

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.
Petitioner

v.

WEBROOT INC.
Patent Owner

Case No. IPR2023-01050
Patent No. 8,763,123

DECLARATION OF DR. MARKUS JAKOBSSON, PH.D.

TABLE OF CONTENTS

I.	Introduction	4
A.	Materials Reviewed	4
B.	Background and Qualifications	5
II.	Legal Framework	14
III.	Opinion.....	21
A.	Overview of the '123 Patent.....	21
B.	Overview of the Relevant File Histories	27
C.	Summary of the EPO Counterpart Application.....	31
D.	Level of a Person Having Ordinary Skill in the Art.....	33
E.	Claim Construction	34
F.	Summary of the Prior Art References	35
1.	Ackroyd.....	35
2.	Dahlstrom.....	39
G.	Opinions Regarding Ground 1: <i>Ackroyd</i> Renders Claims 1, 3-4, and 6-16 Obvious	42
1.	Claim 1	42
2.	Claim 3 - The method according to claim 1, wherein the details of the one or more security products includes the name of the security products, versions, and loaded signature files.	58
3.	Claim 10 - The method according to claim 3, wherein the details of all or selected security products further includes settings at a particular point in time.	60
4.	Claim 11 - The method according to claim 1, further comprising: identifying, by the base computer, one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the at least one of the other remote computers; and determining, by the base computer, that the identified one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the at least one of the other remote computers is vulnerable to the malware process.....	61

5. Claim 14 - The method according to claim 1, wherein the one or more security products include a firewall product and an antivirus product.	62
H. Opinions Regarding Ground 2: <i>Ackroyd</i> in View of <i>Dahlstrom</i> Renders Claims 2 and 5 Obvious	64
1. Claim 2 - The method according to claim 1, further comprising: providing information to the user of the remote computer that the remote computer may be susceptible to attack by the malware processes.	64
IV. Conclusion	69

I, Dr. Markus Jakobsson, declare the following:

I. INTRODUCTION

1. I have been retained by counsel for Petitioner as a technical expert in the above-captioned case. Specifically, I have been asked to render certain opinions in regard to the IPR petition with respect to U.S. Patent No. 8,763,123 (the “123 Patent”) (Ex. 1001). I understand that the Challenged Claims are claims 1-16 and my opinions are limited to those claims. My compensation in this matter is not based on the substance of my opinions or the outcome of this matter. I have no financial interest in Petitioner.

A. Materials Reviewed

2. In reaching my opinions in this matter, I have reviewed the following materials:

- Exhibit 1001 – U.S. Patent No. 8,763,123 (“123 Patent”)
- Exhibit 1002 – File History of U.S. Patent No. 8,763,123 (“123 FH”)
- Exhibit 1003 – European File History (“EPO File History”)
- Exhibit 1005 – U.S. Patent No. 7,269,851 to Ackroyd (“Ackroyd”)
- Exhibit 1006 – U.S. Patent Publication No. 2004/000670 to Dahlstrom et al. (“Dahlstrom”)
- Exhibit 1009 – U.S. Patent No. 6,944,772 to Dozortsev (“Dozortsev”)
- Exhibit 1010 – EP 1,549,012 to De Spiegeleer (“Spiegeleer”)
- Exhibit 1011 – EP 1,280,040 to Hinchliffe et al. (“Hinchliffe”)

- Exhibit 1012 – WO 2002/033525 to Chuang (“*Chuang*”)
- Exhibit 1013 – U.S. Patent Publication No 2004/0073810 to Dettinger et al. (“*Dettinger*”)
- Exhibit 1014 – WO 2003/021402 to Duke (“*Duke*”)
- Exhibit 1015 – U.S. Patent Publication No 2003/0115479 to Edwards et al. (“*Edwards*”)
- Exhibit 1017 – U.S. Patent No. 6,663,000 to Muttik et al. (“*Muttik*”)
- Exhibit 1018 – PC Broadband Security by Darren Meyer (“*PC broadband security*”)
- Exhibit 1019 – Wired to the World Anti-virus Software by Ralph Lee Scott (“*Anti-virus software*”)

B. Background and Qualifications

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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).

11. 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).

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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);
- “Towards Trustworthy Elections: New Directions in Electronic Voting” (Springer, 2010).

20. Books translated to Chinese and Korean have separate titles and years of release.

21. 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)

22. 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.

23. My opinions are based on my years of education, research, and experience, as well as my study of relevant materials. In forming my opinions, I have also considered the materials identified in this declaration and in the Petition.

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

II. LEGAL FRAMEWORK

25. 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.

26. 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).

27. 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.

28. 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

III. OPINION

A. Overview of the '123 Patent

38. The '123 Patent is generally directed to a system and process for identifying vulnerabilities to malware on remote computers by receiving and using information about the security products operating on those remote computers. '123 Patent (Ex. 1001), Abstract. For instance, the '123 Patent explains that “the present invention relates to a method and apparatus for determining the protection that a remote computer has from malware.” *Id.*, 1:12-14. In the embodiments of the '123 Patent, malware includes malicious code or objects, such as viruses, trojans, worms, spyware, adware, etc. *Id.*, 1:19-22, 8:1-4.

39. The '123 Patent provides that traditional anti-malware products typically scan objects to look for signatures that are known to be indicative of malware. *Id.*, 1:23-34. There is, according to the '123 Patent, usually a delay between

a new malware object being released and the development of known signatures for identifying that malware. *Id.*, 1:35-47. The '123 Patent describes how known methods and systems suffer from this delay in between the time when the malware is released, and when the existing anti-malware techniques discover and distribute a signature for identifying the malware. *Id.*, 2:63-3:3. The '123 Patent describes these prior art methods and systems as “rel[ying] solely on signature matching[.]” *Id.*, 3:14-15.

40. The '123 Patent purports to describe different methods and systems which do not rely purely on signature matching to identify malware. For example, the '123 Patent describes alleged techniques for “rapid determination” that overcome the need for detailed analysis of the object itself to determine whether or not the object is malware. *Id.*, 3:14-24. The '123 Patent describes that this “rapid determination” of malware can be accomplished by sharing data between several remote computers and a base computer. *Id.*, 3:25-36. This shared data can include data about a potential malware object, such as: “executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object

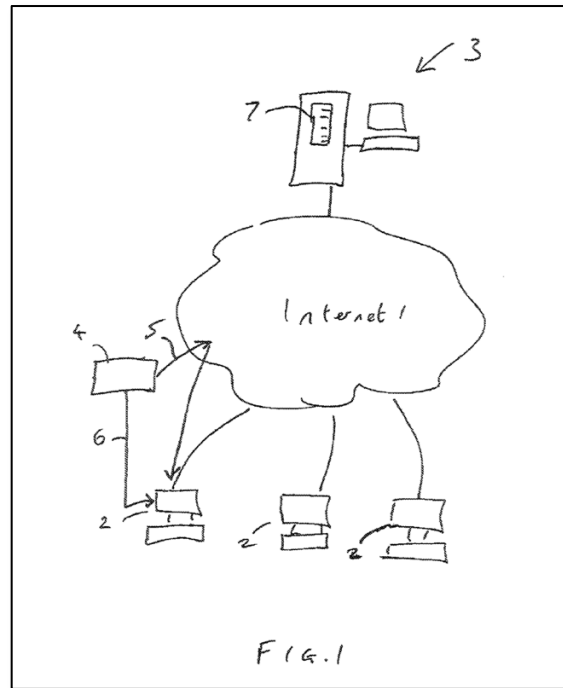
when the object is created, configured or runs on the respective remote computers.”

Id. In certain embodiments, “the data is sent in the form of [a] key that is obtained by a hashing process carried out in respect of the objects on the respective remote computers.” *Id.*, 3:48-56.

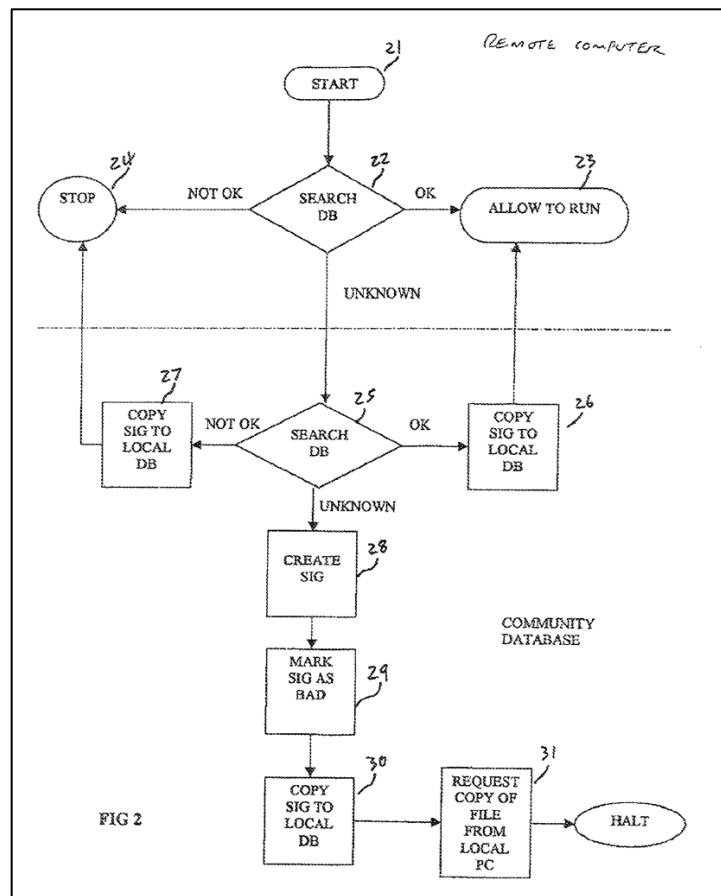
41. For instance, the ’123 Patent describes several techniques for conducting a malware determination. As an example, the ’123 Patent describes a technique for detecting malware that involves “the concept of ancestry[.]” *Id.*, 6:13-19. As described in the ’123 Patent, “[t]he key relating to the first object may be inspected to identify a component that uniquely identifies the first object and that is inherited or otherwise present in the key of a descendant or other related object of the first object.” *Id.* In the ’123 Patent’s instance, the method described will “automatically classify[] as malware any computer object that has a key in which said unique identifier component is present[.]” where the unique identifier is also associated with malware. *Id.*, 6:20-26. In other embodiments, the ’123 Patent describes “trusted installers,” and a method in which “any objects relating to or created by the trusted installer are automatically authorized to proceed.” *Id.*, 7:11-25.

