

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

CROWDSTRIKE, INC.  
Petitioner

v.

WEBROOT INC.  
Patent Owner

---

Case No. IPR2023-01052  
Patent No. 8,201,243

---

**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 '243 Patent .....                                                                                                                                                                                                                                                                                                                                                                                                                                       | 21 |
| B.   | Overview of the '243 Patent's File History .....                                                                                                                                                                                                                                                                                                                                                                                                                        | 22 |
| C.   | Level of a Person Having Ordinary Skill in the Art .....                                                                                                                                                                                                                                                                                                                                                                                                                | 23 |
| D.   | Claim Construction .....                                                                                                                                                                                                                                                                                                                                                                                                                                                | 24 |
| E.   | Summary of the Prior Art References.....                                                                                                                                                                                                                                                                                                                                                                                                                                | 25 |
|      | 1. Gladstone .....                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 25 |
|      | 2. Muttik.....                                                                                                                                                                                                                                                                                                                                                                                                                                                          | 28 |
|      | 3. Pantuso.....                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 29 |
|      | 4. English .....                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 30 |
| F.   | Opinions Regarding Ground 1: Claims 1-3, and 5-14 are rendered obvious by <i>Gladstone</i> in view of <i>Muttik</i> or <i>Gladstone</i> in view of <i>Muttik</i> in further view of <i>Pantuso</i> .....                                                                                                                                                                                                                                                                | 31 |
|      | 1. Claim 1.....                                                                                                                                                                                                                                                                                                                                                                                                                                                         | 31 |
|      | 2. Claim 2 –...wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.....                                                                                                                                                                                                                                                                                                   | 67 |
|      | 3. Claim 3 –...wherein the identifying includes accessing an activity log that includes information that relates the activity to the suspected pestware object. ....                                                                                                                                                                                                                                                                                                    | 68 |
|      | 4. Claim 6(c) – a research portion configured to access, in response to a prompt from the heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is configured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received; and..... | 69 |

|                                                                                                                                                                                                                                                                                                                                                                                                     |    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| 5. Claim 6(d) – a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware..... | 74 |
| 6. Claim 7 –...wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file..... | 75 |
| 7. Claim 9 –...wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer. ....                                                                                                                                                                                                                  | 77 |
| G. Opinions Regarding Ground 2: <i>Gladstone</i> in View of <i>Muttik</i> and <i>English</i> , or Alternatively, <i>Gladstone</i> in View of <i>Muttik</i> , <i>Pantuso</i> , and <i>English</i> renders Claims 1-8 and 10-14 Obvious .....                                                                                                                                                         | 78 |
| Claim 4 –...wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the file .....                                                                                                                                                                                                                       | 78 |
| IV. Conclusion .....                                                                                                                                                                                                                                                                                                                                                                                | 82 |

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. 8,201,243 (the “*243 Patent*”) (Ex. 1001). I understand that the Challenged Claims are claims 1-14 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. 8,201,243 (“*243 Patent*”)
- Exhibit 1002 – File History of U.S. Patent No. 8,201,243 (“*243 FH*”)
- Exhibit 1004 – U.S. Patent No. 7,979,889 to Gladstone et al. (“*Gladstone*”)
- Exhibit 1005 – U.S. Patent No. 6,775,780 to Muttik (“*Muttik*”)
- Exhibit 1006 – U.S. Patent No. 7,093,292 to Pantuso (“*Pantuso*”)
- Exhibit 1007 – U.S. Patent No. 8,321,910 to English et al. (“*English*”)
- Exhibit 1008 – *Responsive Markman Brief*
- Exhibit 1010 – *Device Drivers for Windows*

- Exhibit 1011 – US Patent Appl Publ No 2007/0174911 to Kronenberg et al. (“*Kronenberg*”)
- Exhibit 1012 – U.S. Patent Appl Publ No 2006/0253584 to Dixon et al. (“*Dixon*”)
- Exhibit 1013 – U.S. Patent No. 7,434,261 to Costea et al. (“*Costea*”)
- Exhibit 1014 – U.S. Patent No. 8,117,659 to Hartrell et al. (“*Hartrell*”)

