC 2001: Public Key Cryptography 383-401), both of which relate to virtualization. At the end of my tenure at Bell Labs, I had started to research identity theft, years before the banking industry became aware of the existence of phishing attacks.

10. From 2001 to 2004, I was a Principal Research Scientist at RSA Labs, where I worked on predicting future fraud scenarios in commerce and authentication and developed solutions to those problems. Much of my work related to the development of anti-fraud mechanisms, addressing authentication abuse and identity theft. During that time, I predicted the rise of what later became known as phishing. I also laid the groundwork for what I termed "proof of work," and described how this could be applied in the context of distributed computations such as mining of crypto payments; this work later came to influence the development of BitCoin. I was also an Adjunct Associate Professor in the Computer Science department at New York University from 2002 to 2004, where I taught cryptographic protocols, with an emphasis on authentication.

11. From 2004 to 2016, I held a faculty position at Indiana University at Bloomington, first as an Associate Professor of Computer Science, Associate Professor of Informatics, Associate Professor of Cognitive Science, and Associate Director of the Center for Applied Cybersecurity Research (CACR) from 2004 to

2008; and then as an Adjunct Associate Professor from 2008 to 2016. I was the most senior security researcher at Indiana University, where I built a research group focused on online fraud and countermeasures, resulting in over 50 publications and two books. One of these books, "Crimeware: Understanding New Attacks and Defenses" (Wiley, 2008), described man-in-the-middle attacks, online abuse in general, and countermeasures to attacks and abuses of these types.

12. While a professor at Indiana University, I was also employed by Xerox PARC, PayPal, and Qualcomm to provide thought leadership to their security groups. I was a Principal Scientist at Xerox PARC from 2008 to 2010, a Director and Principal Scientist of Consumer Security at PayPal from 2010 to 2013, a Senior Director at Qualcomm from 2013 to 2015, Chief Scientist at Agari from 2016 to 2018, and Chief of Security and Data Analytics at Amber Solutions from 2018 to 2020.

13. Agari is a cybersecurity company that develops and commercializes technology to protect enterprises, their partners and customers from advanced email phishing attacks. At Agari, my research studied and addressed trends in online fraud, especially as related to email, including problems such as Business Email Compromise, Ransomware, and other abuses based on social engineering and identity deception. My work primarily involved identifying trends in fraud and computing before they affected the market, and developing and testing

countermeasures, including technological countermeasures, user interaction and education. Example publications include "Detecting computer security risk based on previously observed communications" (U.S. Patent No. 10,715,543 B2, 2016 priority date) and "Using message context to evaluate security of requested data" (U.S. Patent No. 10,805,314 B2, 2017 priority date).

14. In 2020, after leaving Agari, I was the Chief of Security and Data Analytics at Amber Solutions, an IoT startup in the San Francisco Bay Area. Amber Solutions is a cybersecurity company that develops home and office automation technologies. At Amber Solutions, my research addressed privacy, user interfaces and authentication techniques in the context of ubiquitous and wearable computing. My work often related to authentication and cloud computing, as exemplified in "Configuration and management of smart nodes with limited user interfaces" (U.S. Patent No. 10,887,447).

15. I left Amber Solutions to take the role of Chief Scientist at ByteDance in 2019, where I guided the security research both for ByteDance and TikTok until I left to co-found Artema Labs, where I am the Chief Scientist. My work at ByteDance involved identifying new threats, developing new solutions, and guiding research in areas relating to cryptography and Internet security.

16. I am also the Chief Technology Officer at ZapFraud, a cybersecurity company that develops techniques to detect deceptive emails, such as Business

Email Compromise ("BEC") emails. At ZapFraud, my research studies and addresses computer abuse, including social engineering, malware and privacy intrusions, and has also involved studying security aspects related to cloud computing. My work primarily involves identifying risks, developing protocols and user experiences, and evaluating the security of proposed approaches. Using virtual machines is an important tool for security researchers, as it allows them to study the impact of a given executable, website, or other context on a computational environment. My students, direct reports and I have often relied on this approach in the context of interacting with online criminals, their websites and emails they send, as virtual machines enable us to identify their motives and report them to the authorities without making us easy for them to track or identify. Doing this is important to identify new and trending attacks.

17. I also work as an independent security researcher and consultant in the fields of computer/mobile security, fraud detection/prevention, digital rights management, malware, phishing, crimeware, mobile malware, and cryptographic protocols. In addition, I am a visiting research fellow of the Anti-Phishing Working Group, an international consortium focused on unifying the global response to cybercrime in the public and private sectors.

18. I have also served on the advisory board of several companies, including Metaforic, a company that developed technology for watermarking

software and provided security software with a built-in framework that resists attacks from malware, bots, hackers and other attempts. Metaforic was acquired by Inside Secure in 2014.

19. I have founded or co-founded several successful computer security companies. In 2005 I co-founded RavenWhite Security, a provider of authentication solutions, and I am currently its Chief Technical Officer. RavenWhite owns intellectual property related to authentication, such as "Performing authentication" (U.S. Patent No. 10,079,823 2007 priority date). In 2007 I co-founded Extricatus, one of the first companies to address consumer security education. In 2009 I founded FatSkunk, a provider of mobile malware detection software; I served as Chief Technical Officer of FatSkunk from 2009 to 2013, when FatSkunk was acquired by Qualcomm and I became a Qualcomm employee. FatSkunk developed anti-virus technology. In 2013 I founded ZapFraud—the same company described above, where I currently serve as Chief Technical Officer. In 2014 I co-founded RightQuestion, a security consulting company.

20. I have additionally served as a member of the fraud advisory board at LifeLock (an identity theft protection company); a member of the technical advisory board at CellFony (a mobile security company); a member of the technical advisory board at PopGiro (a user reputation company); a member of the technical advisory board at MobiSocial dba Omlet (a social networking company); and a member of

the technical advisory board at Stealth Security (an anti-fraud company). I have provided anti-fraud consulting to KommuneData (a Danish government entity), J.P. Morgan Chase, PayPal, Boku, and Western Union.

21. I have authored seven books and over 100 peer-reviewed publications, and have been a named inventor on over 200 patents and patent applications. A large number of these relate to Internet security, authentication, malware, spoofing and related topics.

22. Examples of textbooks I have authored or co-authored on the topic of Internet security include:

- "Crimeware: Understanding New Attacks and Defenses" (Symantec Press, 2008)
- "Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft" (Wiley, 2006);
- "The Death of the Internet" (Wiley, 2012);
- "Understanding Social Engineering Based Scams" (Springer 2016); and
- "Towards Trustworthy Elections: New Directions in Electronic Voting" (Springer, 2010)

23. I have authored numerous publications regarding Internet security, including Internet security as it pertains to web browsers. Relevant examples include:

- "Web Camouflage: Protecting Your Clients from Browser-Sniffing Attacks," 5 IEEE Security & Privacy (Nov. 2007)
- "Invasive Browser Sniffing and Countermeasures," Conference: 15th International Conference on World Wide Web (May 2006)
- "Remote Harm-Diagnostics", (PDF) Privacy-preserving history mining for web browsers (researchgate.net)
- "Privacy-Preserving History Mining for Web Browsers", (PDF) Privacy preserving history mining for web browsers (researchgate.net)
- "Server-Side Detection of Malware Infection", NSPW Proceedings on New Security Paradigms Workshop (2009), Server-side detection of malware infection | Proceedings of the 2009 workshop on New Security Paradigms Workshop (acm.org)

24. Related patent publications include U.S. Patent Nos. 10,498,735, 9,203,835, 8,578,174. These patents were assigned to PayPal, Inc. and Palo Alto Research Center Incorporated arising out of my employment.

25. In sum, I have extensive experience both as a developer and a researcher relating to system monitoring, software security, attack detection, and network security.

III. LEVEL OF ORDINARY SKILL IN THE ART

26. In my opinion, a person of ordinary skill in the art ("POSITA") relating to, and at the time of, the '038 Patent's Critical Date (i.e., December 21, 2005) would have possessed a bachelor's degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and would have had a working knowledge of endpoint monitoring systems and software security analysis. Additional education in a relevant field, or relevant industry experience may compensate for a deficit in one of the other aspects of the requirements stated above.

27. Based on my knowledge, skill, and experience, I have a good understanding of the capabilities of the POSITA. Indeed, I have taught, participated in organizations with, hired, and worked closely with many such persons over the course of my career. For example, from my industry experience, I am familiar with what an engineer would have known and found predictable in the art. From teaching and supervising post-graduate students, I also have an understanding of the knowledge that a person with this academic experience possesses. Furthermore, I possess those capabilities myself.

IV. MATERIALS CONSIDERED AND RELIED UPON

28. In reaching the conclusions described in this declaration, I have relied on the documents and materials cited herein as well as those identified in this declaration, including the '038 Patent, the prosecution history of the '038 Patent, and

prior art references cited herein. These materials comprise patents, related documents, and printed publications. Each of these materials is a type of document that experts in my field would have reasonably relied upon when forming their opinions.

29. I have also relied on my education, training, research, knowledge, and personal and professional experience in the relevant technologies and systems that were already in use prior to and within the timeframe of the earliest asserted priority date of the claimed subject matter in the ’038 Patent, which I have been informed by counsel is December 21, 2005.

- EX1001: U.S. Patent No. 8,955,038 (“the ’038 Patent)
- EX1002: Excerpts from the Prosecution History of the ’038 Patent (“the Prosecution History”)
- EX1004: U.S. Patent Appl. Pub. No. 2006/0203815 to Alain Couillard (“Couillard”)
- EX1005: U.S. Patent No. 5,987,611 to Gregor Freund *et al.* (“Freund”)
- EX1006: U.S. Patent Appl. Pub. No. 2004/0103220 to Bill Bostick *et al.*
- EX1007: U.S. Patent No. 7,415,100 to Robert S. Cooper *et al.*
- EX1008: U.S. Patent No. 9,298,474 to Frederic Bauchot *et al.*

V. LEGAL STANDARDS

30. I am a technical expert and do not offer any legal opinions. However, counsel has informed me as to certain legal principles regarding patentability and

related matters under United States patent law, which I have applied in performing my analysis and arriving at my technical opinions in this matter.

31. I have been informed that claim terms are to be given the meaning they would have to a person having ordinary skill in the art at the time of the invention, taking into consideration the patent, its file history, and, secondarily, any applicable extrinsic evidence (e.g., dictionary definitions).

32. I have also been informed that the implicit or inherent disclosures of a prior art reference may anticipate the claimed invention. Specifically, if a person having ordinary skill in the art at the time of the invention would have known that the claimed subject matter is necessarily present in a prior art reference, then the prior art reference may "anticipate" the claim. Therefore, a claim is "anticipated" by the prior art if each and every limitation of the claim is found, either expressly or inherently, in a single item of prior art.

33. I have also been informed that a person cannot obtain a patent on an invention if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art. I have been informed that a conclusion of obviousness may be founded upon more than a single item of prior art. I have been further informed that obviousness is determined by evaluating the following factors: (1) the scope and content of the prior art, (2) the differences

between the prior art and the claim at issue, (3) the level of ordinary skill in the pertinent art, and (4) secondary considerations of non-obviousness. In addition, the obviousness inquiry should not be done in hindsight. Instead, the obviousness inquiry should be done through the eyes of a person having ordinary skill in the relevant art at the time the patent was filed.

34. In considering whether certain prior art renders a particular patent claim obvious, counsel has informed me that I can consider the scope and content of the prior art, including the fact that one of skill in the art would regularly look to the disclosures in patents, trade publications, journal articles, industry standards, product literature and documentation, texts describing competitive technologies, requests for comment published by standard setting organizations, and materials from industry conferences, as examples. I have been informed that for a prior art reference to be proper for use in an obviousness analysis, the reference must be "analogous art" to the claimed invention. I have been informed that a reference is analogous art to the claimed invention if: (1) the reference is from the same field of endeavor as the claimed invention (even if it addresses a different problem); or (2) the reference is reasonably pertinent to the problem faced by the inventor (even if it is not in the same field of endeavor as the claimed invention). In order for a reference to be "reasonably pertinent" to the problem, it must logically have commended itself to an inventor's attention in considering his problem. In determining whether a

reference is reasonably pertinent, one should consider the problem faced by the inventor, as reflected either explicitly or implicitly, in the specification. I believe that all of the references that my opinions in this IPR are based upon are well within the range of references a person having ordinary skill in the art would consult to address the type of problems described in the Challenged Claims.

35. I have been informed that, in order to establish that a claimed invention was obvious based on a combination of prior art elements, a clear articulation of the reason(s) why a claimed invention would have been obvious must be provided. Specifically, I am informed that a combination of multiple items of prior art renders a patent claim obvious when there was an apparent reason for one of ordinary skill in the art, at the time of the invention, to combine the prior art, which can include, but is not limited to, any of the following rationales: (A) combining prior art methods according to known methods to yield predictable results; (B) substituting one known element for another to obtain predictable results; (C) using a known technique to improve a similar device in the same way; (D) applying a known technique to a known device ready for improvement to yield predictable results; (E) trying a finite number of identified, predictable potential solutions, with a reasonable expectation of success; (F) identifying that known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary

skill in the art; or (G) identifying an explicit teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine the prior art references to arrive at the claimed invention.

36. I am informed that the existence of an explicit teaching, suggestion, or motivation to combine known elements of the prior art is a sufficient, but not a necessary, condition to a finding of obviousness. This so-called "teaching suggestion-motivation" test is not the exclusive test and is not to be applied rigidly in an obviousness analysis. In determining whether the subject matter of a patent claim is obvious, neither the particular motivation nor the avowed purpose of the patentee controls. Instead, the important consideration is the objective reach of the claim. In other words, if the claim extends to what is obvious, then the claim is invalid. I am further informed that the obviousness analysis often necessitates consideration of the interrelated teachings of multiple patents, the effects of demands known to the technological community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art. All of these issues may be considered to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent.

37. I also am informed that in conducting an obviousness analysis, a precise teaching directed to the specific subject matter of the challenged claim need not be sought out because it is appropriate to take account of the inferences and creative

steps that a person of ordinary skill in the art would employ. The prior art considered can be directed to any need or problem known in the field of endeavor at the time of invention and can provide a reason for combining the elements of the prior art in the manner claimed. In other words, the prior art need not be directed towards solving the same specific problem as the problem addressed by the patent. Further, the individual prior art references themselves need not all be directed towards solving the same problem. I am informed that common sense is important and should be considered. Common sense teaches that familiar items may have obvious uses beyond their primary purposes.

38. I also am informed that the fact that a particular combination of prior art elements was "obvious to try" may indicate that the combination was obvious even if no one attempted the combination. If the combination was obvious to try (regardless of whether it was actually tried) or leads to anticipated success, then it is likely the result of ordinary skill and common sense rather than innovation. I am further informed that in many fields it may be that there is little discussion of obvious techniques or combinations, and it often may be the case that market demand, rather than scientific literature or knowledge, will drive the design of an invention. I am informed that an invention that is a combination of prior art must do more than yield predictable results to be non-obvious.

39. I am informed that for a patent claim to be obvious, the claim must be obvious to a person of ordinary skill in the art at the time of the invention. I am informed that the factors to consider in determining the level of ordinary skill in the art include (1) the educational level and experience of people working in the field at the time the invention was made, (2) the types of problems faced in the art and the solutions found to those problems, and (3) the sophistication of the technology in the field.

40. I am informed that it is improper to combine references where the references teach away from their combination. I am informed that a reference may be said to teach away when a person of ordinary skill in the relevant art, upon reading the reference, would be discouraged from following the path set out in the reference, or would be led in a direction divergent from the path that was taken by the patent applicant. In general, a reference will teach away if it suggests that the line of development flowing from the reference's disclosure is unlikely to be productive of the result sought by the patentee. I am informed that a reference teaches away, for example, if (1) the combination would produce a seemingly inoperative device, or (2) the references leave the impression that the product would not have the property sought by the patentee. I also am informed, however, that a reference does not teach away if it merely expresses a general preference for an alternative invention but does

not criticize, discredit, or otherwise discourage investigation into the invention claimed.