42. The ’123 Patent includes what appear to be hand drawn figures that purport to depict embodiments of the alleged invention. For example, Figure 1

illustrates an apparatus for purportedly conducting the alleged methods described therein:



Id., Fig. 1. Various described methods are illustrated in flowcharts, as shown below:



Id., Fig. 2; *see also id.*, Fig. 3 (illustrating flow chart for creating and utilizing a mask); Fig. 4 (illustrating an information obtaining stage).

43. Referencing the flowchart of Figure 2, the '123 Patent describes several processes for determining whether an object is safe, unsafe, or suspicious. *See generally id.*, 8:21-15:35. The five processes for determining whether an object is safe, unsafe, or suspicious are characterized as “preferred central heuristics[.]” *See id.* A first process uses “the singularity or plurality of names, locations, vendor, product and version information captured and correlated from all of the remote computers 2 that have seen the object.” *Id.*, 10:43-46. A second process uses “an

object's relationship to other objects that act upon it or upon which it acts." *Id.*, 11:5-6. A third process involves time and volumes, such that the "[r]elevant data includes when the object was first seen, when it was last seen, how many times it has been seen, how many times it has been seen in a given interval of time, and the increase or decrease of acceleration in it being seen." *Id.*, 11:60-64. A fourth process "considers the behaviour of an object[,]" which "allows a score to be developed based on the types of events performed by an object or events performed on it by itself or other objects." *Id.*, 12:16-19. Finally, a fifth process "considers the behavior of a web page or script." *Id.*, 12:45-46. In each of these processes, the database in the system collects metadata from the remote computers, and that metadata can be used to define behavior across the community, or network. *Id.*, 13:54-65.

44. The metadata described in the '123 Patent can also be used to identify vulnerabilities on particular remote computers. For example, aspects of the present invention describe "a method of determining the protection that a remote computer has from malware," comprising:

receiving at a base computer details of all or selected security products operating at a point in time on said remote computer; receiving similar information from other remote computers connected to the base computer; and, identifying any malware processes that were not identified by said other remote computers having that particular combination of security products.

Id., 5:25-36. In this embodiment, “the base computer can be used to obtain information as to whether for example a particular, specific combination of operating system and various security products, including settings and signature files existing at a point in time, renders a particular computer having those products and settings susceptible or vulnerable to any particular malware object.” *Id.*, 5:37-43. With this, if a base computer knows that a computer has a certain version of an anti-virus product, and it knows that a malware process was not detected at that computer, then this information can be used to determine that the computer has a vulnerability to that malware process. *Id.*, 16:5-17:15. In this instance, the user might be advised of the vulnerability, such as through a prompt to update anti-virus software. *See id.*, 16:5-17:15.

B. Overview of the Relevant File Histories

45. I understand that the application that issued as the '123 Patent was filed on July 8, 2012, as a divisional claiming priority to U.S. Patent Application No. 11/477,807, which was filed on June 30, 2006. '123 *File History* (Ex. 1002). I also understand that this application also claimed foreign priority dating back to June 30, 2005. *Id.* I have been told to assume a June 30, 2005 priority date for the Challenged Claims for the purposes of my opinions herein.

46. On April 15, 2013, the Examiner entered an Office Action that rejected all pending claims 1-9. '123 *File History*, 91-98. Most of the claims, including

independent claims 1 and 4, were rejected as obvious in view of prior art references Dahlstrom and Beddoe. *Id.* Dependent claims 3, 6, and 9, were rejected as obvious over Dahlstrom and Beddoe in further view of Mateev. *Id.* In response, Applicant submitted claim amendments, and emphasized that “the claimed invention generally relates to a computer that provides information to a community database that is representative of all or selected ones of the software products loaded on or available [to] the computer.” ’123 *File History*, 123-134. The Applicant attempted to distinguish the Dahlstrom reference by stressing the ability to determine a computer’s vulnerability to malware based on the security products on that computer. Specifically, the Applicant asserted that “Dahlstrom fails to teach, disclose, or render obvious at least identifying one or more of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer; and identifying one or more malware processes that were not identified by the combination of security products operating on the one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the remote computer.” *Id.*

47. On August 6, 2013, the Examiner entered another Office Action which maintained the obviousness rejections based on Dahlstrom, Beddoe, and Mateev. ’123 *File History*, 138-148. The Applicant requested and received an Examiner

Interview. *'123 File History*, 159-163. In this interview, the Applicant characterized the discussion and the “inventive concept” of the claimed invention, stating: “the inventive concept ‘Security products updated on remote computers by central computer, and scanning for malware not detected on remote computers due to lack of updated antivirus software. Further Detection of malware on cloud of computer networks and updating of security products on computers.’” *Id.* On December 5, 2013, the Applicant submitted a Request for Continued Examination. *'123 File History*, 164-165.

48. Subsequently, after the Examiner Interview and Request for Continued Examination, on December 12, 2013, the Applicant submitted a supplemental Information Disclosure Statement. In that disclosure, the Applicant identified for the first time the Ackroyd reference used in my opinions below (at the time, a pending application with Application No. 2003/0131256). A month later, on January 14, 2014, the Applicant’s representative and the Examiner conducted another Interview. *'123 File History*, 206. The purportedly allowable subject matter discussed in that interview involved “security products on multiple computers scanning remote computers, detecti[ng] malware in cloud by remote and base computers[.]” *Id.* As set out in the interview summary, this subject matter was recited in dependent Claim 3, and the Applicant’s representative and the Examiner discussed amending the claims to include this concept into the independent claims. *Id.* However, just two

weeks later, a Notice of Allowability was entered into the record on January 29, 2014. *'123 File History*, 231. Notably, the Examiner did not require the limitations from Claim 3 to be included into the independent claims. *Id.* Instead, the Examiner included an Examiner's Amendment with the Notice of Allowability, and that amendment required: "receiving, at a base computer, details uniquely identifying one or more security products...." *Id.* (emphasis in original denoting the Examiner's Amendment).

49. Importantly, the Examiner's Reasons for Allowance reference a "submission of amended claims on 1/21/2014[.]" I have reviewed this file history, but those amended claims do not appear in the record. *'123 File History*, 206-231, also *Id.* 138-165. According to the Examiner's Reasons for Allowance, the allowable subject matter hinged on the following aspects of the claims that was purportedly included in the missing claim amendments: "Detecting malware on remote computers by base computer, by comparing the security product(s) on remote and base computers, and comparing malware objects by size, name, logical storage and path of the malware object and details as described in independent claim(s)." *'123 File History*, 231. **But those amendments are not included in the issued claims.**

50. Thus, there is a disconnect in the record between what the Examiner seemed to think was allowable as compared to the claims that were ultimately issued. *Id.* Even worse, the Applicant's representative noted this discrepancy in a letter to

the Office dated April 29, 2014, but **the problem was never cured** and, instead, the Applicant's representative simply suggested that the entirety of the independent claims should be understood as allowable subject matter. *'123 File History*, 235-237.

C. Summary of the EPO Counterpart Application

51. I understand that on May 13, 2013, the Applicant of the '123 Patent in the United States filed a divisional application requesting a grant of a European Patent. *See EPO File History* (Ex. 1003). The application claims priority to GB Application No. 0513375.6 dated June 30, 2005, which I compared with the '123 Patent, and confirmed is the same priority document listed on the face of the '123 Patent. *'123 File History*, 179-235. On August 30, 2013, a European Search Report was entered, which identified a single document considered to be relevant. This was U.S. Patent Application No. 2003/131256 to Ackroyd. *'123 File History*, 168-170. In the opinion in this report, the representative from the European Patent Office noted that Ackroyd was "very relevant for the present invention," and noted that the reference disclosed the same concepts claimed. *'123 File History*, 168-170. After several intervening changes to the applicant's representative on file and the applicant itself, examination started on April 19, 2018. *'123 File History*, 121-128. The examining unit rejected all the claims based on Ackroyd, explaining that Ackroyd discloses the features of the claims. *Id.* The correspondence did note that one feature

seemed to be missing from Ackroyd—receiving at the base computer “details of processes run by said other remote computers that were not locally identified as being malware.” *Id.* That concept was ultimately deemed not patentable in the European Patent Office. I note that this limitation is not present in any of the Challenged Claims of the ’123 Patent.