**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.

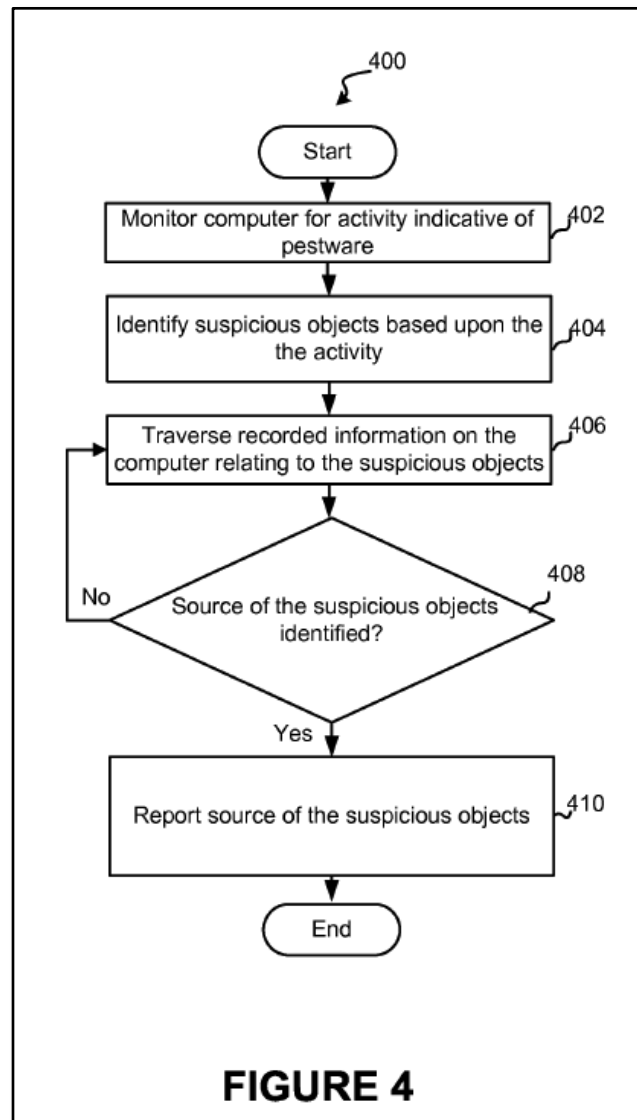
37. I am further informed that secondary considerations evidence is only relevant if the offering party establishes a connection, or nexus, between the

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 '243 Patent

38. The '243 Patent describes “systems and methods for detecting, controlling and/or removing pestware.” *'243 Patent* (Ex. 1001), 1:35-38. The '243 Patent describes “pestware” as software that “collects information about a person or an organization,” such as “trojans, spyware, and adware,” equating it to “malware” and “spyware[.]” *'243 Patent*, 1:42-54. The methods described for the '243 Patent’s system perform steps of monitoring API call activity on the computer using a kernel-mode driver; storing the API call activity in a log; analyzing, heuristically, the API call activity to determine whether weighted factors associated with this activity exceeds a threshold; identifying a suspected pestware object based on this activity; identifying an externally networked source of this pestware object (e.g., IP address or URL); and reporting this source to an externally networked pestware research entity. *Id.*, Abstract, 2:17-26, 8:38-9:4, Claims 1, 12. A high-level example of this method is illustrated below in Figure 4:



'243 Patent, Fig. 4.

**B. Overview of the '243 Patent's File History**

39. I understand that the application which issued as the '243 Patent—Application No. 11/408,146 (the “'146 Appl.”)—was filed on April 20, 2006. I apply this April 20, 2006 date for the purposes of my opinions herein only as the priority date for the Challenged Claims. The Applicant amended the claims during

Prosecution to distinguish from prior art, specifying that the identified pestware object originated from a source distinct from the host computer; an “externally networked source.” ’243 *FH*, 158-169. Specifically, Applicant characterized the application as claiming identification of pestware downloaded from an Internet URL or Web site. *Id.* The Applicant also added a limitation requiring pestware to be reported to an externally networked pestware research entity to “enable” the entity to “research whether the externally networked source is a source of pestware.” ’243 *FH*, 63-76.

**C. Level of a Person Having Ordinary Skill in the Art**

40. 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 ’243 Patent, which I have been instructed to assume is April 20, 2006. 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.

41. In my opinion, a person having ordinary skill in the art, as of April 20, 2006, 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 '243 Patent and the prior art references discussed below.

42. 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 '243 Patent.