41. I am informed that the final determination of obviousness must also consider "secondary considerations" if presented. In most instances, the patentee raises these secondary considerations of non-obviousness. In that context, the patentee argues an invention would not have been obvious in view of these considerations, which include: (a) commercial success of a product due to the merits of the claimed invention; (b) a long-felt, but unsatisfied need for the invention; (c) failure of others to find the solution provided by the claimed invention; (d) deliberate copying of the invention by others; (e) unexpected results achieved by the invention; (f) praise of the invention by others skilled in the art; (g) lack of independent simultaneous invention within a comparatively short space of time; (h) teaching away from the invention in the prior art.

42. I am further informed that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the evidence and the claimed invention. The nexus cannot be based on prior art features. The establishment of a nexus is a question of fact. While I understand that the Patent Owner here has not offered any secondary considerations at this time, I will supplement my opinions if the Patent Owner raises secondary considerations during this proceeding.

VI. OVERVIEW OF THE '038 PATENT

A. Brief Description of the '038 Patent

43. The '038 Patent describes "methods and systems for flexibly monitoring, evaluating, and initiating actions to enforce security compliance policies." EX1001, 6:36-38. FIG. 2 of the '038 Patent (reproduced below) illustrates process 200 for "controlling the access of endpoint system 104 to host system 102." EX1001, 8:65-9:17.

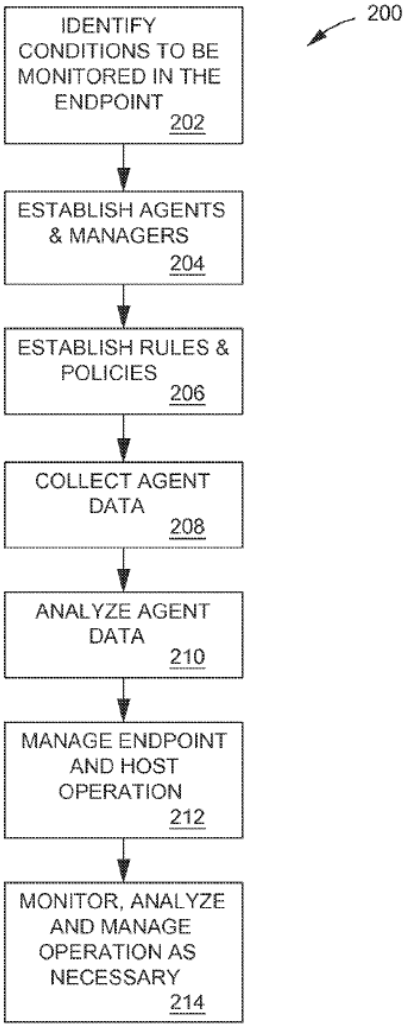


FIG. 2

44. Initially, "conditions" are identified for the system to monitor. EX1001, 9:28-33. The '038 Patent describes these "conditions" broadly, noting that "there are many different data sources and data elements that can be examined to assess the state of the endpoint, form compliance assessments, and ultimately make policy-based access control decisions regarding local and remote computing resources." *Id.* The '038 Patent includes a long list of "illustrative conditions," which include, for example, "Installed service packs," "Running applications," "Antivirus scanning state (e.g. active, idle)," and "Date of last software update." *See* EX1001, 10:21-14:52.

45. "Subsequent to identifying the various conditions to be monitored within endpoint system 104 (step 202), the various agents 104E and agent managers 104D and agent monitor(s) 104C are identified and configured for monitoring those various conditions (step 204)." EX1001, 14:54-57. "Agents can be free standing external software applications, system services provided by the operating system or dedicated, special-purpose monitoring processes that are part of the monitored system itself." EX1001, 15:1-4. In one example, "an agent manager 104D may be configured to query a vendor specific API exposed by a third party antivirus agent, may be configured to query an operating system service periodically to determine if the endpoint has an active network interface and if so, the IP address of that interface, etc." EX1001, 14:57-62.

46. Next, "there are . . . established rules and policies for controlling the access to local resources on the endpoint system 104 or remote host system 102 (step 206)." EX1001, 15:30-36. "The policies established to control access to host system 102 and/or access to local host resources 102G . . . , can specify a number of behavioral options for endpoint system 104." EX1001, 15:37-40. "[C]onfiguration policies include both the configurable behaviors of the compliance analysis engine and the security policies of the systems," including, for example, "[s]ampling interval," an "[e]numerated list of compliance thresholds for different endpoint data elements," "[p]assword expiration age or date," and "[r]equired operating system patches to run a specific application." *See* EX1001, 15:44-21:5.

47. Next, "the various condition data described above is collected by the agent managers through the agents (step 208) and then analyzed (step 210)." EX1001, 24:34-36. "The analysis engine analytical model compares current condition information 104F, policies regarding those conditions 106B and makes action decisions resulting from those conditions and policies, using one or more analytical models." EX1001, 26:29-32. The analysis engine 106C "initiates actions to permit, deny or control access to local and/or remote computing resources based on additional policies that identified permitted and/or denied actions when a noncompliance condition exists." EX1001, 26:33-37.

48. "[W]hen policy violations are detected it may be desired to take one or more discrete actions to either bring the endpoint into compliance, prevent harm from coming to the local and/or remote computers, restrict user actions, or perform any number of different actions (step 212)." EX1001, 50:47-52. "Policy actions may be endpoint actions allowed to take place because the endpoint system 104 is in compliance with security policies, actions to take to partially or wholly restrict access to endpoint resources because the endpoint system 104 is not in compliance with security policies, or a combination thereof." EX1001, 51:4-9. Examples of endpoint policy actions include "[i]nitiate password reset," "[d]elete a malicious file," and/or "[p]ermit or deny network access to an enumerated list of IP addresses or IP network numbers." *See* EX1001, 51:30-53:20, 53:37-54:18. This "process of managing the endpoint and host operations repeats as frequently as necessary (step 214)." EX1001, 50:58-60.

B. File History of the '038 Patent

49. The '038 Patent issued from U.S. Patent App. No. 13/587,505 (the '505 application). The claims of the '505 application were rejected for under 35 U.S.C. § 101, and several claims were rejected as anticipated by U.S. Pat. Pub. No. 2005/0086511 (Balacheff) or rendered obvious by Balacheff in view of U.S. Patent No. 7,805,752 (Newstadt) or U.S. Pub. No 2007/0124803 (Taraz). *See* EX1002, 110-124. To overcome the § 101 rejection, the Applicant amended one independent

claim to recite that the claimed "action" is "carried out by a processor on the endpoint," and noted that another independent claim recited "one or more processors at the computing system configured to . . . ." *See* EX1002, 96-101. To overcome the prior art rejections, the Applicant argued that Belecheff did not describe or suggest "identifying, from the plurality of policies, a plurality of conditions on the endpoint to monitor," "configuring one or more software agents on the endpoint to monitor the plurality of conditions," or that "the action is carried out by a processor on the endpoint." *See* EX1002, 101-103.

50. In allowing the claims, the Examiner entered an Examiner's Amendment in which the term "conditions" was changed to "<u>operating</u> conditions" in several instances, and the processors were specified to be "hardware processors." EX1002, 67-69. Furthermore, the Examiner indicated that Balacheff "teaches providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies; [and] maintaining the plurality of policies in a data store on the computing system." *See* EX1002, 69. However, the Examiner did not believe that the prior art of which he was aware taught or suggested the combination of the remaining "identifying," "configuring," "receiving," "determining," and "initiating" limitations of the independent claims. *See id.* at 69-70. However, the Examiner did not consider the Couillard reference

relied upon in this petition, which alone and/or in combination with Freund teaches and suggests these limitations.

C. Interpretation of the ’038 Patent Claims at Issue

51. I understand that the terms that appear in the claims of the ’038 Patent should be interpreted according to their ordinary and customary meaning in light of the specification (EX1001) and prosecution file history (EX1002). In determining the ordinary and customary meaning, I understand that the words of a claim are first given the plain meaning that those words would have had to one of ordinary skill at the time of the alleged invention. I also understand that the structure of the claims, the specification and file history also may be used to better construe a claim insofar as the plain meaning of the claims cannot be understood. Moreover, I understand that even treatises and dictionaries may be used, albeit under limited circumstances, to determine the meaning attributed by one of ordinary skill to a claim term at the time of filing.

52. I understand that in parallel litigation, certain parties have offered constructions of certain claim terms:

Claim Term	Plaintiff’s Construction	Opposing Construction
“compliance state of the endpoint”	Plain meaning	Level of compliance by the endpoint with compliance policy

		thresholds
"compliance policies"	Plain meaning	The items on an endpoint to monitor, the analysis methods to use, and the permitted thresholds for the monitored items

53. For the purposes of my analysis, I have been instructed to apply the plain and ordinary meaning to the claim terms at issue herein unless noted otherwise. For the above terms, based on the prior art's description of the claimed elements being similar to that of the '038 Patent specification and meeting any of the proposed or otherwise reasonable constructions, I understand that no formal claim constructions are necessary at this stage in this proceeding because claim terms only need to be construed to the extent necessary to resolve a controversy.

54. I also understand that the words of the claims should be interpreted as they would have been interpreted by one of ordinary skill at the time the invention was made (not today). For purposes of my analysis here, I have used the December 21, 2005 purported priority date of the '038 Patent as the date of invention (i.e., the Critical Date). Without exception, however, my analysis of the proper meaning of

the recited claim elements in this declaration would be correct if the date of invention was earlier or later than 2005.

VII. OVERVIEW OF THE CITED REFERENCES

55. The general descriptions that I have provided for the following references and obvious modifications thereof are incorporated into each subsection and mapping of the claims that includes citations to these references.

A. Couillard (EX1004)

56. Couillard "relates to verification of compliance of a device connecting to a corporate network (for example a Local Area Network (LAN)) . . . and connection of the device according to a result of the compliance verification." EX1004, [0002]. The system described by Couillard "protects existing corporate networks by only giving access to compliant workstations and by keeping vulnerable systems out." EX1004, [0015]. "Non-compliant desktops and laptops can be automatically warned and/or quarantined until remediation." *Id.*

57. Couillard's system comprises "'Compliancy Appliance Server' (CAS) deployed centrally within the corporate network along with a lightweight Compliancy Security Agent (CSA) software installed on the workstations." EX1004, [0040]. "The CAS operates as soon as a workstation plugs itself into any network port and a boot up of the device is detected 85." EX1004, [0045]. "At this point, the CAS transparently isolates 87, 88 the workstation within a 'Compliancy

VLAN' (external to corporate resources) and performs 89, 90, 91, 92 a compliancy scan within a few milliseconds." *Id.* "Based on the result of this scan 93, the workstation is then redirected either to its adequate 'Production VLAN' (if deemed compliant) 95 or, alternatively, it may be redirected to either a 'Restricted VLAN' with access to limited resources and where repairs and patch uploads may take place, or a 'Quarantine VLAN' to quarantine the workstation 94." *Id.* As part of the process of sending the device to a different VLAN, the "CAS instructs CSA to close the SSL connection and to make an IP address release and wait a number of second[s] then start an IP address renew." *Id.* "All of these actions are performed based on the compliancy scanning results and depend on the security policies programmed in the CAS by the corporate network administrators and security analysts." *Id.*

58. Couillard's system allows an organization to define a set of Corporate Compliancy Rules (CCR), which are "compliancy process[es] through which is checked a state of the device." *See* EX1004, [0048], [0064]. "The state can be the presence or absence of any information on the device." EX1004, [0064]. For example, the CCRs may include "information concerning all the OS patches, the Antivirus, the spyware, the versions of any piece of software, etc." EX1004, [0064]. The "CSA verifies the compliance of each rule in the set of rules transmitted by the CAS." *See generally* EX1004, [0129]-[0156]. "[A]s soon as a required rule is not

complied with by a device, the device is deemed non-compliant." EX1004, [0061]. "Corrections are made to the device and the process is repeated until the device is deemed compliant." *Id.* "The corrections (remediation) can be made manually or automatically depending on the network settings." *Id.*

59. Couillard describes the CSA as "lightweight . . . software installed on the workstations." EX1004, [0040]. FIG. 3 illustrates the CSA as including various functional components, such as a compliance verifier 72 that "obtain[s] the compliance verification results." EX1004, [0043]. However, beyond these and similarly high-level functional descriptions, Couillard does not dictate or otherwise limit the exact form that the CSA takes, such as the implementation details of the compliance verifier 72 or how it "obtain[s] the compliance verification results." *See id.* Thus, a POSITA would have naturally turned to other prior art and their own knowledge to provide these implementation details.

B. Freund (EX1005)

60. Freund relates to "system and methods for regulating access and maintaining security of individual computer systems and local area networks (LANs) connected to larger open networks (Wide Area Networks or WANs), including the Internet.." EX1005, 1:25-30. Like Couillard, Freund recognizes the security risks from more corporate computers and networks being connected to the Internet, including "attacks by perpetrators (hackers) capable of damaging the local

computer systems, misuse these systems, or steal proprietary data and programs." *See* EX1005, 1:58-2:14.

61. To account for these security risks, Freund describes system and methods providing network administrators, workgroup supervisor[s], and individual PC users with the ability to monitor and regulate the kinds of exchanges permissible between one's local computing environment and external network or WANs, including the Internet." EX1005, 3:41-46. More specifically, the system "provides a client-side filter that is controlled by the centralized authority as long as the centralized authority has a way of enforcing non-compliance, for example, by blocking access to an open network, such as a WAN or the Internet." EX1005, 3:55-59.

62. Like Couillard, Freund's system includes two main structural components: "a client-based filter application (installed at each client), and a central supervisor application that maintains the access rules for the client based filter and verifies the existence and proper operation of the client-based filter application." EX1005, FIG. 3A, 12:45-65, 14:52-15:11; EX1004, FIG. 3, [0040]. "The client-based filter application, which in a preferred embodiment performs all of the monitoring, logging, and filtering work, is responsible for intercepting process loading and unloading," as well as "keeping a list of currently active processes; . . . [and] intercepting and interpreting all TCP/IP communication and build[ing] a

comprehensive representation of these TCP/IP activities." EX1005, 13:23-33. The supervisor application, which is typically installed on a server computer that can be reached via a network by all monitored workstations, "monitors whether a client has the filter application loaded and provides the filter application with the rules for the specific user or workstation." EX1005, 13:66-14:5.

63. In its "Overview" section, Freund also describes an "access management application [that] is employed by the LAN administrator, workgroup administrator, and/or LAN user to maintain a database of the access rules for the workstations being administrated." EX1005, 12:66-13:22. However, Freund does not again refer to the access management application. While Freund does not explicitly describe where the access management application would be executed/hosted, a POSITA would have understood or at least found it obvious that in at least some of the embodiments disclosed in Freund, the access management application would be executed/hosted on the same server as the centralized supervisor application. For example, Freund describes that the supervisor application "specifies rules which govern Internet access by the client computers including the particular client computer" and "provides the filter application with the rules for the specific user or workstation." EX1005, 5:38-41, 13:66-14:5. Thus, even though Freund does not explicitly describe that the access management application and centralized supervisor application are executed/hosted on the same

server, a POSITA would have understood or at least found it obvious that it would be particularly efficient to host the component that "specifies" and "provides" the rules (i.e., the centralized supervisor application) on the same server or server system that "maintain a database of the access rules" (i.e., the access management application). *See generally* EX1005, 12:45-14:12.