52. I understand that after several sets of claim amendments and an oral hearing, the examining division issued a decision refusing the application. ’123 *File History*, 39-58. In that decision, the division concluded that the claims were not inventive over Ackroyd. *Id.* The examining division found two alleged differences between the teachings of Ackroyd and the claims presented to the European Patent Office. These are (1) that information about susceptibility to attack is provided to the user, and (2) that the database search is performed in a different way as described in more detail below (*id.*, 87-93). *Id.*¹ But neither of these were sufficient to show an inventive step and merit a patent award. *Id.* More importantly, neither of these alleged differences that the European Patent Office noted in comparing the claims to Ackroyd are present in any of the independent claims of the ’123 Patent. *Compare id.*, 87-93 (expressly including: (1) “providing information to the user...”; and (2)

¹ I have been informed that the Applicant in the EPO has filed a notice of appeal, and the process is still pending. *See id.* at Notice of Appeal dated October 4, 2019.

“searching the database (7) to identify any processes marked as being malware that occurred on computers (2) having the same particular combination of security products as the first remote computer (2) and that were not locally detected”) *with* ’123 Patent, 20:21- 67, 21: 1-56, and 22:1-56.

53. The first alleged difference (involving providing information to the user) appears only in dependent claims 2 and 5 of the ’123 Patent. But as described below, the prior art central to my opinions below and in view of my analysis renders these claims unpatentable as obvious. The second noted difference (involving the database search) does not appear in any of the Challenged Claims. Therefore, the analysis and conclusion from the European Patent Office that the claims submitted there are not patentable in view of Ackroyd is directly relevant to the Challenged Claims and their patentability here.

D. Level of a Person Having Ordinary Skill in the Art

54. I have been asked to provide my opinion as to the level of skill of a person having ordinary skill in the art at the time of the ’123 Patent, which I have been instructed to assume is June 30, 2005. In determining the characteristics of a hypothetical person having ordinary skill in the art at the time of the claimed invention, I was told to consider several factors, including the type of problems encountered in the art, the solutions to those problems, the rapidity with which innovations are made in the field, the sophistication of the technology, and the

education level of active workers in the field. I also placed myself back in the time frame of the claimed invention and considered the colleagues with whom I had worked at that time.

55. In my opinion, a person having ordinary skill in the art, as of June 30, 2005, would have been a person having 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 host monitoring systems, software security analysis, and dynamic malware analysis. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. Such a person would have been capable of understanding the '123 Patent and the prior art references discussed below.

56. Based on my education, training, and professional experience in the field of the claimed invention, I am familiar with the level and abilities of a person of ordinary skill in the art at the time of the claimed invention. Additionally, I met at least these minimum qualifications to be a person having ordinary skill in the art as of the time of the claimed invention of the '123 Patent.

E. Claim Construction

57. I have been informed by counsel that the first step in a patentability analysis involves construing the claims, as necessary, to determine their scope. Second, the construed claim language is then compared to the disclosures of the prior

art. I am informed that claims are generally given their ordinary and customary meaning as understood by a person having ordinary skill in the art at the time of the invention, in light of the patent specification.

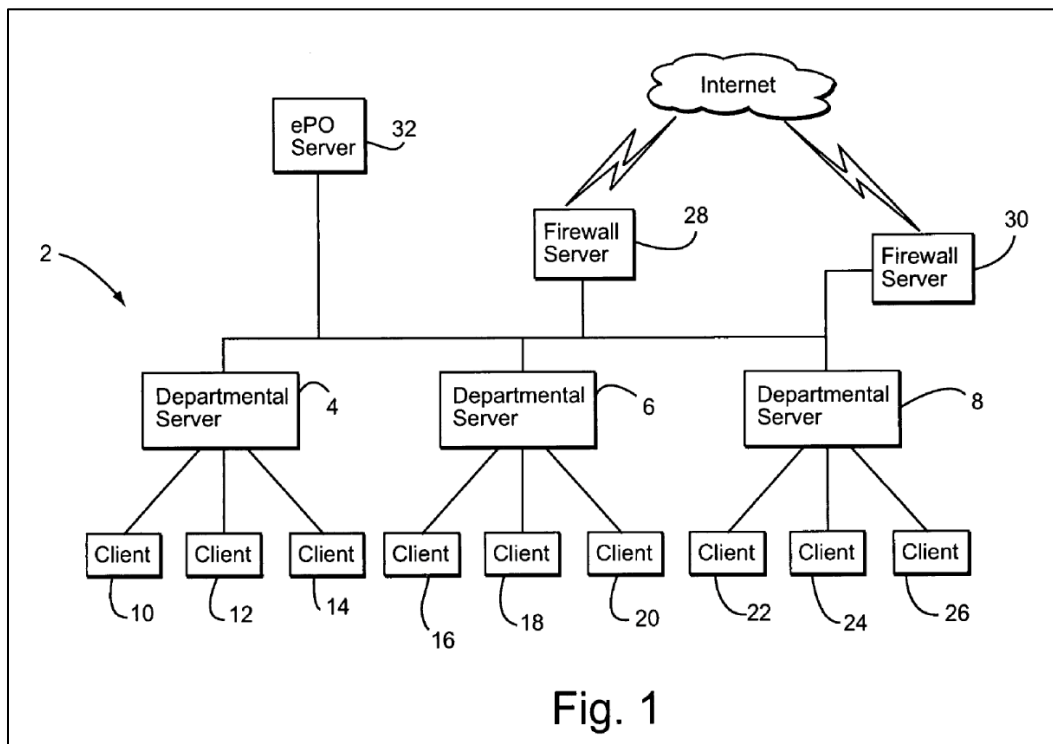
58. I understand that in parallel litigation, Patent Owner contends that no claim language requires express construction. For the purposes of my analysis, I have been instructed to apply the plain and ordinary meaning to the claim terms at issue herein unless noted otherwise.

F. Summary of the Prior Art References

1. Ackroyd

59. *Ackroyd* (Ex. 1005) generally relates to managing malware protection in a computer network, and more specifically, discloses a managing computer within a computer network that “serves to log messages received from individual computers within that computer network indicating detection of malware.” *Ackroyd*, Abstract. For example, “[t]he managing computer detects patterns of malware detection across the network as a whole a[nd] triggers associated predetermined anti-malware actions.” *Id.* The actions “may include forcing specific computers to update their malware definition data, forcing particular computers to change their security settings and isolating individual portions of the computer network.” *Id.*

60. *Ackroyd* provides an exemplary computer network, reproduced below:



Id., Figure 1. In several described embodiments, the managing computer (also referred to therein as the policy organising² server) stores information received from remote computers in a database. *Id.*, 2:56-61. In doing so, “[s]uch an arrangement allows convenient querying of the database, such as automatic running of

² I have been informed that the inventor of Ackroyd, Mr. Robert John Ackroyd, lists a home address in Great Britain. I have also been informed that likely because of this, a few terms in Ackroyd use the British spelling, rather than the American spelling, such as “organising” and “recognising.” Similar to the Petition, rather than using “[sic]” or bracketed changes each time these words appear, I adopt the Petition’s methodology which uses the British spelling of these words where they come from that document.

predetermined queries, in order to detect particular patterns within the logged data messages and trigger appropriate responses.” *Id.* This database can include many types of information related to the security products used by remote computers in the network, including “the malware scanner products being used, the versions of the scanner engines and malware definition data being used, the security settings in force on the computer and the like.” *Id.*, 2:62-67. For example, “[t]his data may be highly useful in identifying patterns within the malware detection reports generated across the computer network to identify weaknesses and vulnerabilities that can be addressed by predetermined anti-malware actions.” *Id.*, 2:67-3:4.

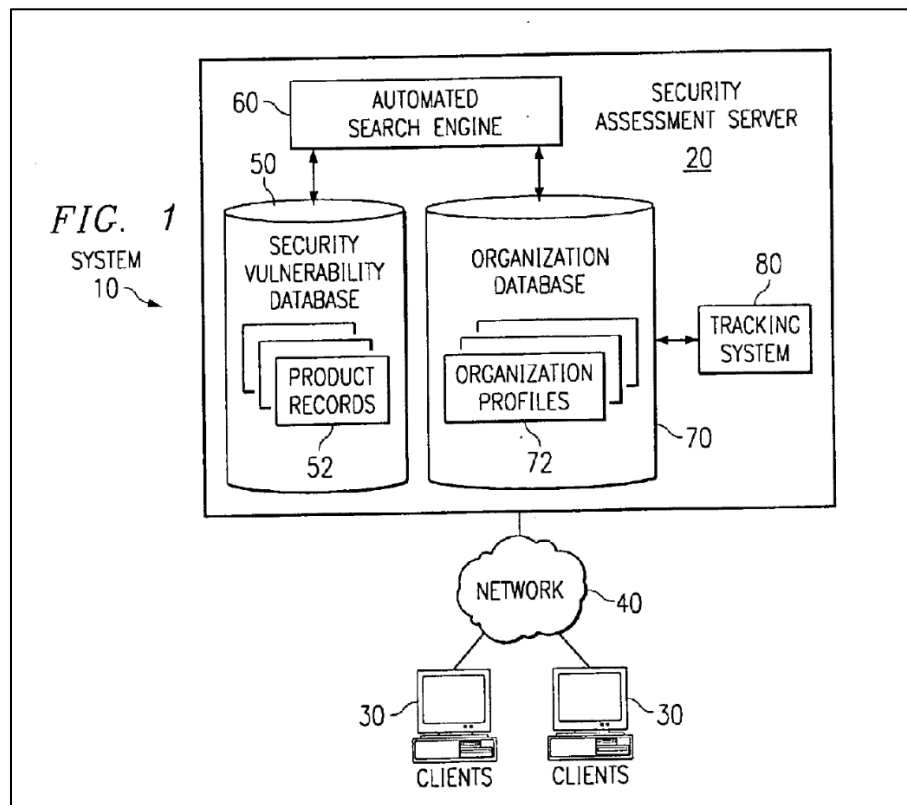
61. A PHOSITA would have recognized *Ackroyd* is in the same field of endeavor as the ’123 Patent. Each of *Ackroyd* and the ’123 Patent are related to methods and apparatus for dealing with malware. *Compare* ’123 Patent, 1:9-10 (“[t]he present invention relates generally to methods and apparatus for dealing with malware”), 1:19-22 (“[t]he term ‘malware’ is used herein to refer generally to any executable computer file or, more generally ‘object,’ that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like”), *with Ackroyd*, 1:6-12 (“this invention relates to the field of malware protection, such as, for example, protection against computer viruses, worms, Trojans, banned files, banned words, banned images etc., upon a network of connected computers”).

62. A PHOSITA would have recognized *Ackroyd* is also directed at solving similar problems to those of the '123 Patent, including malware detection being slow to respond to new forms of malware. The '123 Patent describes a problem with existing malware detection as being slow to respond to new forms of malware, particularly in a network of remote computers. '123 Patent, 1:23-47 (describing existing malware products); 3:14-24 (describing the claimed invention as different from the prior art, and noting that the methods in the '123 Patent allow “a comparison to be made between the objects and/or their effects on the different remote computers to determine whether or not a particular object should be classed as good or as malware. Sophisticated pattern analysis can be carried out. This allows a rapid determination of the nature of the object to be made....”). Like the '123 Patent, *Ackroyd* teaches a solution to the same problem. *Ackroyd*, 1:21-33 (“As computer networks have become more widespread and complex, and the threats posed by newly developed types of malware more sophisticated and potentially damaging, it is important that malware protection is systematically and thoroughly implemented on a computer network. ... Given the threat posed by malware, such as the well known damaging effects of mass-mailing computer viruses, measures that can improve the effectiveness with which such threats can be dealt with are strongly advantageous”).

63. Also, as I discussed in my opinions above, *Ackroyd* was used in EPO rejections as analogous prior art to the EPO counterpart application.

2. *Dahlstrom*

64. *Dahlstrom* (Ex. 1006) is directed to “[a] method for determining security vulnerabilities [that] includes receiving a profile of one or more products used by an organization, the profile including characteristics of each product.” *Dahlstrom*, Abstract. In embodiments, “[t]he method further includes comparing the characteristics of each product to a plurality of product records, each product record including one or more security vulnerabilities associated with the product record and one or more fixes associated with each security vulnerability.” *Id.* *Dahlstrom*’s system is shown below in Figure 1:



Id., Fig. 1. *Dahlstrom*'s "security vulnerability database includes various information about security products used in a network, such that the database can be used to determine vulnerabilities specific to a particular product and to recommend fixes. *Id.*, [0036]-[0073], Figs. 2-10.

65. A PHOSITA would have recognized *Dahlstrom* is in the same field of endeavor as the '123 Patent. Each of *Dahlstrom* and the '123 Patent are related to methods and apparatus for dealing with malware. For example, the '123 Patent states that "[t]he present invention relates generally to methods and apparatus for dealing with malware." '123 Patent, 1:9-10. Further, in the '123 Patent, "[t]he term 'malware' is used herein to refer generally to any executable computer file or, more

generally ‘object’, that is or contains malicious code, and thus includes viruses, Trojans, worms, spyware, adware, etc. and the like.” *Id.*, 1:19-22. Like the ’123 Patent, *Dahlstrom* is in the same field of endeavor, and describes its field of invention as follows: “[t]his invention relates in general to the field of information technology, and more particularly to a system and method for determining security vulnerabilities.” *Dahlstrom*, [0001], [0018].

66. A PHOSITA would have recognized *Dahlstrom* is also directed at solving similar problems to those of the ’123 Patent, including a problem with existing malware detection as being slow to respond to new forms of malware, particularly in a network of remote computers. *See* ’123 Patent, 1:23-47 (describing existing malware products); 3:14-24 (describing the claimed invention as different from the prior art, and noting that the methods in the ’123 Patent allow “a comparison to be made between the objects and/or their effects on the different remote computers to determine whether or not a particular object should be classed as good or as malware. Sophisticated pattern analysis can be carried out. This allows a rapid determination of the nature of the object to be made....”). Likewise, *Dahlstrom* teaches a solution to the same problem. *See Dahlstrom*, [0003] (describing the problem and noting that “organizations are perhaps less prepared than ever to monitor and prevent security vulnerabilities. This is due to both the shear volume of products and the rate at which new products are introduced and/or existing

products modified. Adding to the difficulty of such monitoring and prevention, organizations have also become much more distributed geographically”), [0006] (describing the solution, in part, as “comparing the characteristics of each product to a plurality of product records, each product record including one or more security vulnerabilities associated with the product record and one or more fixes associated with each security vulnerability”).

67. Also, as I discussed in my opinions above, *Dahlstrom* was found analogous art to the ’123 Patent by the Examiner and applied in rejections in U.S. prosecution.

G. Opinions Regarding Ground 1: *Ackroyd* Renders Claims 1, 3-4, and 6-16 Obvious

1. *Claim 1*

(a) *1[Pre]. A method comprising:*

68. *Ackroyd* discloses systems and methods for managing malware protection in a computer network. *Ackroyd*, Abstract, 1:7-12, 1:41-58, claim 14 (“**A method** of managing malware protection...”).

(b) *[1(a)] receiving, at a base computer, details uniquely identifying one or more security products operating at a point in time on a remote computer;*

69. I have been asked to apply PO’s plain meaning of limitations 1(a) through 1(e), such that no particular order is required by these limitations. I express no opinion concerning the correctness of PO’s interpretation.

70. *Ackroyd* teaches that its systems and methods include receiving information at a base computer, which is referred to therein as a “malware policy organising server.” The information received includes details uniquely identifying one or more security products operating at a point in time on a remote computer, as explained in further detail below.

71. For instance, *Ackroyd* describes a “malware policy organising server 32” connected in computer network 2 which “serves to monitor and enforce security settings on all of the computers within the computer network 2.” *Ackroyd*, 3:40-44. I note that the ’123 Patent describes that its remote computers can be any device for loading and operating computer objects, including a server. ’123 Patent, 7:64-8:1 (“The computers 2 may each be variously a personal computer, a server of any type, a PDA, mobile phone, an interactive television, or any other device capable of loading and operating computer objects”). The ’123 Patent also describes the “base” computer 3 as a “central” computer and provides examples of known in the art central computers, which include central servers. ’123 Patent, 7:63-65; *see also id.*, 1:65-2:51. For example, U.S. Patent No. 6,944,772 to Dozortsev (“*Dozortsev*”) described in the ’123 Patent uses a “central computer” and a “central server” interchangeably. Ex. 1009 (*Dozortsev*), 3:22-39, 5:65-6:1, 7:44-47, claim 37. Further, EP 1549012 to De Spiegeleer (“*Spiegeleer*”) also discussed in the ’123 Patent generally describes similar base computer functions occurring on a central

server. Ex. 1010 (*Spiegeleer*), [0004], [0007], [0040]-[0041]; *see also* EP 1280040 (“*Hinchliffe*”) (Ex. 1011), [0016], Fig. 3 (disclosing the same); WO 02/33525 (“*Chuang*”) (Ex. 1012), Fig. 1 (same); US 2004/0073810 (“*Dettinger*”) (Ex. 1013), Fig. 1 (same); WO 03/021402 (“*Duke*”) (Ex. 1014), Abstract (same).

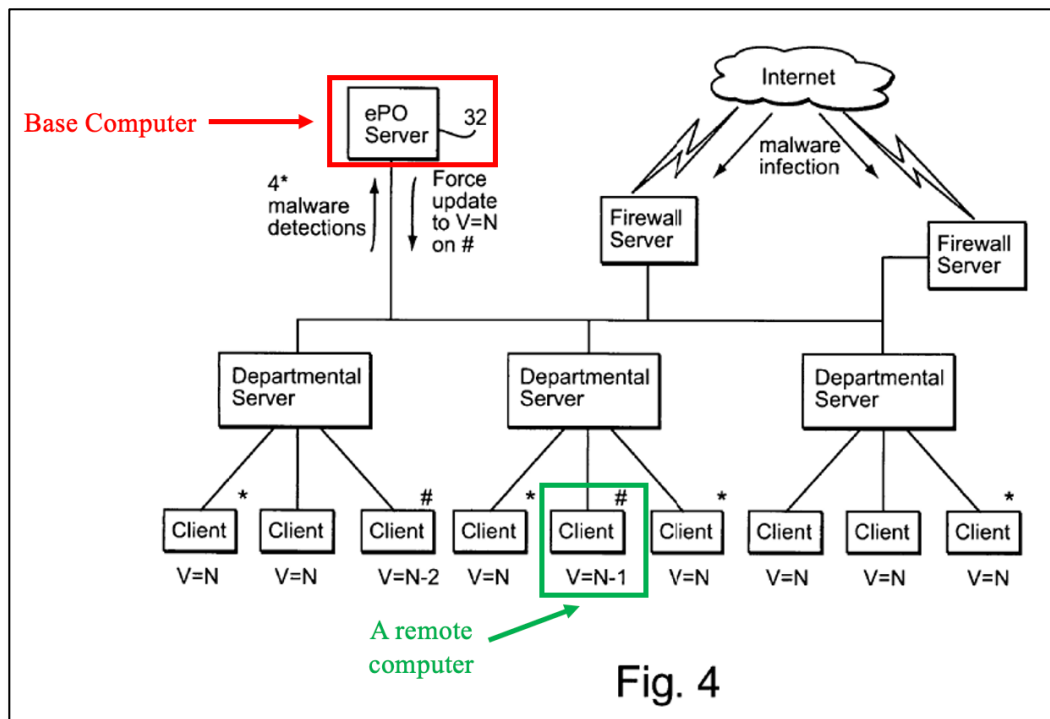
72. I also note that during prosecution the Examiner found the claimed “base computer” disclosed by Dahlstrom’s “Security Assessment Server 20.” ’123 File History, 95-96. Given these disclosures, and based on my knowledge and experience through years of working with malware systems, a PHOSITA would have understood the plain meaning of “base computer” would also include a server, especially as it is well understood that a server is a computer.