64. To perform the "monitoring, logging, and filtering work," the client-based filter application includes a data acquisition module 440, which is illustrated and described with respect to FIGS. 4 and 5. *See* EX1005, 15:12-16:29, 20:50-21:46. The data acquisition module 440, which is preferably implemented as a Windows VxD driver, includes several "hooks" that allow the data acquisition module 440 to hook into various operating system components. EX1005, 20:50-63. For example, data acquisition module 440 includes a "File Hook 503" that "includes functionality allowing the driver 440 to hook into the file subsystem provided by the underlying operating system." EX1005, 20:54-57. Similarly, "Process Hook 505" is a subcomponent that "hooks into the underlying operating system, [and] tracks all currently-executing applications or processes." EX1005, 20:57-60. Each of these hooks "are capable of executing at ring 0--that is, execution at the highest privileged level of the operating system." EX1005, 20:60-63.

C. An Obvious Combination of Couillard and Freund

65. Both Couillard and Freund are analogous art in the same field of art as the '038 Patent, which is at least as broad as controlling endpoint access to computing resources based on the evaluation and enforcement of a set of rules. *See* EX1001, Abstract; EX1004, Abstract; EX1005, Abstract. Given these similarities and based on at least the above noted teachings and their own knowledge, a POSITA would have found it obvious to look to the teachings of Freund when implementing certain features of Couillard's system.

66. In a first example, a POSITA would have recognized that Freund provides teachings of at least one obvious way to implement Couillard's CSA to "obtain the compliance verification results." EX1004, [0043]. As described above, Freund teaches that client-based filter application includes a data acquisition module 440 that includes several "hooks" that allow the data acquisition module 440 to hook into various operating system components and facilitate the "monitoring, logging, and filtering work" performed by the client-based filter application. *See* EX1005, 15:12-16:29, 20:50-21:46. "By intercepting process loading and unloading and keeping a list of currently active processes, each client process can be checked for various characteristics, including checking executable names, version numbers, executable file checksums, version header details, configuration settings, and the like." EX1005, 13:34-39. Similarly, "[b]y intercepting certain file activity and

assigning them to the originating process, the system can track files being created and changed by any process in order to match TCP/IP activities with corresponding file activities." EX1005, 13:57-60.

67. Like Freund's client-based filter application, Couillard describes that its CSA determines the state for the device with respect to rules transmitted by the CAS, where the rules may include the presence, absence, or status of various information of the mobile device, including "any set up and configuration" data. EX1004, [0129]-[0156]. While Couillard does not dictate or otherwise limit how the CSA collects this compliancy information, a POSITA would have found it obvious to look to Freund (e.g., the various hooks utilized by Freund's client-based filter application) to provide at least one obvious implementation of an element of the CSA for collecting at least a portion of the compliancy information. As explained by Freund, hooking into operating system components (e.g., the Winsock communication driver and/or file subsystem) was at least one known way to detect security features or attributes (e.g., checking configuration settings for currently active applications) used to evaluate compliance with security policies. *See* EX1005, 13:23-65, 15:12-16:7, 20:50-63. A POSITA would have been motivated to utilize Freund's teachings, for example, because Freund teaches that these hooks execute "at ring 0," which offers them the highest privilege level and therefore access to the greatest amount of relevant and secure information. *See* EX1005,

20:60-63. Further, a POSITA would have recognized that Couillard and Freund monitor overlapping conditions (e.g., both monitor the list of running processes), and therefore would have naturally turned to Freund for implementation details on how to monitor these conditions. *See* EX1004, [0144]-[0155]; EX1005, 13:23-65, 20:50-63.

68. A POSITA would have had a reasonable expectation of success in implementing this Couillard-Freund combination, because both systems are similarly structured (i.e., a central server maintaining and evaluating rules based on conditions that are monitored by software installed on endpoint/client devices), and the implementation details provided by Freund are intended for use in a similar operating system structure as described in Couillard (e.g., both Couillard and Freund describe the use of Microsoft Windows operating system on the endpoint/client devices). *See* EX1004, [0040], [0142]; EX1005, 5:36-41, 7:13-30. Furthermore, this was a highly predictable art using well known techniques. Thus, it would have been well within the skill of a POSITA to implement the Couillard-Freund combination.

VIII. OVERVIEW OF UNPATENTABILITY GROUNDS

Ground	Claim(s)	Prior Art Basis
1	1, 23, 25, 31, 33	§103 – Couillard and Freund

IX. GROUND 1: COUILLARD AND FREUND RENDER OBVIOUS CLAIMS 1, 23, 25, 31, 33

A. Claim 1

69. Claim 1 of the '038 Patent recites:

> 1. A method for controlling the operation of an endpoint, comprising:
>
> providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;
>
> maintaining the plurality of policies in a data store on the computing system;
>
> identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;
>
> configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;
>
> receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents;
>
> determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and
>
> initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint.

70. As I explain in more detail below through my feature-by-feature analysis, Couillard and Freund disclose or render obvious claim 1.

1. [1pre] A method for controlling the operation of an endpoint, comprising:

71. To the extent the preamble is deemed to be limiting, the Couillard-Freund combination renders it obvious. Couillard describes a system with two

primary elements: a "Compliancy Appliance Server (CAS) deployed centrally within the corporate network along with a lightweight Compliancy Security Agent (CSA) software installed on the workstations." EX1004, [0040]. The CAS and CSAs work together to perform compliancy scans when a workstation attempts to log onto a corporate network. *See* EX1004, [0045]-[0046]. As soon as a workstation plugs itself into a managed network, the CAS and CSA set up an SSL session during which the CAS transparently isolates the workstation within a "Compliancy VLAN" external to corporate resources and performs a compliancy scan. EX1004, [0045]-[0046]. Only after the workstation is determined to be complaint with the security policies programmed in the CAS by the corporate network administrators and security analysts will it be permitted to access the corporate resources. EX1004, [0045]-[0046]. In this regard, "the CAS . . . provides corporate IT personnel the ability to monitor and ***control*** the entire corporate fleet of ***devices (laptop, desktop, PDA, etc.)*** used by users accessing the network." EX1004, [0051][1]. A POSITA would have understood that Couillard's workstations/devices that include a Compliancy Security Agent (CSA) are "endpoints," as that term is used in the '038 Patent. EX1001, 7:52-59 ("endpoint system 104 comprises any processing system capable of interconnecting with host system 102, for example: a ***laptop computer,***

[1] Emphasis added throughout unless otherwise noted.

personal computer, server system, enterprise system, ***personal digital assistant***, cellular telephone, smart telephone or other personal device, or ***any other processing system capable of remotely accessing host system 102 for the purpose of accessing the resources available there on***.").

2. [1a] providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies;

72. Couillard teaches that the actions of the system "are performed based on the compliancy scanning results and depend on the ***security policies*** programmed ***in the CAS by the corporate network administrators and security analysts***," and uses for example a "Microsoft-based Management Console (MMC) . . . use[d] on a daily basis to monitor, manage and query desktops, laptops, servers, networks and other LAN resources." EX1004, [0045]. Thus, the security policies are programmed into the Compliancy Appliance Server (CAS) side 76.

73. With respect to FIG. 2, Couillard teaches that its "invention is composed of a OSI Layer-2 Network Appliance, the 'Compliancy Appliance Server' (CAS) ***deployed centrally within the corporate network*** along with a lightweight Compliancy Security Agent (CSA) software installed on the workstations." EX1004, [0040]. The CSAs on the workstations communicate with the central CAS via TCP/IP connection. *See* EX1004, [0041]. Couillard further teaches that the "term 'corporate network' is intended to cover a Local Area Network (LAN), a

Metropolitan Area Network (MAN) and a Wide Area Network (WAN)." EX1004, [0018]. Accordingly, at least where the corporate network encompasses a MAN or WAN—networks in which components are often separated into remote geographic locations—a POSITA would have understood or at least found it obvious that the Compliancy Appliance Server (CAS) side 76 into which the security policies are programmed is remote from at least some of the workstations/client devices that include the Compliancy Security Agents (CSAs). *See* EX1004, FIG. 3, [0018]; *see also* [0051] (explaining that "the entire corporate fleet of devices" includes mobile devices such as laptops and PDAs that would have been able to connect wirelessly via WAN).

74. Couillard teaches that the "system is preferably accessible within an ***administrator management interface***, such as the Microsoft-based Management Console (MMC), which network and system administrators are already familiar with and use on a daily basis to monitor, manage and query desktops, laptops, servers, networks and other LAN resources." EX1004, [0053]. The proposed UI is custom, for example "preferably implemented in small software items called "snap-in"" built over MMC." EX1004, [0053]. As noted above, Couillard teaches that "the security policies [are] programmed ***in the CAS***," so a POSITA would have understood or at least found it obvious that the CAS would include the administrator management interface through which at least some of those policies (e.g., rules) are programmed.

EX1004, [0045]. Furthermore, it was well known in the art to specify security policies through a central server.

75. For example, as I described in my overview of Freund (Section VII.B), Freund describes an "access management application [that] is employed by the LAN administrator, workgroup administrator, and/or LAN user to maintain a database of the access rules for the workstations being administrated." EX1005, 12:66-13:22. And with respect to FIGS. 7A-K, Freund "illustrate[s] a preferred user interface or 'wizard' dialogs for configuring rules." EX1005, 24:16-17. Freund does not explicitly describe where the access management application and/or rule wizard interface would be executed/hosted.[2] However, Freund describes that the supervisor application—which is hosted on the server accessed by the client workstations—"specifies rules which govern Internet access by the client computers including the particular client computer" and "provides the filter application with the rules for the specific user or workstation." EX1005, 5:38-41, 13:66-14:5. Thus, even though Freund does not explicitly state that the access management application and

[2] This contrasts with the separate user interface illustrated in FIGS. 6A-E, which Freund describes specifically as provided by the client-side monitoring component, and would therefore be executed on the client workstations on which the client-side monitoring component is installed. EX1005, 12:54-61, 22:44-47.

centralized supervisor application are executed/hosted on the same server, a POSITA would have understood or at least found it obvious that it would be practical and efficient to host the component that "specifies" and "provides" the rules (i.e., the centralized supervisor application) on the same server or server system that "maintain[s] a database of the access rules" (i.e., the access management application). *See generally* EX1005, 12:45-14:12.

76. Because Freund does not separately specify a server or other device for the access management application and/or rule wizard interface in the Internet-based (client/server) system 300 illustrated in FIG. 3A, there are only a finite and limited number of provided devices on which to execute/host the access management application and/or rule wizard interface. *See* EX1005, 14:52-15:11. A POSITA thus would have found at least the server 321, which also executes/hosts the supervisor component 323, to have been a logical host for the access management application and/or rule wizard interface for at least the reasons noted above. When applied in the context of Couillard's system, a POSITA would have understood Freund's similar teachings to describe or at least suggest that Couillard's administrator management interface through which the system's security policies are configured would be executed/hosted at the central server that also stores those same rules. Alternatively and furthermore, a POSITA would also have found it obvious, based on the aforementioned teachings of Couillard in view of Freund, that one way to

configure policies would be utilizing a server-based user interface such as that depicted by Freund, for a centrally located user interface to manage policies system-wide.

77. Thus, the Couillard-Freund combination teaches or at least renders obvious "providing a user interface, at a computing system remote from the end point, configured to allow configuration of a plurality of policies," as recited in 1[a].

3. [1b] maintaining the plurality of policies in a data store on the computing system;

78. Couillard describes a "Block and Scan" method that "consists in 'Blocking' any workstation from entering the corporate network, that is blocking it before it obtains an IP address, and 'Scanning' it to make sure it is ***compliant with corporate policies (operating systems, hot fixes, security patches, antivirus software, etc.)***." EX1004, [0014]. As I described with respect to 1[a], Couillard teaches that the actions of the system "are performed based on the compliancy scanning results and depend on the ***security policies programmed in the CAS*** by the corporate network administrators and security analysts." EX1004, [0045]. Thus, these policies define "what is allowed, what is tolerated and what is blocked, in terms of antivirus software, operating systems, and associated security patches and signature files," etc. EX1004, [0014], [0048].

79. Couillard describes that these security policies can comprise Corporate Compliancy Rules (CCRs). EX1004, [0064]. For example, Couillard describes that

the CCRs are each "a compliancy process through which is checked a state of the device." EX1004, [0064]. Consistent with Couillard's description of the security policies, Couillard describes that the CCRs may, for example, "include[] information concerning all the OS patches, the Antivirus, the spyware, the versions of any piece of software, etc." EX1004, [0064]. "The state can be the presence or absence of any information on the device." EX1004, [0064]. The CCRs may include both detection rules (a "rule which is able to identify different characteristics of the device") and compliancy rules (a rule that "can be the presence or the absence or the status of" various conditions of the device). *See* EX1004, [0129]-[0156]. "For example, in the case a Norton Antivirus software was detected in the detection rule, a version and signature file may be checked in the compliance rule to ensure that the proper virus definitions are used by the device." EX1004, [0156]. Thus, a "plurality of policies," as recited in 1[b], is shown by at least any of the following: (1) detection rules, (2) compliancy rules, or (3) sets of rules applicable to different communities. EX1004, [0099], [0110]-[0111], [0127-128], [0142]-[0143], [0198] (discussing sets of rules).

80. The plurality of policies are maintained in a data store on the computing system. Couillard teaches that the Compliancy Appliance Server (CAS) side 76 is preferably designed as a "UNIX-O/S based appliance (OpenBSD ver, 3.5) for the Network Kernel built on carrier-grade Intel servers with redundant components

(power Supplies, fans, ***hardware-based RAID storage***, network interface cards)." EX1004, [0055]-[0056]. As shown in FIG. 3, Couillard teaches that the CAS includes compliance rules 79 (i.e., CCRs), and later describes that, once the CCRs have been defined by the administrator, they "***are stored in the Compliancy Appliance Server (CAS)***." EX1004, [0065]-[0066]; *see also* [0130], [0142] (CAS sends detection and compliancy rules to CSA). The CCRs "can be any electronic format of data sitting on a Computer hard disk device or in a memory of a Computer device." EX1004, [0064].

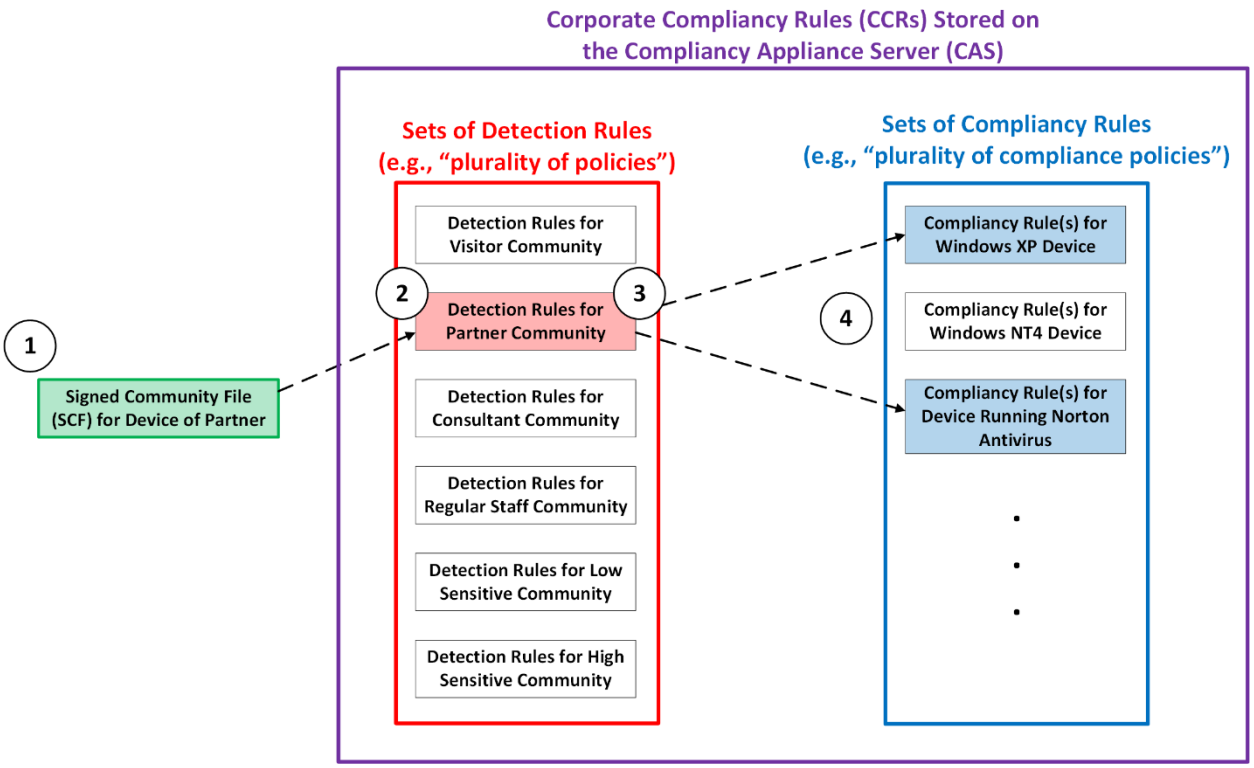
4. [1c] identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;

81. Couillard describes that every time a device attempts to sign into the corporate network via the CAS, the CAS asks the CSA on the device to submit a Signed Community File (SCF). EX1004, [0098]. "The SCF is a signed file allowing the CAS to determine which community the device is identified to and therefore which set of compliancy rules [i.e., CCRs] applies." EX1004, [0099]. An administrator can "define as many communities as the corporation needs," and "[i]t is possible to define an unlimited number of communities." EX1004, [0100]. For example, for the "Partner" community, "the devices are allowed to enter on the corporate network frequently but are not allowed to access sensitive resources," so a "single <<presence of>> Antivirus software [rule] may be sufficient." EX1004, [0108]. On the other hand, for the regular staff community, "the set of compliancy

rules for this community will be much more thorough than that of visitors, consultants or partners because the staff will have access to most of the corporate network resources and confidential corporate information like client files." EX1004, [0110].

82. Couillard describes that the first set of rules applicable for the submitted SCF that are sent to the CSA of the device requesting access to the corporate network are "detection rules." *See* EX1004, [0129]-[0130]. As described above, the "detection rule is a rule which is able to identify different characteristics of the device such as" the presence or the absence of "[a]ny Operating System (O/S) type and version," "[a]ny Antivirus Software installed," or "[a]ny running process on the device." EX1004, [0130]-[0132]. "The detection rules are used to tell the CAS on what type of device the compliance verification will be performed." EX1004, [0142]. "CSA sends the results of detection rules and CAS analyses the detection rule results, and determine[s] and sends to the CSA the proper set of <<compliancy>> rules to check on the device." EX1004, [0142]. Couillard identifies various operating conditions that can be monitored with compliancy rules, with results sent from the CSA to CAS for analysis. EX1004, [0143]-[0158].

83. The following diagram illustrates the sets of policies stored in the CAS and how each is selected for a given device requesting access to the corporate network:



Thus, (1) the CSA of a device requesting access sends its Signed Community File (SCF) to the CAS (*see* EX1004, [0098]-[0112], [0197]); (2) the CAS selects a set of detection rules applicable for the submitted SCF to the CSA of the requesting device (*see* EX1004, [0129]-[0141], [0197]); (3) CSA sends the results of detection rules and CAS analyses the detection rule results (*see* EX1004, [0142], [0197]); (4) the CAS determines and sends to the CSA the proper set of compliancy rules to check on the requesting device (*see* EX1004, [0142]-[0156], [0198]); and (5) the CSA checks the compliancy rules and sends results to the CAS for determination of compliance (EX1004, [0157]-[0158]).

84. A POSITA would have understood or at least found it obvious that the detection rules and/or compliancy rules include a plurality of operating conditions

on the endpoint (e.g., installed antivirus software, running processes, registry key data and state, firewall activation, signature files, etc.) to monitor on the device. *See* EX1004, [0130]-[0146]; *see also* EX1004, [0051] ("the CAS also provides corporate IT personnel the ability to ***monitor*** and control the entire corporate fleet of devices…."). Couillard further discloses that "as soon as a required rule is not complied with by a device, the device is deemed non-compliant," with an option to notify end-users "when their workstations are 'no longer' compliant," and that the "process is repeated until the device is deemed compliant," such as through correcting the non-compliant state (e.g., missing running process or antivirus software). EX1004, [0050]-[0051], [0061].

85. Moreover, it would have been alternatively obvious to a POSITA to configure the CSA to continuously monitor operating conditions specified in the detection rules and associated compliancy rules, after an initial verification, because a POSITA would have known that the state of a device is often continuously changing during its operation and that such changes may render the device non-compliant or alter the relevant compliancy rules. *See, e.g.*, EX1004, [0050] (describing the ability of the CAS to notify end-users when their workstations are no longer compliant); EX1005, 4:5-28 (describing ongoing rules that need to be continuously monitored, such as the "total time a user can be connected," and that some rules may be enforced at certain times of day). Moreover, as described in

greater detail below with respect to 1[g], Couillard describes that non-compliant devices are given an opportunity to remediate issues and recheck their verification state, which would lead to multiple, successive checks of the operating conditions identified in the detection rules and associated compliancy rules. *See* EX1004, [0061], [01609]-[0163], [0190]-[0195]. Thus, a POSITA would have been motivated to implement Couillard's CAS and CSA to continuously monitor the operating conditions of the detection rules and associated compliancy rules, because it would have ensured ongoing security of the corporate network.

86. Thus, when the CAS identifies the set of detection rules applicable for the SCF submitted by the CSA of a device requesting access, and/or the applicable compliancy rules, a POSITA would have understood or at least found it obvious that the CAS is "identifying, from the plurality of policies [i.e., all detection rules and/or compliancy rules for all communities], a plurality of operating conditions on the endpoint to monitor [i.e., the operating conditions specified in the detection rules and/or compliancy rules applicable for the community to which the SCF of the requesting device is associated]," as recited in 1[c]. *See* EX1004, [0142]-[0156].

5. [1d] configuring one or more software agents on the endpoint to monitor the plurality of operating conditions;

87. Couillard generally teaches that the "CSA verifies the compliance of each rule in the set of rules transmitted by the CAS." EX1004, [0143]. FIG. 3 illustrates the CSA as including various components, such as a compliance verifier

72 that "obtain[s] the compliance verification results." EX1004, [0043]. However, as I described in my overview of Couillard and the obvious combination of Couillard and Freund (Sections VII.A and VII.C), Couillard does not dictate or otherwise limit the form that the CSA takes, such as the implementation details of the compliance verifier 72 or how it "obtain[s] the compliance verification results." *See id.*

88. Thus, for at least the reasons described above in my overview of the obvious combination of Couillard and Freund (Section VII.C), a POSITA would have found it obvious to look to Freund (e.g., the implementation of Freund's monitor and data acquisition module 440 and associated hooks) to provide at least one obvious implementation of an element of the CSA for collecting data about the operating conditions specified in the CCRs (and/or compliancy rules and/or detection rules). Like Couillard, Freund's system includes two main components: "a client-based filter application (installed at each client), and a central supervisor application that maintains the access rules for the client based filter and verifies the existence and proper operation of the client-based filter application." EX1005, FIG. 3A, 12:45-65, 14:52-15:11; EX1004, FIG. 3, [0040]. "The client-based filter application, which in a preferred embodiment performs all of the monitoring, logging, and filtering work, is responsible for intercepting process loading and unloading," as well as "keeping a list of currently active processes; . . . [and]

intercepting and interpreting all TCP/IP communication and build[ing] a comprehensive representation of these TCP/IP activities." EX1005, 13:23-33.

89. In order to perform the "monitoring, logging, and filtering work," Freund's client-based filter application includes a data acquisition module 440, which is illustrated and described with respect to FIGS. 4 and 5. *See* EX1005, 15:12-16:29, 20:50-21:46. The data acquisition module 440, which is preferably implemented as a Windows VxD driver, includes several "hooks" that allow the data acquisition module 440 to hook into various operating system components. EX1005, 20:50-63. For example, data acquisition module 440 includes a "File Hook 503" that "includes functionality allowing the driver 440 to ***hook into the file subsystem provided by the underlying operating system***." EX1005, 20:54-57. Similarly, "Process Hook 505" is a subcomponent that "***hooks into the underlying operating system***, [and] tracks all currently-executing applications or processes." EX1005, 20:57-60. Each of these hooks "are capable of executing at ring 0--that is, execution at the highest privileged level of the operating system." EX1005, 20:60-63.

90. A POSITA would have known that:

> In the Microsoft Windows operating system, a hook is a mechanism by which a function can intercept events (messages, mouse actions, keystrokes) before they reach an application. The function can act on events and can, in some cases, modify or discard these events.

> Functions that receive events are called filter functions and are classified according to the type of event they intercept. . . . ***For Windows, the filter function must be installed—that is, attached—to a Windows hook (for example, to a keyboard hook) to be called. Attaching one or more filter functions to a hook is known as setting a hook***. . . . The Win32® (a trademark of Microsoft Corporation) Application Programming Interface (API) ***provides a set of functions to access and modify***: the z-order list; the windows position and styles; and the hook operating system mechanism. . . . In the Microsoft Windows Operating System environment, a Hook Filter is a dynamic library registered at the system level. To set such filter, it is necessary to initialise and ***configure the Hook mechanism using the SetWindowsHook Win32® API*** (Application Programming Interface).

EX1008, 4:52-4:5, 6:5-12.

91. Based on these teachings and for the reasons outlined above in my overview of the obvious combination of Couillard and Freund (Section VII.C), a POSITA would have found it obvious to implement at least one element of Couillard's CSA (e.g., the compliance verifier 72 or a portion thereof) to collect at least a portion of the data about the operating conditions specified in the CCRs (and/or detection rules and/or compliancy rules) in association with step 126 and/or 127 of Couillard's FIG. 6 by setting one or more hooks into the operating system of the device on which the CSA is installed. Having set these hooks, the CSA would have been able to "intercept[] process loading and unloading and keep[] a list of

currently active processes," which would have allowed the CSA to "check[] for various characteristics, including checking ***executable names, version numbers***, executable file checksums, version header details, ***configuration settings***, and the like," as taught by Freund. EX1006, 13:34-39. In this manner, having received the appropriate CCRs (and/or detection rules and/or compliancy rules) from the CAS, Couillard's CSA would thus have been configured via the CCRs (and/or detection rules and/or compliancy rules) to monitor various characteristics with respect to the CCRs (and/or detection rules and/or compliancy rules) being evaluated by the CSA and CAS for compliancy, and for the operating conditions specified in Couillard. *See* EX1004, [0129]-[0156] (describing step 126 of verifying compliance of a device).

92. Under this obvious implementation of the combined teachings of Couillard and Freund, Couillard's CSA itself would be "one or more software agents on the endpoint" that is configured "to monitor the plurality of operating conditions," as recited in 1[d]. Furthermore, Couillard's teachings alone regarding configuring the CSA to monitor the aforementioned operating conditions specified in any of the CCRs, detection rules, and/or compliancy rules would satisfy 1[d], without the teachings of Freund.

6. [1e] receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents;

93. Couillard teaches that, after the CSA verifies compliance for the device for each rule applicable for the submitted SCF in step 126 of FIG. 6, the "CSA transmits a message to CAS containing the result of compliance verification for each rule." EX1004, FIG. 6, [0157]-[0158]. The "CSA, after checking all the compliancy rules status, transmits to CAS the results of each rule." EX1004, [0158]. The results sent to the CAS show the claimed status information about the plurality of operating conditions.

94. Couillard teaches that the CAS receives status information about operating conditions specified in each of the detection and compliancy rules. As described with respect to 1[b], the CCRs include both the detection rules (a "rule which is able to identify different characteristics of the device") and the compliancy rules (a rule that "can be the presence or the absence or the status of" various conditions of the device). *See* EX1004, [0129]-[0156]. As shown in FIG. 6 and explained with respect to steps 125 and 126, Couillard teaches that the proper set of compliancy rules to evaluate on the device is determined from the detection rules. *See* EX1004, [0142]. Thus, as described with respect to 1[c], the CSA first sends status information associated with the detection rules to the CAS to get the proper set of compliancy rules. *See* EX1004, [0142]. Thereafter, the "CSA verifies the

compliance of each rule in the set of rules transmitted by the CAS," and "transmits a message to CAS containing the result of compliance verification for each rule [i.e., status information about the operating conditions specified in the compliancy rules]." *See* EX1004, [0143]-[0158]

95. Here, the "computing system" recited in 1[e] includes at least the Compliancy Appliance Server (CAS) side 76, the "endpoint" recited in 1[e] is the device requesting access to the corporate network, and the "one or more software agents" that gather the "status information about the plurality of operating conditions" recited in 1[e] are the Compliancy Security Agent (CSA) side 70 in conjunction with the hooks it sets in view of Freund (or alternatively without the hooks based on Couillard alone), as described with respect to 1[d]. The communications between the CAS and the CSA happen over a Secure Sockets Layer (SSL) connection via the CSA's network TCP/IP connection 53, and therefore happen "across a network," as recited in 1[e]. *See* EX1004, FIG. 2, [0041], [0071]-[0072], [0096]-[0097].

7. [1f] determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and

96. Couillard describes that the "CSA, after checking all the compliancy rules status, transmits to CAS the results of each rule." EX1004, [0157]-[0158]. Then, Couillard describes that, in step 128, the "CAS analyses [the results from the

CSA] and decides if the device is compliant or not with the rules." EX1004, [0159]-[0164]. "The CAS decision about the compliancy is to check if all required rules are respected." EX1004, [0163]. "A required rule is a rule where a non compliancy will block the device from logging onto the network." EX1004, [0162].

97. Couillard provides an example:

> [A] compliant device could be defined by a network administrator as a device having its O/S up to date with the latest Security OS patches from the manufacturer plus an Antivirus Software version up to date and up and running with the last signature file from the Antivirus manufacturer. In this example, the CAS would have four required rules. One rule for the O/S patches, one rule for the Antivirus Software version, one rule to confirm if the Antivirus is running of the device and the last one to check if the Antivirus has the latest virus signature file from the Antivirus manufacturer. A compliant device will have a successful compliancy verification if all four compliancy rules are respected. The CAS analyses all the rules and make the compliancy decision.

EX1004, [0163]-[0164].

98. In this example, the CAS "determin[es] . . . a compliance state of the endpoint based on the status information and a plurality of compliance policies [e.g., the four required rules] in the data store," as recited in 1[f]. The "compliance state of the endpoint" would be the determination by the CAS of whether "the device is compliant or not with the compliancy rules" (e.g., "O/S up to date with the latest

Security OS patches from the manufacturer") and whether each rule is an "informative," "advisable," or "mandatory" rule. *See* EX1004, [0159]-[0163]. The "status information" is the message transmitted from the CSA to the CAS containing the results of the compliance verification for each rule. *See* EX1004, [0157]-[0158]. And the "plurality of compliance policies in the data store" are the proper set of compliancy rules checked by the CSA, which as noted in 1[b] are stored in the data store. *See* EX1004, [0142]-[0158].

99. The compliance state of the endpoint is "based on" the status information received with respect to each of the detection and compliancy rules. As described with respect to 1[b], the CCRs include both the detection rules (a "rule which is able to identify different characteristics of the device") and the compliancy rules (a rule that "can be the presence or the absence or the status of" various conditions of the device). *See* EX1004, [0129]-[0156]. As shown in FIG. 6 and explained with respect to steps 125 and 126, Couillard teaches that the proper set of compliancy rules to evaluate on the device is determined from the detection rules. *See* EX1004, [0142]. Thus, as described with respect to 1[c], the CSA first sends status information associated with the detection rules to the CAS to get the proper set of compliancy rules. *See* EX1004, [0142]. Thereafter, the "CSA verifies the compliance of each rule in the set of rules transmitted by the CAS," and "transmits a message to CAS containing the result of compliance verification for each rule [i.e.,

the compliancy rules associated with the detection rules]," which the CAS "analyses and decides if the device is compliant or not with the rules." *See* EX1004, [0143]-[0159], [0163]-[0164]. Because the status information associated with the compliancy rules is sent by the CSA after and as a result of the initial status information associated with the detection rules, the compliance state of the endpoint is "based on" the status information received by the CAS from the CSA with respect to each of the detection and compliancy rules. *See generally* EX1004, [0127]-[0159], [0163]-[0164].