73. *Ackroyd* further discloses that “[t]he policy organising server 32 [] serves to receive logged data messages from the various different servers and client computers within the computer network 2 indicating detection of malware items by the malware scanners operating at those individual computers.” *Ackroyd*, 3:44-49.

74. Importantly, the policy organising server 32 “also receives status information from the various computers indicating **the malware scanning products being used, the scanner engine versions and virus definition data versions being used and the security settings being applied within those different computers on the network.**” *Ackroyd*, 3:40-54 (emphasis added); *see also id.*, 2:62-3:4, 3:64-4:23; 4:43-5:39. A PHOSITA would have understood that the teachings of *Ackroyd*

disclose *details uniquely identifying one or more security products* as required by the '123 Patent. For example, as claimed in claim 3, example details which uniquely identify a security product include “the name of the security products, versions, and loaded signature files.” '123 Patent, claim 3. Consistent with this disclosure, as explained above, *Ackroyd's* policy organising server 32 receives name and version details of the malware scanning products being used at the point in time the data was transmitted. *Ackroyd* explains that “[t]his data may be highly useful in identifying patterns within the malware detection reports generated across the computer network to identify weaknesses and vulnerabilities that can be addressed by predetermined anti-malware actions.” *Ackroyd*, 2:62-3:4.

75. The above-mentioned information is collected in an “SQL database maintained by the policy organising server 32.” *Id.*, 3:60-63. The policy organising server 32 (i.e., *base computer*) is shown below, boxed in red, in the exemplary computer network, along with a remote client computer, boxed in green:

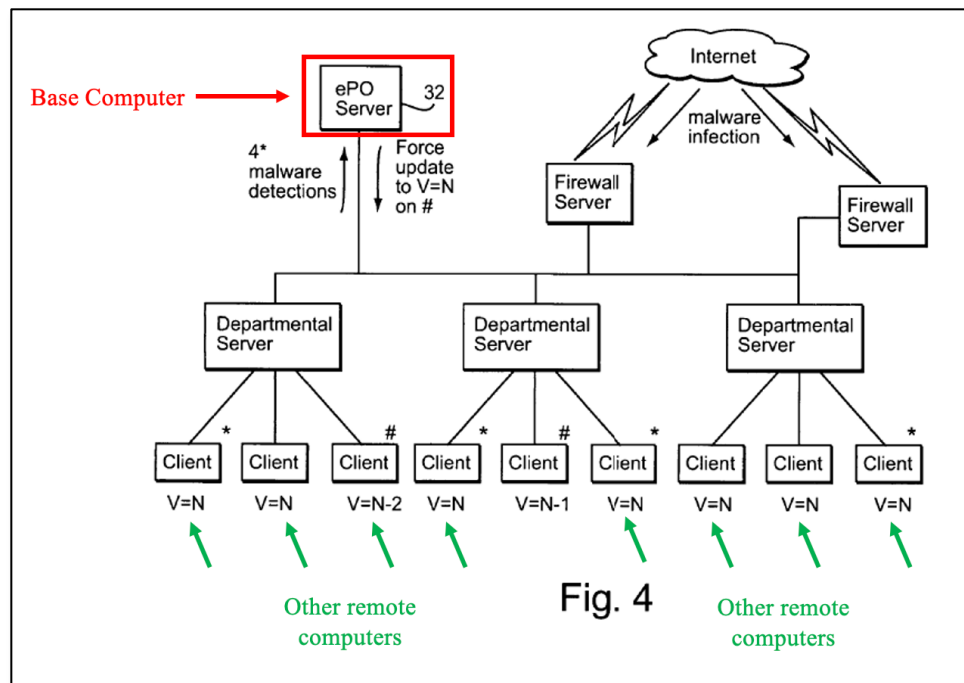


Id., Fig. 4;³ see also *id.*, Figs. 1-3, 5-7.

- (c) *[1(b)]* receiving, at the base computer, details uniquely identifying one or more security products operating on other remote computers in communication with the base computer;

76. As I described above in my opinions concerning claim 1(a), *Ackroyd* discloses receiving status information from several remote computers in communication with the base computer in a computer network. See above, Claim 1(a). I have provided an exemplary figure below showing base computer 32 receiving status information from “other remote computers”:

³ All annotations added.



Id., Fig. 4. As shown above, Figure 4 depicts multiple “other remote computers” in addition to the remote computer identified in claim 1(a) above (which was boxed in green) with green arrows pointing to these other remote computers. As above, the base computer receives status information from each of these remote computers, including: **“the malware scanner products being used, the versions of the scanner engines and malware definition data being used, the security settings in force on the computer and the like.”** *Id.*, 2:62-3:4 (emphasis added); *see also id.*, 3:40-54; 3:64-4:23; 4:43-5:39.

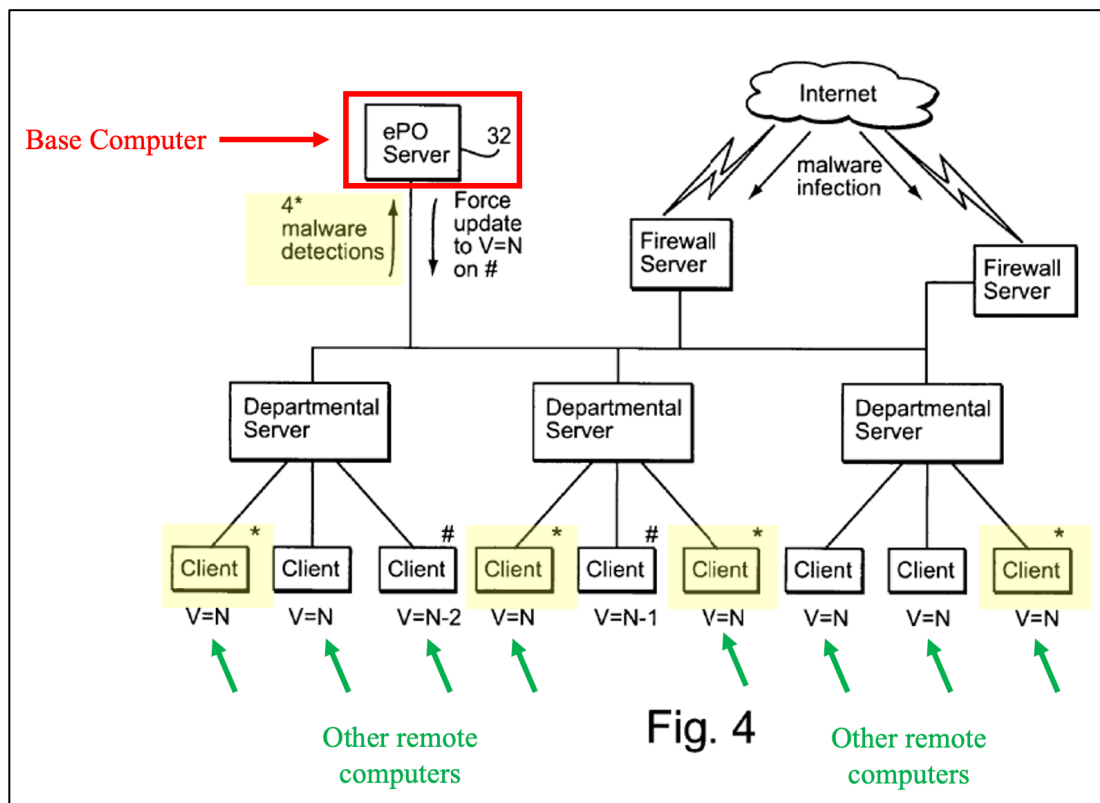
- (d) *[1(c)] receiving, at the base computer, details of a process that has been executed by at least one of the other remote computers;*

77. *Ackroyd* discloses that its policy organising server receives additional information from at least one of the other remote computers (e.g., client computer V=N with up-to-date malware definition data), including a malware detection event which identifies a detected malware process. From this reported information, the policy organising server determines that the same malware process has been executed by at least one of the other remote computers (e.g., client computer V=N-2 with outdated malware definition data).