100. Couillard describes that "[c]ompliancy rules can be the presence or the absence or the status of," for example, "[a]ny Operating System (O/S) type and version," configuration data, antivirus version, and/or "[a]ny software status (i.e. Antivirus is up and running, personal firewall is activated, etc.)." *See* EX1004, [0144]-[0155]. Accordingly, these compliancy rules include the items on an endpoint to monitor, the analysis methods to use, and the permitted thresholds for the monitored items. *See* EX1004, [0144]-[0155].

8. 1[g] initiating, by the computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint

101. As I described with respect to 1[f], Couillard's "CAS analyses and decides if the device is compliant or not with the rules." EX1004, [0159]-[0164]. Couillard describes that the "CAS can manage many different types of rules."

EX1004, [0161]. One type of rule is a "required rule," which "is a rule where a non compliancy will block the device from logging onto the network." EX1004, [0162]. If the CAS determines that a device is not in compliance with a "required rule," the "device is then put in quarantine until the time a remediation is applied." EX1004, [0162]. On the other hand, if the CAS determines that a device is compliant with all of the applicable rules, the CAS assigns the device to the "production VLAN," where it gains access to the corporate network and associated resources. *See* EX1004, [0044]-[0045], [0165]-[0167].

102. To put a device into any of the production, quarantine, or restricted VLANs, the CAS "sends a <<change VLAN>> request to CAS SNMP server with the device MAC address and device production VLAN assignment." EX1004, [0166], [0192]. As part of the process of sending the device to a different VLAN, the "CAS instructs CSA to close the SSL connection and to make an IP address release and wait a number of second[s] then start an IP address renew." *See* EX1004, [0175]. Thus, a first action that the CAS remotely initiates based on the compliance state is to cause a processor of the device (endpoint) to assist in moving the device to the appropriate separate VLAN.

103. A POSITA would have understood or at least found it obvious that this action (i.e., the instruction to "close the SSL connection and to make an IP address release and wait a number of second then start an IP address renew") would have

been "identified in at least one rule in the data store," as recited in 1[g], such as the exemplary RAID storage on the CAS. EX1004, [0053], [0065]-[0066]. For example, policies and compliance policies are already stored on the CAS, and compliance is determined by the CAS. *See* EX1004, [0065]-[0066], [0157]-[0164]. The instruction from the CAS to the endpoint is a rule (or part of a rule) based on the compliance determination. *See* EX1004, [0160]-[0162], [0165]-[0167], [0190]-[0193]. All of this amounts to instructions that govern the CAS's operation. Thus, the rule implemented by the CAS would be stored on the CAS data store, just like the compliancy rules, as I described above with respect to 1[b] and 1[f].

104. Furthermore, Couillard teaches that each of the Corporate Compliancy Rules (CCRs) is "a compliancy ***process*** through which is checked a state of the device." EX1004, [0064]. A POSITA would have understood or at least found it obvious that one step in this stored "process" would have been the resulting action (e.g., remediation instructions, VLAN directions, notifications) from compliance/non-compliance with the policy, and thus the action is within the compliance rule (or at least a rule) in the data store. Moreover, Couillard teaches that the "CAS can manage many different types of rules," and describes that different rules can be associated with different actions/outcomes. *See* EX1004, [0160]-[0162]. Thus, a POSITA would have at least found it obvious that one straightforward way to associate each rule or rule type with the appropriate

action/outcome would be for the action to be "identified in at least one rule in the data store," as recited in 1[g], because this approach would avoid the need to maintain and access more than one source of data and avoid the need provide logical links between those data stores. A POSITA also would have been motivated with a reasonable expectation of success because it is logical for the CAS, which already makes the compliance determinations and implements rules based on it, to store the rules in the same storage as the compliance policies.

105. Beyond moving the device to a particular VLAN, another action that the CAS remotely initiates based on the compliance state of the device is to initiate remediation. *See* EX1004, [0061], [0161]-[0162]. Specifically, Couillard teaches that "[t]he only way to make [a non-compliant] device compliant again is by having the device go through the same compliancy verification process" after "[c]orrections are made to the device." *See* EX1004, [0061]. "***The corrections (remediation) can be made*** manually or ***automatically*** depending on the network settings." EX1004, [0061]. The CAS can also provide a notification of non-compliance. EX1004, [0050].

106. In one example, Couillard describes that the "device can also be fixed with a CAS automated integrated patch management tool." EX1004, [0162]. In other words, the CAS automatically fixes the device via the integrated patch management tool. A POSITA would have understood or at least found it obvious

that the automatic remediation provided by Couillard's CAS includes "initiating, by the computing system [i.e., at least Couillard's CAS], based on the compliance state, an action [i.e., automatic remediation and/or user notification]. . . , wherein the action is carried out by a processor on the endpoint [i.e., the processor of the non-compliant device installing the patch or other remediation, or displaying the notification, received from the CAS]," as recited in 1[g].

107. A POSITA would have understood or at least found it obvious that the action would have been "identified in at least one rule in the data store" for the reasons described with respect to the VLAN action above. Furthermore, because remediation for any given rule is often associated with that rule (*see, e.g.*, EX1004, [0160]-[0162]), a POSITA would have understood or at least found it obvious that a remediation action would also have been "identified in at least one rule in the data store," as recited in 1[g]. For example, Couillard describes that one required rule could be "to check if the Antivirus has the latest virus signature file from the Antivirus manufacturer." EX1004, [0163]. The remediation for this rule would be to download and install the latest virus signature file, which is an action directly tied to this particular rule. *See* EX1004, [0162]-[0163]. In at least this example from Couillard, a POSITA would have understood or at least found it obvious that the action (i.e., automatically downloading and installing the latest virus signature file) would have been "identified in at least one rule in the data store" (i.e., the required

rule that "the Antivirus has the latest virus signature file from the Antivirus manufacturer" or at least a rule based on the outcome of that determination), as recited in 1[g].

B. Claim 23

108. Claim 23 of the '038 Patent recites:

> **23**. A system for controlling the operation of an endpoint, comprising:
> a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;
> a data store, at the computing system, that contains the plurality of policies;
> one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and
> one or more hardware processors at the computing system configured to:
> receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents,
> determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and
> initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint.

109. As I explain in more detail below through my feature-by-feature analysis, Couillard and Freund disclose or render obvious claim 23.

1. 23[pre] A system for controlling the operation of an endpoint, comprising:

110. Limitation 23[pre] is substantively similar to limitation 1[pre] and is therefore taught by or at least rendered obvious by the combination of Couillard and

Freund for at least the same reasons described above with respect to 1[pre]. Furthermore, Couillard teaches that its invention provides "a ***system*** for verifying compliance of a device wanting to access a corporate network and OSI layer 2 connecting of the device using the compliance verification." EX1004, [0017]. The system taught by Couillard that provides the functionality described with respect to claim 1 is illustrated in at least FIGS. 2 and 3. EX1004, [0021]-[0022], [0040]-[0044].

1. 23[a] a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;

111. Limitation 23[a] is substantively similar to limitation 1[a] and is therefore taught by or at least render obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[a].

2. 23[b] a data store, at the computing system, that contains the plurality of policies;

112. Limitation 23[b] is substantively similar to limitation 1[b] and is therefore taught by or at least render obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[b].

3. 23[c] one or more software agents on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies; and

113. Limitation 23[c] is substantively similar to limitation 1[d] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[d].

4. 23[d] one or more hardware processors at the computing system configured to:

114. Couillard teaches that the Compliancy Appliance Server (CAS) side 76 is preferably designed as a "UNIX-O/S based appliance (OpenBSD ver, 3.5) for the Network Kernel built on carrier-grade ***Intel servers*** with redundant components (power Supplies, fans, hardware-based RAID storage, network interface cards)." EX1004, [0055]-[0056]. As described with respect to 11[pre], Intel servers running UNIX-O/S were known to employ Intel processors executing computer instructions stored on a computer readable medium (e.g., in the RAID storage). Thus, a POSITA would have known or at least found it obvious that Couillard's CAS included "one or more hardware processors at the computing system configured to" perform the various functions described with respect to the CAS and elements 23[d.i]-[d.iii], and indeed a POSITA would have known that such computer functions were ordinarily carried out by hardware processor configured to implement them.

5. 23[d.i] receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software agents,

115. Limitation 22[d.i] is substantively similar to limitation 1[e] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[e].

6. 23[d.ii] determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and

116. Limitation 23[d.ii] is substantively similar to limitation 1[f] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[f].

7. 23[d.iii] initiate, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint.

117. Limitation 23[d.iii] is substantively similar to limitation 1[g] and is therefore taught by or at least rendered obvious by the combination of Couillard and Freund for at least the same reasons described above with respect to 1[g].

C. Claim 25

118. Claim 25 of the ’038 Patent recites:

> **25**. The system of claim **23**, wherein the user interface comprises a web page.

119. The Couillard-Freund combination teaches [25] or at least renders [25] obvious. As I described with respect to 1[a], in order to program the security policies into the CAS, Couillard teaches that the "system is preferably accessible within an ***administrator management interface***, such as the Microsoft-based Management Console (MMC), which network and system administrators are already familiar with and use on a daily basis to monitor, manage and query desktops, laptops, servers, networks and other LAN resources." EX1004, [0053]. As further described with respect to 1[a], it would have been obvious that at least one logical component of Couillard's system to host/execute the administrator management interface would be the CAS (or at least a component of the computing system that includes the CAS), and that Freund provides exemplary descriptions of user interfaces for configuring policies. *See* EX1004, [0045], [0053]; EX1005, 12:45-14:12, 14:52-15:11.

120. Further, it would have been obvious as of the Critical Date that administrator management interfaces could be implemented as a web interface to permit remote access through a web page (as an alternative to or in conjunction with the Microsoft-based Management Console (MMC)). *See, e.g.*, EX1006, [0101]-[0106]; EX1007, 9:14-26; *see also* EX1004, [0161] (describing the provision of compliancy information via a webpage, suggesting access to the compliancy system via web page). Web page-based interfaces were very well known by the 2005 Critical Date. A POSITA would have been motivated to implement the

administrator management interface to comprise a webpage, because it would have permitted remote access to the administrator management interface, not required the administrator to be physically present at the CAS that hosts/executes the administrator management interface, provides ability to readily update the interface through known web-based languages, could provide an interface accessible without installing additional software on a computer accessing the interface, and could provide an interface compatible with different types of hardware and software configurations without needing to program the interface specifically for each (e.g., a web-based interface may run on various operating systems and hardware without modifying interface code). EX1004, [0009] (describing that wireless access to the corporate network and its associated resources—*e.g.*, the administrator management interface–enhances productivity). A POSITA would have had a reasonable expectation of success implementing this predictable interface. *See, e.g.*, EX1006, [0101]-[0106]; EX1007, 9:14-26; *see also* EX1004, [0161] (describing the provision of compliancy information via a webpage, suggesting access to the compliancy system via web page). Thus, a POSITA would have understood or at least found it obvious based on the teachings of Couillard and their own knowledge that Couillard's administrator management interface would have included a web page for configuring policies.

D. Claim 31

121. Claim 31 of the '038 Patent recites:

> **31**. The system of claim **23**, wherein the conditions comprise at least one software condition.

122. As I described above with respect to 1[f], Couillard describes that, in step 128, the "CAS analyses and decides if the device is compliant or not with the rules." EX1004, [0159]-[0164]. "The CAS decision about the compliancy is to check if all required rules are respected." EX1004, [0163]. "A required rule is a rule where a non compliancy will block the device from logging onto the network." EX1004, [0162].

123. Couillard provides an example:

> [A] compliant device could be defined by a network administrator as a device having its O/S up to date with the latest Security OS patches from the manufacturer plus an Antivirus Software version up to date and up and running with the last signature file from the Antivirus manufacturer. In this example, the CAS would have four required rules. One rule for the O/S patches, one rule for the Antivirus Software version, one rule to confirm if the Antivirus is running of the device and the last one to check if the Antivirus has the latest virus signature file from the Antivirus manufacturer. A compliant device will have a successful compliancy verification if all four compliancy rules are respected. The CAS analyses all the rules and make the compliancy decision.

EX1004, [0163]-[0164]. In this example, a POSITA would have understood or at least found it obvious that at least the rules for "confirm[ing] if the Antivirus is running of the device," OS and antivirus version, and "check[ing] if the Antivirus has the latest virus signature file from the Antivirus manufacturer" are "software conditions," as recited in [8], because they are conditions of software. Furthermore, software conditions for detection rules and/or compliancy rules include at least presence, absence, or status of: antivirus software installed, registry key data and state, spyware, file format or program size/date stamp/folder location, running processes, set up and configuration data, and software status (e.g., is antivirus or firewall running). EX1004, [0130]-[0156].

E. Claim 33

124. Claim 33 of the '038 Patent recites:

> **33.** The system of claim **23**, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action.

125. Couillard teaches that the actions of the system "are performed based on the com-pliancy scanning results and depend on the ***security policies programmed in the CAS*** by the corporate network administrators and security analysts." EX1004, [0045]. As I described with respect to 1[b], Couillard describes that these security policies can comprise Corporate Compliancy Rules (CCRs). EX1004, [0064]. For example, Couillard describes that the CCRs are each "a

compliancy process through which is checked a state of the device." EX1004, [0064]. Consistent with Couillard's description of the security policies, Couillard describes that the CCRs may, for example, "include[] information concerning all the OS patches, the Antivirus, the spyware, the versions of any piece of software, etc." EX1004, [0064]. "The state can be the presence or absence of any information on the device." EX1004, [0064]. The CCRs may include both detection rules (a "rule which is able to identify different characteristics of the device") and compliancy rules (a rule that "can be the presence or the absence or the status of" various conditions of the device). *See* EX1004, [0129]-[0156]. "For example, in the case a Norton Antivirus software was detected in the detection rule, a version and signature file may be checked in the compliance rule to ensure that the proper virus definitions are used by the device." EX1004, [0156]. Thus, a "plurality of policies," as recited in 1[b], is shown by at least any of the following: (1) detection rules, (2) compliancy rules, or (3) sets of rules applicable to different communities. EX1004, [0099], [0110]-[0111], [0127-128], [0142]-[0143], [0198] (discussing sets of rules).

126. Furthermore, as described with respect to 1[g], Couillard teaches that each of the Corporate Compliancy Rules (CCRs) is "a compliancy ***process*** through which is checked a state of the device." EX1004, [0064]. A POSITA would have understood or at least found it obvious that one step in this stored "process" would have been the resulting action (e.g., remediation instructions, VLAN directions,

notifications) from compliance/non-compliance with the policy, and thus the action is within a compliance rule (or at least a rule) in the data store. Moreover, Couillard teaches that the "CAS can manage many different types of rules," and describes that different rules can be associated with different actions/outcomes. *See* EX1004, [0160]-[0162]. Thus, a POSITA would have at least found it obvious that one straightforward way to associate each rule or rule type with the appropriate action/outcome would be for policies (detection rules, compliancy rules, CCRs) to "include the at least one rule that identifies the action," because this is a logical organization of the data and avoid the need to maintain and access more than one source of data and avoid the need provide logical links between those data stores.

127. Furthermore, as described for 1[g], Couillard describes multiple possible actions to take in response to a compliance determination (e.g., directing the endpoint to a particular VLAN, automatic remediation, notifications). *See* EX1004, [0160]-[0162], [0165]-[0179]. Couillard explains that "the CAS allows organizations to easily and rapidly define their workstation compliancy policies," and "once defined, the CAS provides corporate network administrators and security analysts the ability to publish and ***enforce*** predefined workstation compliancy policies." EX1004, [0048]-[0049]. A POSITA would have understood from this language that the enforcement rules that identify actions for remediation, notification, and/or VLAN direction are themselves part of the policies, or at least

would have found the language and common sense to suggest that obvious solution so that the consequences of compliance/non-compliance were logically organized and associated with the rules that are used to define compliance. A POSITA also would have been motivated because it is common sense to allow administrators freedom to specify actions specific to particular policies (e.g., that violating a policy with an outdated software version should result in patching it to a specified version, that a particular policy violation should result in an endpoint being directed to a quarantined VLAN instead of a restricted VLAN, etc.), with a reasonable expectation of success as this involves only predictable use of well-known programming techniques. *See* EX1004, [0045] (noting non-compliant endpoints may be directed to restricted VLANs or quarantine VLANs).

128. From at least these teachings, a POSITA would have understood or at least found it obvious that "the plurality of policies includes at least one policy that includes the at least one rule that identifies the action," as recited in [33].

X. ADDITIONAL REMARKS

I currently hold the opinions expressed in this declaration. But my analysis may continue, and I may acquire additional information and/or attain supplemental insights that may result in added observations.

I hereby declare that all statements made are of my own knowledge are true and that all statements made on information and belief are believed to be true. I further declare 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 the Title 18 of the United States Code and that such willful false statements may jeopardize the validity of this proceeding.

Dated: October 24, 2023 By: _____
Dr. Markus Jakobsson

APPENDIX A

CV and Research Statement

Markus Jakobsson
www.linkedin.com/in/markusjakobsson
www.markus-jakobsson.com

1 At a Glance

- **Focus.** *Identification of security problems, trends and solution along four axes* – computational, structural, physical *and* social*; quantitative and qualitative fraud analysis; development of disruptive security technologies.*
- **Education.** *PhD* (Computer Science/Cryptography, University of California at San Diego, 1997); *MSc* (Computer Science, University of California at San Diego, 1994); *MSc* (Computer Engineering, Lund Institute of Technology, Sweden, 1993).
- **Large research labs.** *San Diego Supercomputer Center* (Researcher, 1996-1997); *Bell Labs* (Member of Technical Staff, 1997-2001); *RSA Labs* (Principal Research Scientist, 2001-2004); *Xerox PARC* (Principal Scientist, 2008-2010); PayPal (Principal Scientist of Consumer Security, Director, 2010-2013); Qualcomm (Senior Director, 2013-2015); Agari (Chief Scientist, 2016–2018); Amber Solutions Inc (Chief of Security and Data Analytics, 2018 – 2019); ByteDance (Principal Scientist, 2020-2021)
- **Academia.** *New York University* (Adjunct Associate Professor, 2002-2004); *Indiana University* (Associate Professor & Associate Director, 2004-2008; Adjunct Associate Professor, 2008-2016).
- **Entrepreneurial activity.** *ZapFraud* (Anti-scam technology; CTO and founder, 2012-current); *RavenWhite Security* (Authentication solutions; CTO and founder, 2005-); *RightQuestion* (Consulting; Founder, 2007-current); *FatSkunk* (Malware detection; CTO and founder, 2009-2013 – FatSkunk was acquired by Qualcomm); *LifeLock* (Id theft protection; Member of fraud advisory board, 2009-2013); *CellFony* (Mobile security; Member of technical advisory board, 2009-2013); *PopGiro* (User Reputation; Member of technical advisory board, 2012-2013); *MobiSocial* (Social networking, Member of technical advisory board, 2013); *Cequence Security* (Anti-fraud, Member of technical advisory board, 2013–current)
- **Anti-fraud consulting.** *KommuneData* [Danish govt. entity] (1996); *J.P. Morgan Chase* (2006-2007); *PayPal* (2007-2011); *Boku* (2009-2010); *Western Union* (2009-2010).

- **Intellectual Property, Testifying Expert Witness.** *Inventor of 100+ patents; expert witness in 25+ patent litigation cases* (McDermott, Will & Emery; Bereskin & Parr; WilmerHale; Hunton & Williams; Quinn Emanuel Urquhart & Sullivan; Freed & Weiss; Berry & Domer; Fish & Richardson; DLA Piper; Cipher Law Group; Keker & Van Nest). Details and references upon request.

- **Publications**. Books: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley, 2006); *Crimeware: Understanding New Attacks and Defenses* (Symantec Press, 2008); *Towards Trustworthy Elections: New Directions in Electronic Voting* (Springer Verlag, 2010); *Mobile Authentication: Problems and Solutions*)Springer Verlag, 2012); *The Death of the Internet* (Wiley, 2012); *Understanding Social Engineering* (Springer Verlag, 2016); *Security, Privacy and User Interaction* (Springer Verlag, 2020); *100+ peer-reviewed publications*

2 At a Glance

Ten years before Bitcoin was created, I formalized the notion of Proof of Work and described its use for mining of crypto payments. I later developed energy-efficient alternatives to this paradigm, and showed how to enable mining on mobile devices, which is not possible for Bitcoin. I am the founder of the academic discipline of phishing and have developed techniques to predict fraud trends years before they emerge, enabling countermeasures to be developed before they are needed. I developed the notion of implicit authentication, which is now ubiquitous; I also founded a company that developed the first retroactive virus detection technology, with guarantees of detection; the company was acquired by Qualcomm in 2013. I have worked as chief scientist and similar positions in startups as well as industry behemoths, such as PayPal. I have several hundred patents to my name and am a prominent security researcher with hundreds of peer reviewed publications and an array of textbooks. My 1997 PhD thesis, from University of California at San Diego, was on distributed electronic payment systems with revocable privacy.

3 Work History (Highlights)

1. **Member of Technical Staff, Bell Labs (1997-2001).** Markus was part of the security research group at Bell Labs. He formalized the notion of *proof of work*, later an integral part of BitCoin.

2. **Principal Scientist, RSA Labs (2001-2005).** Markus posited that phishing would become a mainstream problem, and developed ethical techniques for identifying likely trends based on human subject experiments.

3. **Associate Professor, Indiana University (2005-2008).** Markus was hired to lead the newly formed security group at Indiana University, and

created a research group comprising approximately 10 professors and 30 students, studying social engineering and fraud.

4. **Principal Scientist, Xerox PARC (2008-2010).** Markus was hired to lead the research efforts of the Xerox PARC security group, and developed the notion of *implicit authentication*, a technology that is now ubiquitous.

5. **Principal Scientist, PayPal (2010-2013).** Markus did research on security and user interfaces, and developed techniques to reduce the losses associated with *liar buyer fraud*.

6. **Senior Director, Qualcomm (2013-2016).** Qualcomm acquires FatSkunk, a company founded by Markus. At FatSkunk, Markus developed *retroactive* malware detection with provable security guarantees. A simplified version of this is now deployed with almost all Qualcomm chipsets.

7. **Chief Scientist, Agari (2016-2018).** Markus developed a technique to acquire fraudster intelligence by compromising scammer email accounts – *while staying within the law* – resulting in the extradition of several African scam lords to the U.S.

8. **Chief of Security and Data Analytics, Amber Solutions (2018-2020).** Markus developed usable configuration methods supporting improved security and privacy for IoT installations.

9. **Chief Scientist, ByteDance (2020-2021).** Markus oversaw the establishment of a research group and a research agenda at ByteDance, and contributed to their intellectual property and product security.

10. **Chief Scientist, Artema LABS (2021-).** Managing the research, product strategy, and patent strategy for Artema LABS, a Los Angeles based startup in the Crypto/NFT sector.

4 Publication List

Books (1-8); book chapters, journals, conference publications and other scientific publications (9-147), issued /published U.S. patents (148-234). For an updated list, and for international patents, please see `www.markus-jakobsson.com/publications` and appropriate patent search engines.

References

[1] M. Jakobsson, *Security, Privacy and User Interaction*, ISBN 978-3-030-43753-4, 110 pages, 2020.

[2] M. Jakobsson, *Understanding Social Engineering Based Scams*, ISBN 978-1-4939-6457-4, 130 pages, Springer, 2016.

[3] M. Jakobsson, *Mobile Authentication: Problems and Solutions*, ISBN 1461448778, 125 pages, Springer, 2013.

[4] M. Jakobsson, (editor) *The Death of the Internet*, ASIN B009CN2JVE, 359 pages, IEEE Computer Society Press, 2012.

[5] D. Chaum, M. Jakobsson, R. L. Rivest, P. Y. Ryan, J. Benaloh, and M. Kutylowski, (editors), *Towards Trustworthy Elections: New Directions in Electronic Voting*, 411 pages, (Vol. 6000), Springer, 2010.

[6] M. Jakobsson and Z. Ramzan (editors), *Crimeware: Trends in Attacks and Countermeasures*, ISBN 0321501950, Hardcover, 582 pages, Symantec Press / Addison Wesley, 2008.

[7] M. Jakobsson and S. A. Myers (editors), *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft*, ISBN 0-471-78245-9, Hardcover, 739 pages, Wiley, 2006.

[8] M. Jakobsson, M. Yung, J. Zhou, *Applied Cryptography and Network Security: Second International Conference , Yellow Mountain, China, 2004*, 511 pages, Lecture Notes in Computer Science (Book 3089), 2004.

[9] M. Jakobsson, "Permissions and Privacy," in IEEE Security & Privacy, vol. 18, no. 2, pp. 46-55, March-April 2020

[10] M. Jakobsson, "The Rising Threat of Launchpad Attacks," in IEEE Security & Privacy, vol. 17, no. 5, pp. 68-72, Sept.-Oct. 2019

[11] J Koven, C Felix, H Siadati, M Jakobsson, E Bertini, "Lessons learned developing a visual analytics solution for investigative analysis of scamming activities," IEEE transactions on visualization and computer graphics 25 (1), 225-234

[12] M Jakobsson, "Two-factor inauthentication?the rise in SMS phishing attacks" Computer Fraud & Security 2018 (6), 6-8

[13] M. Dhiman, M. Jakobsson, T.-F. Yen, "Breaking and fixing content-based filtering," 2017 APWG Symposium on Electronic Crime Research (eCrime), 52-56

[14] M. Jakobsson, "Addressing sophisticated email attacks," 2017 International Conference on Financial Cryptography and Data Security, 310-317

[15] M. Jakobsson, "User trust assessment: a new approach to combat deception," Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust, 2016, pages 73-78

[16] H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, "Mind your SMSes: Mitigating social engineering in second factor authentication," Computers and Security, 2016

[17] M. Jakobsson, W. Leddy, "Could you fall for a scam? Spam filters are passe. What we need is software that unmasks fraudsters," IEEE Spectrum 53 (5), 2016, 40-55

[18] N. Sae-Bae, M. Jakobsson, *Hand Authentication on Multi-Touch Tablets*, HotMobile 2014

[19] Y. Park, J. Jones, D. McCoy, E. Shi, M. Jakobsson, *Scambaiter: Understanding Targeted Nigerian Scams on Craigslist*, NDSS 2014

[20] D. Balfanz, R. Chow, O. Eisen, M. Jakobsson, S. Kirsch, S. Matsumoto, J. Molina, and P. van Oorschot, "The future of authentication," Security & Privacy, IEEE, 10(1), 22-27, 2012.

[21] M. Jakobsson, and H. Siadati, *Improved Visual Preference Authentication: Socio-Technical Aspects in Security and Trust*, (STAST), 2012 Workshop on IEEE, 27–34, 2012.

[22] M. Jakobsson, R. I. Chow, and J. Molina, "Authentication-Are We Doing Well Enough?[Guest Editors' Introduction]" Security & Privacy, IEEE, 10(1), 19-21, 2012.

[23] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit authentication through learning user behavior," Information Security, 99-113, Springer Berlin Heidelberg, 2011.

[24] M. Jakobsson and K. Johansson, "Practical and Secure Software-Based Attestation," Lightweight Security & Privacy: Devices, Protocols and Applications (LightSec), 1–9, 2011.

[25] A. Juels, D. Catalano, and M.Jakobsson, *Coercion-resistant electronic elections: Towards Trustworthy Elections*, 37–63, Springer Berlin Heidelberg, 2010.

[26] M. Jakobsson and F. Menczer, "Web Forms and Untraceable DDoS Attacks," in Network Security, Huang, S., MacCallum, D., and Du, D. Z., Eds.,77–95, Springer, 2010.

[27] R. Chow, M. Jakobsson, R. Masuoka, J. Molina, Y. Niu, E. Shi, and Z. Song, "Authentication in the Clouds: A Framework and its Application to Mobile Users," 2010.

[28] X. Wang, P. Golle, M. Jakobsson, and A. Tsow, "Deterring voluntary trace disclosure in re-encryption mix-networks," ACM Trans. Inf. Syst. Secur., 13(2), 1-24, 2010.

[29] X. Wang, P. Golle, M. Jakobsson, A.Tsow, "Deterring voluntary trace disclosure in re-encryption mix-networks," ACM Trans. Inf. Syst. Secur. 13(2): (2010)

[30] M. Jakobsson, and C. Soghoian, "Social Engineering in Phishing," Information Assurance, Security and Privacy Services, 4, 2009.

[31] M. Jakobsson, C. Soghoian and S. Stamm, "Phishing," Handbook of Financial Cryptography (CRC press, 2008)

[32] M. Jakobsson and A. Tsow, "Identity Theft," In John R. Vacca, Editor, "Computer And Information Security Handbook" (Morgan Kaufmann, 2008)

[33] S. Srikwan and M. Jakobsson, "Using Cartoons to Teach Internet Security," Cryptologia, vol. 32, no. 2, 2008

[34] M. Jakobsson, N. Johnson and P. Finn, "Why and How to Perform Fraud Experiments," IEEE Security and Privacy, March/April 2008 (Vol. 6, No. 2) pp. 66-68

[35] M. Jakobsson and S. Myers, "Delayed Password Disclosure," International Journal of Applied Cryptography, 2008, pp. 47-59.

[36] M. Jakobsson and S. Stamm, "Web Camouflage: Protecting Your Clients from Browser Sniffing Attacks," IEEE Security & Privacy Magazine. November/December 2007

[37] P. Finn and M. Jakobsson, "Designing and Conducting Phishing Experiments," IEEE Technology and Society Magazine, Special Issue on Usability and Security

[38] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer. "Social Phishing," The Communications of the ACM, October 2007

[39] A. Tsow, M. Jakobsson, L. Yang and S. Wetzel, "Warkitting: the Drive-by Subversion of Wireless Home Routers," Anti-Phishing and Online Fraud, Part II Journal of Digital Forensic Practice, Volume 1, Special Issue 3, November 2006

[40] M. Gandhi, M. Jakobsson and J. Ratkiewicz, "Badvertisements: Stealthy Click-Fraud with Unwitting Accessories," Anti-Phishing and Online Fraud, Part I Journal of Digital Forensic Practice, Volume 1, Special Issue 2, November 2006

[41] N. Ben Salem, J.-P. Hubaux and M. Jakobsson. "Reputation-based Wi-Fi Deployment," Mobile Computing and Communications Review, Volume 9, Number 3 (Best papers of WMASH 2004)

[42] N. Ben Salem, J. P. Hubaux, and M. Jakobsson. "Node Cooperation in Hybrid Ad hoc Networks," IEEE Transactions on Mobile Computing, Vol. 5, No. 4, April 2006.

[43] P. MacKenzie, T. Shrimpton, and M. Jakobsson. "Threshold Password-Authenticated Key Exchange," Journal of Cryptology, 2005

[44] A. Juels, M. Jakobsson, E. Shriver, and B. Hillyer. "How To Turn Loaded Dice Into Fair Coins." IEEE Transactions on Information Theory, vol. 46(3). May 2000. pp. 911–921.