78. For example, to detect malware events, *Ackroyd* discloses that “[i]n preferred embodiments of the invention, the network connected computers will typically run their own malware scanners and these malware scanners will preferably use malware definition data to identify the items of malware to be detected.” *Id.*, 2:36-40. As an example, the malware scanners “detect a particular Trojan infection and make reports of this to the policy organising server 32.” *Id.*, 5:26-29; *see also id.*, 4:39-60 (discussing process for malware detection of a “malware infection [] received into the network from the internet” that is “spread within the computer network”), 4:65-67 (detecting “occurrences of internet traffic infected with a particular item of malware”), 5:7-9 (describing detection of malware-related “events”), Fig. 2 (depicting detection and logging of malware events).

79. After malware is detected by certain client computers, *Ackroyd* discloses that the policy organising server “serves to receive logged data messages from the various different servers and client computers within the computer network 2 indicating detection of malware items by the malware scanners operating at those individual computers.” *Ackroyd*, 3:44-49.

80. For example, Figure 4 below displays an exemplary embodiment where the base computer receives this malware detection data from other remote client computers identified with “*” (highlighted yellow):



Id., Fig. 4. In this figure, there were “4*” malware detections by remote computers with up-to-date V=N malware definition data. *Id.*, 4:39-60.

81. In more detail, with respect to Figure 4, *Ackroyd* discloses that “a malware infection is received into the network from the internet” and “starts to spread within the computer network.” *Id.*, 4:39-42. “Those computers running the most up-to-date version of the virus definition data (indicated by $V=N$) detect this malware infection and take appropriate anti-malware action themselves as well as issuing a log data message back to the policy organising server 32.” *Id.*, 4:43-47. In contrast, “[t]he computers within the network running out-of-date malware definition data (indicated by $V=N-1$ or $V=N-2$) do not detect the malware infection and do not give rise to any logged data messages sent back to the policy organising server.” *Id.*, 4:47-51.

82. Based on *Ackroyd's* disclosures, a PHOSITA would have understood or found obvious that *Ackroyd's* client computers with scanners having up-to-date malware definition data ($V=N$) would identify malware processes and report their associated details to the policy organising server. From the reported information, the policy organising server determines that the same malware process was executed at other remote computers with out-of-date definition data, such as client computer with definition data $V=N-2$. *Ackroyd*, 4:47-60 (disclosing that the policy organising server “detects that none of [the event detection messages] originate from a computer running out-of-date malware definition data” and compares received messages to a “predetermined threshold” to force anti-malware actions). In this way, the remote

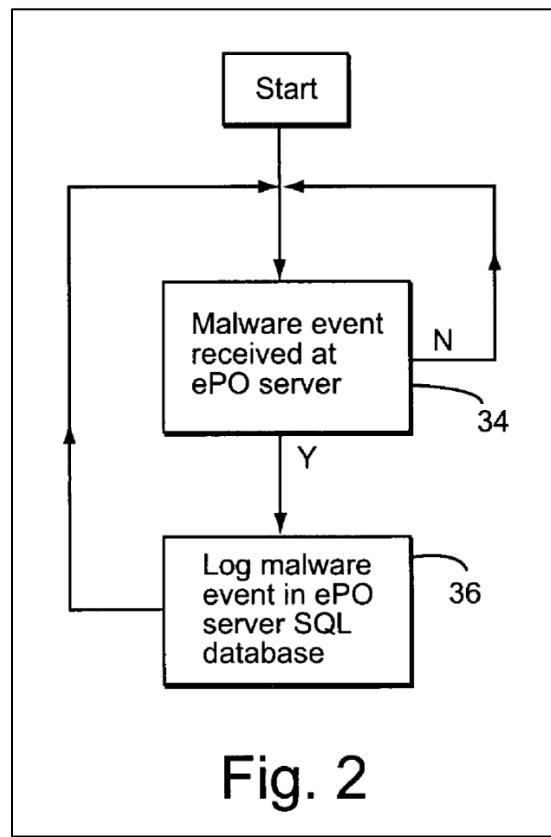
computers with V=N definition data are sending details of malware processes executing on other less protected remote computers to the base computer as malware event data. Indeed, those remote computers with outdated scanners would not identify malware, and therefore would not trigger anti-malware actions which would allow malware to execute processes thereon.

83. In other words, remote computers with definition data V=N would detect malware starting to spread through the network, including, for example, a Trojan infection as it spreads and executes on the other remote computer with outdated definition data, and these remote computers with V=N definition data send malware event data related to this infection to the base computer. *Ackroyd*, 4:39-60; *see also id.*, 3:44-55 (discussing scanners with updated malware definition data detecting malware processes). It was well-known that Trojan infections execute potentially malicious processes. For example, U.S. Patent Application No. 2003/0115479 to Edwards et al. (“*Edwards*”) (Ex. 1015), which relates to a known system for detecting malware, describes that “a Trojan horse program is typically a destructive program that masquerades as a benign application. Unlike a virus, Trojan horses do not replicate themselves but they can be just as destructive. One insidious type of Trojan horse is a program that claims to rid a computer of malwares but instead introduces malwares onto the computer.” *Edwards*, [0015]. *Edwards* system notes that these programs execute potentially malicious processes, and its system

detects these processes and halts them if malware is detected. *Id.*, [0016]-[0021]; *see also id.*, [0009], Claim 11, Claim 23, and Claim 35, Figs. 2, 4.

84. Therefore, when *Ackroyd's* remote computers with V=N definition data send malware event data related to a Trojan infection executing on remote computers with outdated definition data, these remote computers with updated definition data are sending “*details of a process*” executed by those remote computers with outdated products.

85. After the detection of a malware process, the malware event data is sent to the policy organising server 32. The process for capturing and sending a malware event is depicted below in Figure 2:



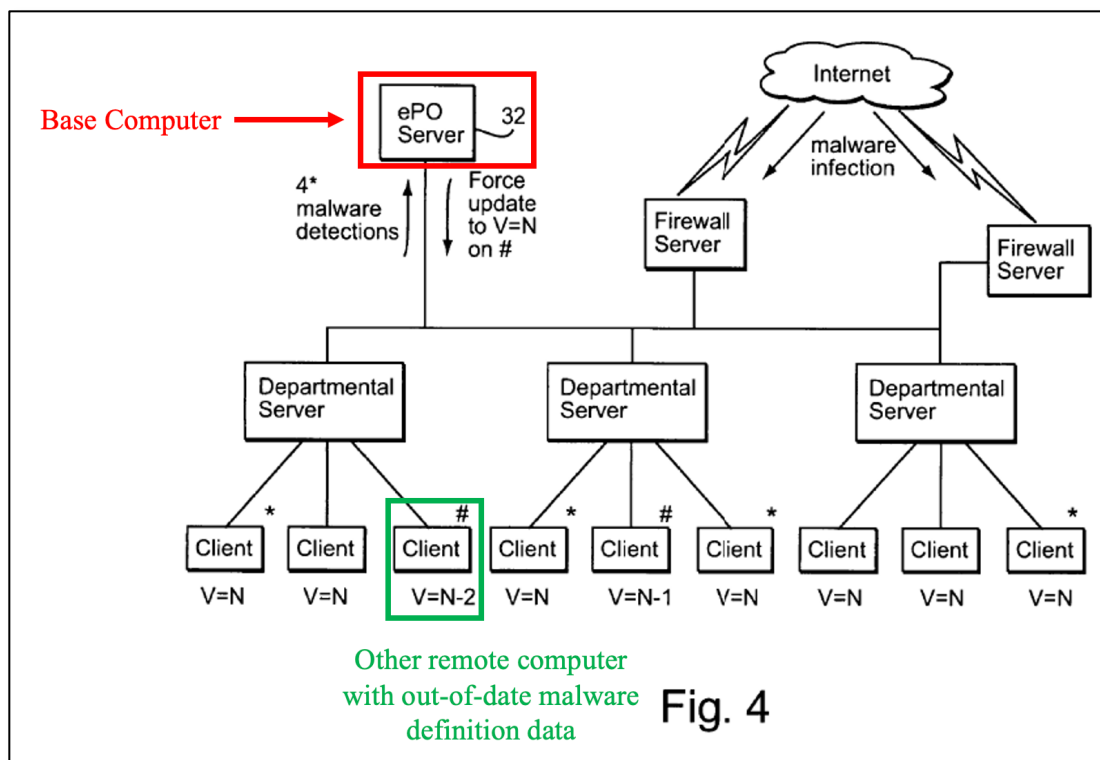
Id., Fig. 2. Further, describing Figure 2, *Ackroyd* discloses that:

FIG. 2 illustrates the action of the policy organising server 32 in receiving logged data messages. **At step 34 the policy organising server 32 waits to receive a malware detection event message from one of the various computers it is managing. When such an event is received, processing proceeds to step 36 at which it is logged within an SQL database maintained by the policy organising server 32. Processing then returns to step 36.**

Id., 3:56-63 (emphasis added).

- (e) [1(d)] determining, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers; and

86. *Ackroyd* discloses that its base computer determines that a process is malware not identified by one or more security products on a remote client computer. This malware determination process is described with reference to Figure 4, as shown below:



Ackroyd, Fig. 4.

87. With respect to this figure, *Ackroyd* discloses:

FIG. 4 schematically illustrates a pattern of malware detections and an associated anti-malware action. First of all a malware infection is received into the network from the internet. This starts to spread within the computer network. Those computers running the most up-to-date version of the virus definition data (indicated by $V=N$) detect this malware infection and take appropriate anti-malware action themselves as well as issuing a log data message back to the policy organising server 32. The computers within the network running out-of-date malware definition data (indicated by $V=N-1$ or $V=N-2$) do not detect the malware infection and do not give rise to any logged data messages sent back to the policy organising server. **When the policy organising server 32 has detected four logged data messages corresponding to the particular item of malware [identified with “*”] and also detects the pattern that none of these originate from a computer running out-of-date malware definition data [identified with “#”],** the policy organising server 32 recognises the exceeding of a predetermined threshold in combination with a predetermined pattern of infection and serves to force the anti-malware action of updating the malware definition data on those computers that are out-of-date.

Id., 4:39-60 (emphasis added); *see also id.*, 5:7-12 (noting further that malware detection events in excess of a threshold on one scanner with no events on another can “indicate[] that this different malware scanner for some reason is not identifying the malware threat concerned”).

88. Based on the disclosures in *Ackroyd*, the “policy organising server” (*base computer*) receives logged data messages from remote client computer $V=N$ with details of processes executed by remote client computers $V=N-1/V=N-2$ with out-of-date malware definition data (i.e., *the received details of the process that has been executed by the least one of the other remote computers*). Then, the policy organising server determines the processes were not detected by remote client

computers V=N-1 and V=N-2 with out-of-date malware definition data (i.e., *not identified by the one or more security products operating on the at least one of the other remote computers*). And the policy organising server determines these processes were malware based on the received data (i.e., *determining, by the base computer and based on the received details...that the process is a malware process*). *See id.*, 4:39-60; *see also id.*, 4:61-5:12 (describing the process in the context of a firewall server); 5:26-39 (describing the process in the context of isolating a departmental server and related remote computers); Figs. 5-6. A PHOSITA would have understood *Ackroyd* discloses the requirements of the claim limitation “determining, by the base computer and based on the received details...that the process is a malware process.” *See id.* To make this malware determination, the policy organising server generates reports from the malware event data, compares these reports to thresholds, and if a threshold is exceeded, initiates predefined anti-malware actions. *Id.*; 3:64-4:38, Fig. 3.

- (f) *[1(e)] determining, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer.*

89. As I discussed in my opinions above, *Ackroyd* discloses that the policy organising server determines that remote computers with out-of-date security

products are vulnerable to a specific malware process. This determination is based on an overall assessment of the network, including computers with up-to-date security products and one or more computers with the same or similar vulnerability due to out-of-date security products.

90. For instance, *Ackroyd* discloses:

FIG. 4 schematically illustrates a pattern of malware detections and an associated anti-malware action. First of all a malware infection is received into the network from the internet. This starts to spread within the computer network. Those computers running the most up-to-date version of the virus definition data (indicated by $V=N$) detect this malware infection and take appropriate anti-malware action themselves as well as issuing a log data message back to the policy organising server 32. **The computers within the network running out-of-date malware definition data (indicated by $V=N-1$ or $V=N-2$) do not detect the malware infection and do not give rise to any logged data messages sent back to the policy organising server.** When the policy organising server 32 has detected four logged data messages corresponding to the particular item of malware and also detects the pattern that none of these originate from a computer running out-of-date malware definition data, the policy organising server 32 recognises the exceeding of a predetermined threshold in combination with a predetermined pattern of infection and serves to **force the anti-malware action of updating the malware definition data on those computers that are out-of-date.**

Id., 4:39-60 (emphasis added). In this disclosure, the policy organising server determines that the remote computer (client computer $V=N-1$) is vulnerable to this malware process based on having out-of-date malware definition data, similar to the remote computer (client computer $V=N-2$) which also has out-of-date malware definition data, and both of which did not detect a malware event. Thus, this

determination is based, at least in part, on at least one of the other remote computers (client computer V=N-2) having similar out-of-date malware definition data (i.e., an older version of the security product).

91. Depending on the output of the vulnerability determination, *Ackroyd* describes forcing an update of the security products on the vulnerable computers. *Id.*; *see also id.*, 4:61-5:12 (describing the process in the context of a firewall server); 5:26-39 (describing the process in the context of isolating a departmental server and related remote computers); Figs. 4-6.

2. *Claim 3 - The method according to according to claim 1, wherein the details of the one or more security products includes the name of the security products, versions, and loaded signature files.*

92. As I described in my opinions concerning claim 1 above, *Ackroyd* discloses the method of claim 1. *See above*, Claim 1. As I described above, *Ackroyd* discloses sending details of one or more security products to the base computer 32.

As part of these details, *Ackroyd* discloses:

The database may also advantageously store other information concerning the computers within the computer network relating to their malware protection, such as **the malware scanner products** being used, the **versions** of the scanner engines and **malware definition data** being used, the security settings in force on the computer and the like. This data may be highly useful in identifying patterns within the malware detection reports generated across the computer network to identify weaknesses and vulnerabilities that can be addressed by predetermined anti-malware actions.

Ackroyd, 2:62-3:4 (emphasis added). In *Ackroyd*, the database includes, among other things, “malware protection mechanisms[,]” “versions of malware protection[,]” versions of malware definition data[,]” and “security settings of malware protection mechanisms”). *Id.*, Claim 8.

93. To the extent Patent Owner or its expert argues that *Ackroyd* does not use the word “name” or the words “signature files,” a PHOSITA would have understood that when information about “the malware scanner products being used” is sent to the base computer, to identify the specific malware scanner product, this would include the name of those products. Or, at a minimum, it would have been obvious to include the name of the malware scanner product to identify the specific “malware scanner products being used.”

94. A PHOSITA would have also understood that the virus/malware definition data disclosed in *Ackroyd* would include signature file information as claimed. Indeed, it was known that “definition data” is made up of signature files. For example, U.S. Patent No. 6,663,000 to Muttik et al. (“*Muttik*”) (Ex. 1017) uses malware definition data that “can include program code operable to utilize the validating data 32 embedded within the malware definition data 24 for checking the signature 26 of the malware scanner engine 22.” *Muttik*, Abstract. As another example, *Muttik* describes that “[a] further aspect of the invention provides a malware definition data component of a malware scanner, **said malware definition**

data component comprising signature data[.]” *Muttik*, 3:57-60; *see also id.*, 4:61-

63. Thus, a PHOSITA would have understood that *Ackroyd*’s malware definition data includes *loaded signature files*, as was well-known in the art.

3. *Claim 10 - The method according to claim 3, wherein the details of all or selected security products further includes settings at a particular point in time.*

95. As I described in my opinions above, *Ackroyd* discloses the method of Claim 3. *See above*, Claim 3. As I noted above, *Ackroyd* discloses that:

The database may also advantageously store other information concerning the computers within the computer network relating to their malware protection, such as the malware scanner products being used, the versions of the scanner engines and malware definition data being used, **the security settings in force on the computer and the like**. This data may be highly useful in identifying patterns within the malware detection reports generated across the computer network to identify weaknesses and vulnerabilities that can be addressed by predetermined anti-malware actions.

Ackroyd, 2:62-3:4, claim 8 (claiming “security settings of malware protection mechanisms used by respective network connected computers” stored in the database). A PHOSITA would have understood the security settings stored with respect to the client computers “in force on the computer” relates to settings at a particular point in time. Namely, the point in time that information was sent in the logged data message.

4. Claim 11 - The method according to claim 1, further comprising: identifying, by the base computer, one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the at least one of the other remote computers; and determining, by the base computer, that the identified one or more of the other remote computers having the same or similar combination of security products as the combination of security products operating on the at least one of the other remote computers is vulnerable to the malware process.

96. As I discussed in my opinions above concerning claim 1, *Ackroyd* discloses the method of Claim 1. *See above*, Claim 1. Additionally, referring back to Figure 4 above, *Ackroyd* discloses that the policy organising server 32 detects “four logged data messages corresponding to the particular item of malware” and also detects “that none of these originate from a computer running out-of-date malware definition data[,]” such as client computers running software V=N-1 and V=N-2. *Ackroyd*, 4:43-60. A PHOSITA would have understood, based on the disclosures in *Ackroyd*, that the policy organising server identifies that V=N-1 and V=N-2, the two remote computers which did not detect the malware event, have similar out-of-date software. *Id.* After the prior step, “the policy organising server 32 recognises the exceeding of a predetermined threshold in combination with a predetermined pattern of infection and serves to force the anti-malware action of updating the malware definition data on those computers that are out-of-date.” *Id.*, 4:43-60. In doing so, the policy organising server determines that each of client

computers running software V=N-1 and V=N-2 are vulnerable to the malware process and prompts an update to resolve this vulnerability. Indeed, the system is aware of the security products operating on the remote computers, and the system can also determine vulnerabilities based on this information, such as old versions of malware detection data not identifying a malware infection affecting the network.

5. Claim 14 - The method according to claim 1, wherein the one or more security products include a firewall product and an antivirus product.

97. As I described in my opinions above concerning claim 1, *Ackroyd* discloses the method of Claim 1. *See above*, Claim 1. Moreover, *Ackroyd* discloses that its malware detection products (e.g., scanners) can include “internet traffic scanning” and can detect “Trojan[s].” *See, e.g., Ackroyd* 2:45-49, 5:26-29 (describing scanner detecting a “Trojan”), Figs. 4-6. A PHOSITA would have understood or found obvious that to conduct internet traffic scanning, including scanning for Trojans, *Ackroyd’s* scanners would employ a known in the art firewall product. Indeed, numerous firewall products were well-known by June 30, 2005, the priority date I have applied for the Challenged Claims of ’123 Patent for my opinions herein. For example, “PC broadband security” by Darren Meyer (Ex. 1018) describes that “[m]ost major anti-virus vendors also offer some sort of software firewall, such as Norton Personal Firewall from Symantec Corporation or Personal Firewall Plus from McAfee Security. These firewalls can be quite useful, offering

everything from port filtering to blocking certain IP addresses. They can also control what programs on your computer actually are able to access the Internet, such as blocking Windows from accessing the Internet in the background without your knowledge.” Ex. 1018, 3.