[45] M. Jakobsson, P. MacKenzie, and J.P. Stern. "Secure and Lightweight Advertising on the Web," Journal of Computer Networks, vol. 31, issue 11–16, Elsevier North-Holland, Inc., 1999. pp. 1101–1109.

[46] M. Jakobsson, "Cryptographic Protocols," Chapter from The Handbook of Information Security. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.

[47] M. Jakobsson, "Cryptographic Privacy Protection Techniques," Chapter from The Handbook of Information Security. Hossein Bidgoli, Editor-in-Chief. Copyright John Wiley & Sons, Inc., 2005, Hoboken, N.J.

[48] M. Jakobsson, E. Shi, P. Golle, R. Chow, "Implicit authentication for mobile devices," 4th USENIX Workshop on Hot Topics in Security (HotSec '09); 2009 August 11; Montreal, Canada.

[49] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masuoka, J. Molina, "Controlling data in the cloud: outsourcing computation without outsourcing control," Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW 2009); 2009 November 13; Chicago, IL. NY: ACM; 2009; pp. 85–90.

[50] M. Jakobsson, H. Siadati, M. Dhiman, "Liar Buyer Fraud, and How to Curb It," NDSS, 2015

[51] M. Jakobsson, T.-F. Yen, "How Vulnerable Are We To Scams?," BlackHat, 2015

[52] M. Jakobsson, "How to Wear Your Password," BlackHat, 2014

[53] M. Jakobsson and G. Stewart, "Mobile Malware: Why the Traditional AV Paradigm is Doomed, and How to Use Physics to Detect Undesirable Routines," in BlackHat, 2013.

[54] M. Jakobsson, and H. Siadati,"SpoofKiller: You Can Teach People How to Pay, but Not How to Pay Attention" in Socio-Technical Aspects in Security and Trust (STAST), 2012 Workshop on, 3-10, 2012.

[55] M. Jakobsson, and M. Dhiman,"The benefits of understanding passwords," in Proceedings of the 7th USENIX conference on Hot Topics in Security, Berkeley, CA, USA, 2012.

[56] M. Jakobsson, and S. Taveau, "The Case for Replacing Passwords with Biometrics," Mobile Security Technologies, 2012.

[57] M. Jakobsson and D. Liu, "Bootstrapping mobile PINs using passwords," W2SP, 2011.

[58] M. Jakobsson and R. Akavipat, "Rethinking passwords to adapt to constrained keyboards," 2011.

[59] Y. Niu, E. Shi, R. Chow, P. Golle, and M. Jakobsson, "One Experience Collecting Sensitive Mobile Data," In USER Workshop of SOUPS, 2010.

[60] E. Shi, Y. Niu, M. Jakobsson, and R. Chow, "Implicit Authentication through Learning User Behavior," 2010.

[61] M. Jakobsson and K. Johansson, Assured Detection of Malware With Applications to Mobile Platforms, 2010.

[62] M. Jakobsson and K. Johansson, "Retroactive Detection of Malware With Applications to Mobile Platforms," in HotSec 2010, Washington, DC, 2010.

[63] M. Jakobsson, A Central Nervous System for Automatically Detecting Malware, 2009.

[64] R. Chow, P. Golle, M. Jakobsson, R. Masuoka, J. Molina, E. Shi, and J. Staddon, "Controlling data in the cloud: outsourcing computation without outsourcing control," ACM workshop on Cloud computing security (CCSW), 2009.

[65] M. Jakobsson and A. Juels, "Server-Side Detection of Malware Infection," in New Security Paradigms Workshop (NSPW), Oxford, UK, 2009.

[66] M. Jakobsson, "Captcha-free throttling," Proceedings of the 2nd ACM workshop on Security and artificial intelligence, 15–22, 2009.

[67] M. Jakobsson, E. Shi, P. Golle, and R. Chow, "Implicit authentication for mobile devices," Proceedings of the 4th USENIX conference on Hot topics in security, 9–9, 2009.

[68] C. Soghoian, O. Friedrichs and M. Jakobsson, "The Threat of Political Phishing," International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008)

[69] R. Chow, P. Golle, M. Jakobsson, L. Wang and X. Wang, "Making CAPTCHAs Clickable," In proc. of HotMobile 2008.

[70] M. Jakobsson, A. Juels, and J. Ratkiewicz, "Privacy-Preserving History Mining for Web Browsers," Web 2.0 Security and Privacy, 2008.

[71] M. Jakobsson, E. Stolterman, S. Wetzel, L. Yang, "Love and Authentication," (Notes) ACM Computer/Human Interaction Conference (CHI), 2008. Also see `www.I-forgot-my-password.com`

[72] M. Jakobsson and S. Myers, "Delayed Password Disclosure," Proceedings of the 2007 ACM workshop on Digital Identity Management

[73] M. Jakobsson, S. Stamm, Z. Ramzan, "JavaScript Breaks Free," W2SP '07

[74] A. Juels, S. Stamm, M. Jakobsson, "Combatting Click Fraud via Premium Clicks," USENIX Security 2007

[75] R. Chow, P. Golle, M. Jakobsson, X. Wang, "Clickable CAPTCHAs," Ad-Fraud '07 Workshop; 2007 September 14; Stanford, CA, USA

[76] S. Stamm, Z. Ramzan, and M. Jakobsson, "Drive-by Pharming," In Proceedings of Information and Communications Security, 9th International Conference, ICICS 2007

[77] M. Jakobsson, A. Tsow, A. Shah, E. Blevis, Y.-K. Lim, "What Instills Trust? A Qualitative Study of Phishing," USEC '07.

[78] R. Akavipat, V. Anandpara, A. Dingman, C. Liu, D. Liu, K. Pongsanon, H. Roinestad and M. Jakobsson, "Phishing IQ Tests Measure Fear, not Ability," USEC '07.

[79] M. Jakobsson, "The Human Factor in Phishing," American Conference Institute's Forum on Privacy & Security of Consumer Information, 2007

[80] S. Srikwan, M. Jakobsson, A. Albrecht and M. Dalkilic, "Trust Establishment in Data Sharing: An Incentive Model for Biodiversity Information Systems," TrustCol 2006

[81] J.Y. Choi, P. Golle, M. Jakobsson, "Tamper-Evident Digital Signatures: Protecting Certification Authorities Against Malware," DACS '06

[82] L. Yang, M. Jakobsson, S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad hoc Networks," SECURECOMM '06

[83] P. Golle, X. Wang, M. Jakobsson, A. Tsow, "Deterring Voluntary Trace Disclosure in Re-encryption Mix Networks." IEEE S&P '06

[84] M. Jakobsson, A. Juels, T. Jagatic, "Cache Cookies for Browser Authentication (Extended Abstract)," IEEE S&P '06

[85] M. Jakobsson and J. Ratkiewicz, "Designing Ethical Phishing Experiments: A study of (ROT13) rOnl auction query features.", WWW '06

[86] M. Jakobsson and S. Stamm. "Invasive Browser Sniffing and Countermeasures," WWW '06

[87] J.Y. Choi, P. Golle and M. Jakobsson. "Auditable Privacy: On Tamper-Evident Mix Networks," Financial Crypto '06

[88] A. Juels, D. Catalano and M. Jakobsson. "Coercion-Resistant Electronic Elections," WPES '05

[89] V. Griffith and M. Jakobsson. "Messin' with Texas, Deriving Mother's Maiden Names Using Public Records," ACNS '05, 2005.

[90] M. Jakobsson and L. Yang. "Quantifying Security in Hybrid Cellular Networks," ACNS '05, 2005

[91] Y.-C. Hu, M. Jakobsson, and A. Perrig. "Efficient Constructions for One-way Hash Chains," ACNS '05, 2005

[92] M. Jakobsson. "Modeling and Preventing Phishing Attacks," Phishing Panel in Financial Cryptography '05. 2005, abstract in proceedings.

[93] N. Ben Salem, J.-P. Hubaux, and M. Jakobsson. "Reputation-based Wi-Fi Deployment Protocols and Security Analysis," In WMASH '04. ACM Press, 2004. pp. 29–40.

[94] M. Jakobsson and S. Wetzel. "Efficient Attribute Authentication with Applications to Ad Hoc Networks," In VANET '04. ACM Press, 2004. pp. 38–46.

[95] M. Jakobsson, X. Wang, and S. Wetzel. "Stealth Attacks in Vehicular Technologies," Invited paper. In Proceedings of IEEE Vehicular Technology Conference 2004 Fall (VTC-Fall 2004). IEEE, 2004.

[96] A. Ambainis, H. Lipmaa, and M. Jakobsson. "Cryptographic Randomized Response Technique," In PKC '04. LNCS 2947. Springer-Verlag, 2004. pp. 425–438.

[97] P. Golle, M. Jakobsson, A. Juels, and P. Syverson. "Universal Re-encryption for Mixnets," In CT-RSA '04. LNCS 2964. Springer-Verlag, 2004. pp. 163–178.

[98] P. Golle and M. Jakobsson. "Reusable Anonymous Return Channels," In WPES '03. ACM Press, 2003. pp. 94–100.

[99] M. Jakobsson, S. Wetzel, B. Yener. "Stealth Attacks on Ad-Hoc Wireless Networks," In IEEE VTC '03, 2003.

[100] N. Ben Salem, L. Buttyan, J.-P. Hubaux, and M. Jakobsson. "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks," In ACM MobiHoc '03. ACM Press, 2003. pp. 13–24.

[101] M. Jakobsson, J.-P.Hubaux and L. Buttyan. "A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks," In FC '03. LNCS 2742. Springer-Verlag, 2003. pp. 15–33.

[102] M. Jakobsson, T. Leighton, S. Micali and M. Szydlo. "Fractal Merkle Tree Representation and Traversal," In RSA-CT '03 2003.

[103] A. Boldyreva and M Jakobsson. "Theft protected proprietary certificates," In DRM '02. LNCS 2696, 2002. pp. 208–220.

[104] P. Golle, S. Zhong, M. Jakobsson, A. Juels, and D. Boneh. "Optimistic Mixing for Exit-Polls," In Asiacrypt '02. LNCS 2501. Springer-Verlag, 2002. pp. 451–465.

[105] P. MacKenzie, T. Shrimpton, and M. Jakobsson. "Threshold Password-Authenticated Key Exchange," In CRYPTO '02. LNCS 2442. Springer-Verlag, 2002. pp. 385–400.

[106] M. Jakobsson. "Fractal Hash Sequence Representation and Traversal," In Proceedings of the 2002 IEEE International Symposium on Information Theory (ISIT '02). 2002. pp. 437–444.

[107] M. Jakobsson, A. Juels, and R. Rivest. "Making Mix Nets Robust For Electronic Voting By Randomized Partial Checking," In Proceedings of the 11th USENIX Security Symposium. USENIX Association, 2002. pp. 339–353.

[108] D. Coppersmith and M. Jakobsson. "Almost Optimal Hash Sequence Traversal," In Financial Crypto '02. 2002.

[109] M. Jakobsson. "Financial Instruments in Recommendation Mechanisms," In Financial Crypto '02. 2002.

[110] J. Garay, and M. Jakobsson. "Timed Release of Standard Digital Signatures," In Financial Crypto '02. 2002.

[111] F. Menczer, N. Street, N. Vishwakarma, A. Monge, and M. Jakobsson. "Intellishopper: A Proactive, Personal, Private Shopping Assistant," In AAMAS '02. ACM Press, 2002. pp. 1001–1008.

[112] M. Jakobsson, A. Juels, and P. Nguyen. "Proprietary Certificates," In CT-RSA '02. LNCS 2271. Springer-Verlag, 2002. pp. 164–181.

[113] M. Jakobsson and A. Juels. "An Optimally Robust Hybrid Mix Network," In PODC '01. ACM Press. 2001. pp. 284–292.

[114] M. Jakobsson and M. Reiter. "Discouraging Software Piracy Using Software Aging," In DRM '01. LNCS 2320. Springer-Verlag, 2002. pp. 1–12.

[115] M. Jakobsson and S. Wetzel. "Security Weaknesses in Bluetooth," In CT–RSA '01. LNCS 2020. Springer-Verlag, 2001. pp. 176–191.

[116] M. Jakobsson and D. Pointcheval. "Mutual Authentication for Low-Power Mobile Devices," In Financial Crypto '01. LNCS 2339. Springer-Verlag, 2001. pp. 178–195.

[117] M. Jakobsson, D. Pointcheval, and A. Young. "Secure Mobile Gambling," In CT–RSA '01. LNCS 2020. Springer-Verlag, 2001. pp. 110–125.

[118] M. Jakobsson and S.Wetzel. "Secure Server-Aided Signature Generation," In PKC '01. LNCS 1992. Springer-Verlag, 2001. pp. 383–401.

[119] M. Jakobsson and A. Juels. "Addition of ElGamal Plaintexts," In T. Okamoto, ed., ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 346–358.

[120] M. Jakobsson, and A. Juels. "Mix and Match: Secure Function Evaluation via Ciphertexts," In ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 162–177.

[121] R. Arlein, B. Jai, M. Jakobsson, F. Monrose, and M. Reiter. "Privacy-Preserving Global Customization," In ACM E-Commerce '00. ACM Press, 2000. pp. 176–184.

[122] C.-P. Schnorr and M. Jakobsson. "Security of Signed ElGamal Encryption," In ASIACRYPT '00. LNCS 1976. Springer-Verlag, 2000. pp. 73–89.

[123] P. Bohannon, M. Jakobsson, and S. Srikwan. "Cryptographic Approaches to Privacy in Forensic DNA Databases," In Public Key Cryptography '00. LNCS 1751. Springer-Verlag, 2000, pp. 373–390.

[124] J. Garay, M. Jakobsson, and P. MacKenzie. "Abuse-free Optimistic Contract Signing," In CRYPTO '99. LNCS 1666. Springer-Verlag, 1999. pp. 449–466.

[125] M. Jakobsson. "Flash Mixing," In PODC '99. ACM Press, 1999. pp. 83–89.

[126] G. Di Crescenzo, N. Ferguson, R. Impagliazzo, and M. Jakobsson. "How To Forget a Secret," In STACS '99. LNCS 1563. Springer-Verlag, 1999. pp. 500–509.

[127] M. Jakobsson, D. M'Raihi, Y. Tsiounis, and M. Yung. "Electronic Payments: Where Do We Go from Here?," In CQRE (Secure) '99. LNCS 1740. Springer-Verlag, 1999. pp. 43–63.

[128] C.P. Schnorr and M. Jakobsson. "Security Of Discrete Log Cryptosystems in the Random Oracle + Generic Model," In Conference on The Mathematics of Public-Key Cryptography. 1999.

[129] M. Jakobsson and A. Juels "Proofs of Work and Breadpudding Protocols," In CMS '99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 252 – 272.

[130] M. Jakobsson and C-P Schnorr. "Efficient Oblivious Proofs of Correct Exponentiation," In CMS '99. IFIP Conference Proceedings, Vol. 152. Kluwer, B.V., 1999. pp. 71–86.

[131] M. Jakobsson, P. MacKenzie, and J.P. Stern. "Secure and Lightweight Advertising on the Web," In World Wide Web '99

[132] M. Jakobsson, J.P. Stern, and M. Yung. "Scramble All, Encrypt Small," In Fast Software Encryption '99. LNCS 1636. Springer-Verlag, 1999. pp. 95–111.

[133] M. Jakobsson and J. Mueller. "Improved Magic Ink Signatures Using Hints," In Financial Cryptography '99. LNCS 1648. Springer-Verlag, 1999. pp. 253–268.

[134] M. Jakobsson. "Mini-Cash: A Minimalistic Approach to E-Commerce," In Public Key Cryptography '99. LNCS 1560. Springer-Verlag, 1999. pp. 122–135.

[135] M. Jakobsson. "On Quorum Controlled Asymmetric Proxy Re-encryption," In Public Key Cryptography '99. LNCS 1560. Springer-Verlag, 1999. pp. 112–121.

[136] M. Jakobsson and A. Juels. "X-Cash: Executable Digital Cash," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 16–27.

[137] M. Jakobsson and D. M'Raihi. "Mix-based Electronic Payments," In Proceedings of the Selected Areas in Cryptography. LNCS 1556. Springer-Verlag, 1998. pp. 157173.

[138] M. Jakobsson, E. Shriver, B. Hillyer, and A. Juels. "A Practical Secure Physical Random Bit Generator," In CCS '98: Proceedings of the 5th ACM conference on Computer and communications security. ACM Press, 1998. pp. 103–111.

[139] M. Jakobsson. "A Practical Mix," In Advances in Cryptology – EuroCrypt '98. LNCS 1403. Springer-Verlag, 1998. pp. 448–461.

[140] M. Jakobsson and M. Yung. "On Assurance Structures for WWW Commerce," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 141–157.

[141] E. Gabber, M. Jakobsson, Y. Matias, and A. Mayer. "Curbing Junk E-Mail via Secure Classification," In Financial Cryptography '98. LNCS 1465. Springer-Verlag, 1998. pp. 198–213.

[142] M. Jakobsson and M. Yung. "Distributed 'Magic Ink' Signatures," In Advances in Cryptology – EuroCrypt '97. LNCS 1233. Springer-Verlag, 1997. pp. 450–464.

[143] M. Jakobsson and M. Yung. "Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System," In Financial Cryptography '97. LNCS 1318. Springer-Verlag, 1997. pp. 217–238.

[144] A. Herzberg, M. Jakobsson, S. Jarecki, H. Krawczyk, and M. Yung. "Proactive public-key and signature schemes," In Proceedings of the 4th Annual Conference on Computer Communications Security. ACM Press, 1997. pp. 100–110.

[145] M. Bellare, M. Jakobsson, and M. Yung. "Round-Optimal Zero-Knowledge Arguments Based on any One-Way Function," In Advances in Cryptology – EuroCrypt '97. LNCS 1233. Springer-Verlag, 1997. pp. 280–305.

[146] M. Jakobsson and M. Yung. "Proving Without Knowing," In Crypto '96. LNCS 1109. Springer-Verlag, 1996. pp. 186–200.

[147] M. Jakobsson, K. Sako, and R. Impagliazzo. "Designated Verifier Proofs and Their Applications," In Advances in Cryptology – EuroCrypt '96. LNCS 1070. Springer-Verlag, 1996. pp. 143–154.

[148] M. Jakobsson and M. Yung. "Revokable and Versatile Electronic Money," In CCS '96: Proceedings of the 3rd ACM conference on Computer and communications security. ACM Press, 1996. pp. 76–87.

[149] M. Jakobsson. "Ripping Coins for a Fair Exchange," In Advances in Cryptology – EuroCrypt '95. LNCS 921. Springer-Verlag, 1995. pp. 220–230.

[150] M. Jakobsson. "Blackmailing using Undeniable Signatures," In Advances in Cryptology EuroCrypt '94. LNCS 950. Springer-Verlag, 1994. pp. 425–427.

[151] M. Jakobsson. "Reducing costs in identification protocols," Crypto '92, 1992.

[152] M. Jakobsson. "Machine-Generated Music with Themes," In International Conference on Artificial Neural Networks '92. Vol 2. Amsterdam: Elsevier, 1992. pp. 1645–1646

[153] M. Jakobsson, "Social Engineering 2.0: What's Next," McAfee Security Journal, Fall 2008

[154] M. Jakobsson and S. Myers, "Delayed Password Disclosure," ACM SIGACT News archive, Volume 38, Issue 3 (September 2007), pp. 56 - 75

[155] V. Griffith and M. Jakobsson. "Messin' with Texas, Deriving Mother's Maiden Names Using Public Records," CryptoBytes, 2007.

[156] M. Jakobsson, A. Juels, J. Ratkiewicz, "Remote-Harm Detection," Beta-version available at `rhd.ravenwhitedevelopment.com/`

[157] S. Stamm, M. Jakobsson, "Social Malware," Experimental results available at `www.indiana.edu/ phishing/verybigad/`

[158] M. Jakobsson. "Privacy vs. Authenticity," Ph.D. Thesis, University of California at San Diego, 1997

[159] Markus Jakobsson, Automatic PIN creation using passwords, US20130125214 A1, 2012.

[160] Markus Jakobsson, Systems and methods for creating a user credential and authentication using the created user credential, US 20130111571 A1, 2012.

[161] Markus Jakobsson, Password check by decomposing password, US 20120284783 A1, 2012.

[162] Markus Jakobsson, William Leddy, System and methods for protecting users from malicious content, US 20120192277 A1, 2011.

[163] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US8370935 B1, 2011.

[164] Markus Jakobsson, Methods and Apparatus for Efficient Computation of One-Way Chains in Cryptographic Applications, US20120303969 A1, 2011.

[165] Markus Jakobsson, Automatic PIN creation using password, US 20120110634 A1, 2011.

[166] Markus Jakobsson, Jim Roy Palmer, Gustavo Maldonado, Interactive CAPTCHA, US20130007875 A1, 2011.

[167] Markus Jakobsson, System access determination based on classification of stimuli, US 20110314559 A1, 2011.

[168] Markus Jakobsson, System access determination based on classification of stimuli, WO 2011159356 A1, 2011.

[169] Markus Jakobsson, Method, medium, and system for reducing fraud by increasing guilt during a purchase transaction, US8458041 B1, 2011.

[170] Markus Jakobsson, Visualization of Access Information, US 20120233314 A1, 2011.

[171] Markus Jakobsson, Richard Chow,Runting Shi, Implicit authentication, US20120137340 A1, 2010.

[172] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, EP2467793 A1, 2010.

[173] Markus Jakobsson, Event log authentication using secure components, US 20110314297 A1, 2010.

[174] Markus Jakobsson, Philippe J.P. Golle, Risk-based alerts, US 20110314426 A1, 2010.

[175] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US 20110041178 A1, 2010.

[176] M. Jakobsson, A. Juels, J. Kaliski Jr, S. Burton and others, Identity authentication system and method, US Patent 7,502,933, 2009.

[177] Markus Jakobsson, Method and system for facilitating throttling of interpolation-based authentication, US8219810 B2, 2009.

[178] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US8375442 B2, 2009.

[179] Markus Jakobsson, Karl-Anders R. Johansson, Auditing a device, US 20110041180 A1, 2009.

[180] Markus Jakobsson, Pattern-based application classification, US 20110055925 A1, 2009.

[181] Markus Jakobsson, Method and apparatus for detecting cyber threats, US8286225 B2, 2009.

[182] Markus Jakobsson, Method and apparatus for detecting cyber threats, US20110035784 A1, 2009.

[183] Markus Jakobsson, CAPTCHA-free throttling, US8312073 B2, 2009.

[184] Markus Jakobsson, Captcha-free throttling, US 20110035505 A1, 2009.

[185] Markus Jakobsson, Christopher Soghoian, Method and apparatus for throttling access using small payments, US 20100153275 A1, 2008.

[186] Markus Jakobsson, Christopher Soghoian, Method and apparatus for mutual authentication using small payments, US 20100153274 A1, 2008.

[187] Philippe J.P. Golle, Markus Jakobsson,Richard Chow, Resetting a forgotten password using the password itself as authentication, US 20100125906 A1, 2008.

[188] Philippe J. P. Golle, Markus Jakobsson,Richard Chow, Authenticating users with memorable personal questions, US8161534 B2, 2008.

[189] Richard Chow, Philippe J.P. Golle, Markus Jakobsson, Jessica N. Staddon, Authentication based on user behavior, US20100122329 A1, 2008.

[190] Richard Chow, Philippe J.P. Golle, Markus Jakobsson, Jessica N. Staddon, Enterprise password reset, US 20100122340 A1, 2008.

[191] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, US8086866 B2, 2008.

[192] Richard Chow, Philippe J. P. Golle, Markus Jakobsson, Selectable captchas, US8307407 B2, 2008.

[193] Markus Jakobsson, Ari Juels, Sidney Louis Stamm, Method and apparatus for combatting click fraud, US 20080162227 A1, 2007.

[194] Jakobsson, Method and apparatus for evaluating actions performed on a client device, US 20080037791 A1, 2007.

[195] Jakobsson, Ari Juels, Method and apparatus for storing information in a browser storage area of a client device, US 20070106748 A1, 2006.

[196] Markus Jakobsson, Steven Andrew Myers, Anti-phising logon authentication object oriented system and method, WO 2006062838 A1, 2005.

[197] Jakobsson, Jean-Pierre Hubaux,Levente Buttyan, Micro-payment scheme encouraging collaboration in multi-hop cellular networks, US 20050165696 A1, 2004.

[198] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane D. Rice,Less , System and method providing disconnected authentication, WO2005029746 A3, 2004.

[199] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane Rice, Ronald Rivest, Less , System and method providing disconnected authentication, US 20050166263 A1, 2004.

[200] Andrew Nanopoulos, Karl Ackerman, Piers Bowness, William Duane, Markus Jakobsson, Burt Kaliski, Dmitri Pal, Shane D. Rice,Less , Systeme et procede d'authentification deconnectee, WO 2005029746 A2, 2004.

[201] Markus Jakobsson, Ari Juels, Burton S. Kaliski Jr., Identity authentication system and method, WO2004051585 A3, 2003.

[202] Markus Jakobsson, Ari Juels, Burton S. Kaliski, Jr., Identity authentication system and method, US 7502933 B2, 2003.

[203] Markus Jakobsson, Ari Juels, Burton S. Kaliski Jr., Systeme et procede de validation d'identite, WO 2004051585 A2, 2003.

[204] Markus Jakobsson, Burton S. Kaliski, Jr., Method and apparatus for graph-based partition of cryptographic functionality, US7730518 B2, 2003.

[205] Markus Jakobsson, Phong Q. Nguyen, Methods and apparatus for private certificates in public key cryptography, US7404078 B2, 2002.

[206] Jakobsson, Philip MacKenzie, Thomas Shrimpton, Method and apparatus for performing multi-server threshold password-authenticated key exchange, US20030221102 A1, 2002.

[207] Markus Jakobsson, Philip D MacKenzie, Method and apparatus for distributing shares of a password for use in multi-server password authentication, US 7073068 B2, 2002.

[208] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, EP 1389376 A1 (text from WO2002084944A1), 2002.

[209] Markus Jakobsson, Adam Lucas Young, Method and apparatus for identification tagging documents in a computer system, US 7356845 B2, 2002.

[210] Juan A. Garay, Markus Jakobsson, Methods and apparatus for computationally-efficient generation of secure digital signatures, US 7366911 B2, 2001.

[211] Markus Jakobsson, Methods and apparatus for efficient computation of one-way chains in cryptographic applications, US 7404080 B2, 2001.

[212] Markus Jakobsson, Susanne Gudrun Wetzel, Securing the identity of a bluetooth master device (bd addr) against eavesdropping by preventing the association of a detected channel access code (cac) with the identity of a particular bluetooth device, WO2002019641 A3, 2001.

[213] Markus Jakobsson, Susanne Gudrun Wetzel, Procede et appareil permettant d'assurer la securite d'utilisateurs de dispositifs a capacites bluetooth, WO 2002019641 A2, 2001.

[214] Robert M. Arlein, Ben Jai, Markus Jakobsson, Fabian Monrose, Michael Kendrick Reiter, Less , Methods and apparatus for providing privacy-preserving global customization, US 7107269 B2, 2001.

[215] Markus Jakobsson, Susanne Gudrun Wetzel, Secure distributed computation in cryptographic applications, US6950937 B2, 2001.

[216] Markus Jakobsson, Susanne Gudrun Wetzel, Method and apparatus for ensuring security of users of short range wireless enable devices, US6981157 B2, 2001.

[217] Markus Jakobsson, Susanne Gudrun Wetzel, Method and apparatus for ensuring security of users of bluetooth TM-enabled devices, US 6574455 B2, 2001.

[218] Garay; Juan A. (West New York, NJ), Jakobsson; M. (Hoboken, NJ), Kristol; David M. (Summit, NJ), Mizikovsky; Semyon B.(Morganville, NJ), Cryptographic key processing and storage , 7023998, 2001.

[219] Markus Jakobsson, Method, apparatus, and article of manufacture for generating secure recommendations from market-based financial instrument prices, US 6970839 B2, 2001.

[220] Markus Jakobsson, Encryption method and apparatus with escrow guarantees, US7035403 B2, 2001.

[221] Jakobsson, Call originator access control through user-specified pricing mechanism in a communication network, US20020099670 A1, 2001.

[222] Markus Jakobsson, Claus Peter Schnorr, Tagged private information retrieval, US7013295 B2, 2000.

[223] Markus Jakobsson, Secure enclosure for key exchange, US 7065655 B1, 2000.

[224] Markus Jakobsson, Michael Kendrick Reiter, Software aging method and apparatus for discouraging software piracy, US 7003110 B1, 2000.

[225] Markus Jakobsson, Probabilistic theft deterrence, US6501380 B1, 2000.

[226] Markus Jakobsson, Michael Kendrick Reiter, Abraham Silberschatz, Anonymous and secure electronic commerce, EP 1150227 A1, 2000.

[227] Markus Jakobsson, Ari Juels, Proofs of work and bread pudding protocols, US 7356696 B1, 2000.

[228] Markus Jakobsson, Joy Colette Mueller, Methods of protecting against spam electronic mail, US7644274 B1, 2000.

[229] Philip L. Bohannon, Markus Jakobsson,Fabian Monrose, Michael Kendrick Reiter,Susanne Gudrun Wetzel, Less , Generation of repeatable cryptographic key based on varying parameters, EP1043862 B1, 2000.

[230] Markus Jakobsson, Ari Juels, Mix and match: a new approach to secure multiparty computation, US6772339 B1, 2000.

[231] Markus Jakobsson, Ari Juels, Mixing in small batches, US6813354 B1, 2000.

[232] Philip L. Bohannon, Markus Jakobsson,Fabian Monrose, Michael Kendrick Reiter,Susanne Gudrun Wetzel, Less , Generation of repeatable cryptographic key based on varying parameters, US 6901145 B1, 36566

[233] Markus Jakobsson, Claus Peter Schnorr, Non malleable encryption method and apparatus using key-encryption keys and digital signature, US6931126 B1, 2000.

[234] Markus Jakobsson, Claus Peter Schnorr, Non malleable encryption method and apparatus using key-encryption keys and digital signature, US 6931126 B1, 2000.

[235] Markus Jakobsson, Flash mixing apparatus and method, US 6598163 B1, 1999.

[236] Markus Jakobsson, Minimalistic electronic commerce system, US 6529884 B1, 1999.

[237] Markus Jakobsson, Method and system for providing translation certificates, US 6687822 B1, 1999.

[238] Markus Jakobsson, Verification of correct exponentiation or other operations in cryptographic applications, US6978372 B1, 1999.

[239] Markus Jakobsson, Non malleable encryption apparatus and method, US 6507656 B1, 1999.

[240] Markus Jakobsson, Method and system for quorum controlled asymmetric proxy encryption, US 6587946 B1, 1998.

[241] Markus Jakobsson, Practical mix-based election scheme, US 6317833 B1, 1998.

[242] Markus Jakobsson, Ari Juels, Method and apparatus for extracting unbiased random bits from a potentially biased source of randomness, US 6393447 B1, 1998.

[243] Markus Jakobsson, Ari Juels, Executable digital cash for electronic commerce, US6157920 A, 1998.

[244] Bruce Kenneth Hillyer, Markus Jakobsson, Elizabeth Shriver, Storage device random bit generator, US 6317499 B1, 1998.

[245] Markus Jakobsson, Method and apparatus for encrypting, decrypting, and providing privacy for data values, US 6049613 A, 1998.