98. A PHOSITA would have been motivated to use any of these well-known firewall products in *Ackroyd*’s scanners to accomplish the “internet traffic scanning” functions because this is simply combining prior art elements according to known methods to yield predictable results. Further, *Ackroyd* notes that these scanners can be “alter[ed]” to “perform[] more thorough malware scanning.” *Ackroyd*, claim 4. A PHOSITA would have understood that the firewall product (and antimalware product described below) would provide means for more thorough scanning. And a PHOSITA would have had success implementing these known products in *Ackroyd*’s scanners, particularly when these scanners are already programmed to scan for “internet traffic.”

99. Additionally, *Ackroyd* discloses its “invention relates to the field of malware protection, such as, for example, protection against computer viruses” *Ackroyd*, 1:8-10, 1:59-2:35 (describing “anti-malware” products in the context of computer viruses), 4:39-60 (same). A PHOSITA would have understood or found obvious that the scanners would additionally include an antivirus product to protect against computer viruses as disclosed in *Ackroyd*. Indeed, just as above, numerous

antivirus products were well-known by June 30, 2005. For example, “PC broadband security” further describes that “the first piece of software to install is some type of anti-virus software. The more popular ones include Symantec’s Norton Antivirus and McAfee Security’s VirusScan. These software packages are typically reasonably priced.” Ex. 1018, 2. As another example, “Anti-virus software” by Ralph Lee Scott (Ex. 1019) supports that Symantec’s Norton Antivirus and McAfee’s VirusScan antimalware products were well-known in the art before June 30, 2005. Ex. 1019, 1 (noting the “standard method” to “prevent the spread of viruses” was to “install, and run anti-virus software such as Symantec/Norton AntiVirus or McAfee VirusScan”).

100. Like above, a PHOSITA would have been motivated to use any of these well-known antivirus products in *Ackroyd’s* scanners to facilitate *Ackroyd’s* “protection against computer viruses.” Likewise, a PHOSITA would have had success implementing these known products in *Ackroyd’s* scanners to accomplish *Ackroyd’s* express goals.

H. Opinions Regarding Ground 2: *Ackroyd* in View of *Dahlstrom* Renders Claims 2 and 5 Obvious

1. *Claim 2 - The method according to claim 1, further comprising: providing information to the user of the remote computer that the remote computer may be susceptible to attack by the malware processes.*

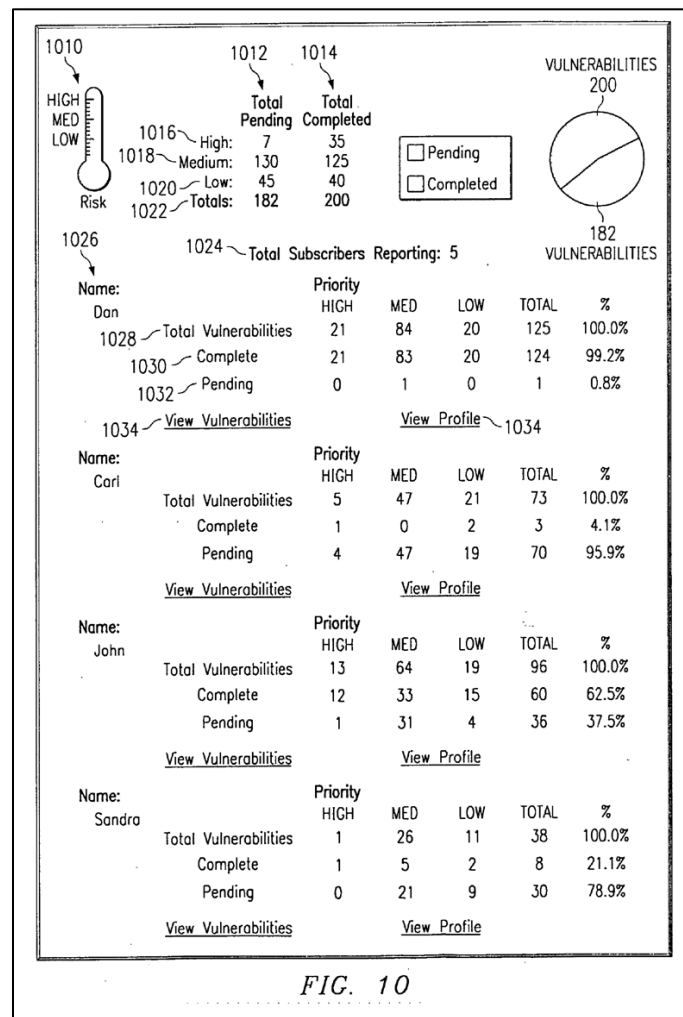
101. As I discussed in my opinions above concerning claim 1, *Ackroyd* discloses the method of Claim 1. *See above*, Claim 1. Additionally, *Ackroyd*

discloses “[t]he results of the processing performed” related to malware and vulnerability determinations “may be **displayed to a user** via the display driver 212 and the monitor 214.” *Ackroyd*, 5:52-54; *see also id.*, 3:64-4:13 (disclosing the system will “run various queries/**reports** (these terms are used generically to indicate mechanisms for retrieving specified data from a database and **presenting it to a user** rather than implying the use of any particular software or display/data format)...”). Accordingly, a PHOSITA would have understood that *Ackroyd* discloses means by which a user is provided information that the remote computer may be susceptible to attack by the malware processes (e.g., by a Trojan infection spreading through the network). Those means being a report presented to the user via display driver 212 and monitor 214.

102. I understand, however, that the EPO found that *Ackroyd*’s teachings here were unconvincing. To the extent it is argued or found that *Ackroyd*’s disclosures are insufficient, in my opinion, it would have been obvious to combine *Dahlstrom*’s vulnerability data outlined in its generated report with the report presented to the user in *Ackroyd*. For example, *Dahlstrom* discloses “a tracking report generated by the tracking system 80[,]” which includes both a risk thermometer and also “vulnerability tracking categories of 1012 and 1014, corresponding to pending vulnerabilities that have not been neutralized or otherwise addressed and completed vulnerabilities that have been neutralized or otherwise

addressed, respectively.” *Dahlstrom*, [0071]. *Dahlstrom* also explains that “[t]he tracking report [] breaks down the overall vulnerabilities of an organization into vulnerabilities under the scope or direction of individuals or subscribers within the organization.” *Id.*, [0072]. That way, “a supervisor or IT manager can easily access, monitor, and track the efforts of individuals within an organization to neutralize or otherwise address vulnerabilities.” *Id.* As described in *Dahlstrom*, these tracking reports and other risk assessments can be retrieved from, and provided to, the user of the remote computer. *See, e.g., id.*, [0019], [0021], [0037]-[0038], [0049]-[0052].

103. I provide below an exemplary tracking report as disclosed in *Dahlstrom*:



Dahlstrom, Fig. 10.

104. It would have been obvious for a PHOSITA to incorporate *Dahlstrom*'s vulnerability data associated with certain product configurations outlined in the tracking report with the report disclosed in *Ackroyd* that is already being presented to the user. *Dahlstrom* provides a broader range of implementation details, but the concepts from the two references are the same—information about the network and its exposure to possible malware is communicated to users. A PHOSITA would have

been motivated to make this combination because the implementation details described and illustrated in the tracking report from *Dahlstrom* would be useful in communicating the necessary information from the system processing that is described in *Ackroyd*. Indeed, there is express motivation in the references themselves for this combination. For instance, *Ackroyd* describes determining that a computer is vulnerable to a malware attack. *See, e.g., Ackroyd*, 4:43-60. And *Ackroyd* describes communicating this information to a user. *See, e.g., id.*, 5:52-54. Further, *Ackroyd* discloses that its reports “may be configured and enhanced by individual users to tailor them to their particular networks[.]” *Id.*, 4:9-17. Thus, it would have been obvious to a PHOSITA to configure and/or enhance *Ackroyd*’s report to include the vulnerability data in the tracking report described in *Dahlstrom*. Further, this would have required only combining prior art reports according to known methods to predictable yield a report presented to the user identifying vulnerabilities to malicious processes.

105. I additionally note that this is an obvious design choice, and would accomplish the goals that are already described in *Ackroyd*. Moreover, a PHOSITA would have appreciated success making this simple modification as it would have required simple reprogramming and reformatting of a report already generated and presented to a user, per *Ackroyd*’s express teachings which explain these reports are broadly configurable and can be tailored for certain needs.

IV. CONCLUSION

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

Date: July 12, 2023



By: _____
Dr. Markus Jakobsson

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; Kecker & Van Nest). Details and references upon request.
- **Publications.** Books: *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* (Wiley, 2006); *Crime-ware: 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. 157–173.
- [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/](http://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-phishing 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, Procédé et appareil permettant d'assurer la sécurité d'utilisateurs de dispositifs à capacités bluetooth, WO 2002019641 A2, 2001.
- [214] Robert M. Arlein, Ben Jai, Markus Jakobsson, Fabian Monroe, 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 Monroe, 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 Monroe, 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.