**D. Claim Construction**

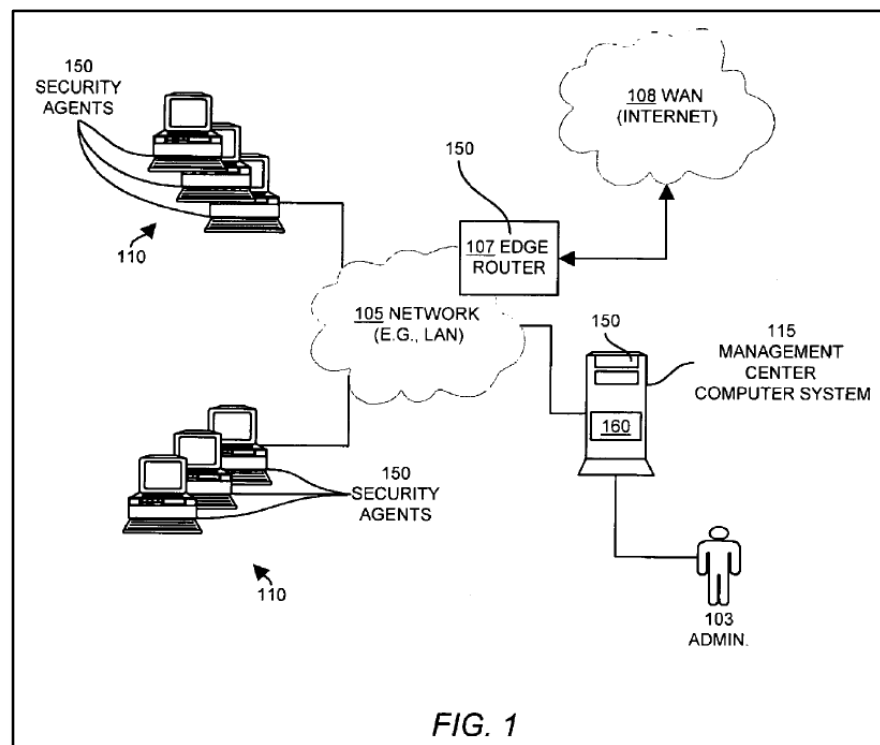
43. I have been informed by counsel that the first step in a patentability analysis involves construing the claims, as necessary, to determine their scope. Second, the construed claim language is then compared to the disclosures of the prior art. I am informed that claims are generally given their ordinary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

44. 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.

**E. Summary of the Prior Art References**

1. Gladstone

45. *Gladstone* (Ex. 1004) is generally directed to a security system comprising “security agents” that perform a method to “indicate types of operations that may be allowed or disallowed within a computer system.” *Gladstone*, 3:13-65. An exemplary networking environment where this security system is implemented is identified below:



*Id.*, Fig. 1. *Gladstone* expressly envisions identifying “processing operations such as a sequence of system calls that a malicious program has properly orchestrated to cause a failure” and maintaining “a security history of those calls that resulted in the failure so that a similar sequence calls executed in the future will be prevented, thus preventing the failure.” *Id.*, 4:5-12. *Gladstone* recognizes conventional anti-pestware techniques rely on virus definitions to identify and mitigate pestware, and thus include limitations such as an inability to recognize and remove new, never-before-seen viruses. *Id.*, 1:32-45, 2:36-3:12. As an improvement, *Gladstone*’s system monitors “recorded processing operations that led up to [the] undesired operation or problem to identify the root cause of the failure” to prevent those processing operations from executing again, resulting in “[t]he ability to learn of processing associated with a new attack, identify its root cause, and prevent it from happening in the future...without external input (e.g., virus definition files)[.]” *Id.*, 5:61-64.

46. To accomplish its methods, in embodiments, *Gladstone* discloses a security agent 150 operating on a host computer 110, router 107, or management center 115 includes “a plurality of security interceptors” (*see, e.g.*, Fig. 2) which “monitor processing activities and collect and report event data[.]” *Id.*, 6:23-7:15, Fig. 2 (depicting interceptors, including those in “kernel space 242”). Processing operations/event data can include, for example, network packet data from

communication session attempts, including the IP address from where the packet originated; or data regarding a file system access attempt including the identity of the application making this attempt, the file accessed, and type of access requested. *Id.*, 7:64-8:13, 9:18-21 (describing data associated with a buffer overflow attempt including URL data related to the attack), 12:7-12.

47. This information is then sent to an “event correlation engine” operating on security agent 150 or at management center 115, is stored in “security histories[,]” and a security violation is identified if a processing outcome violates a security policy. *Id.*, 8:14-56. Security agent 150 subsequently detects attempted performance of similar sequences of related processing operations and can deny those operations to avoid future violations. *Id.*, 8:58-9:11, Figs. 5-8 (detailing operation of *Gladstone’s* security methods). After detection and analysis, security agent 150 can “distribute the root cause to the management center 160 for distribution to other computers 110” to preemptively avoid violation on those computers. *Id.*, 11:42-55, 16:40-52.

48. A PHOSITA would have recognized that each of *Gladstone* and the ’243 Patent are related to the fields of detecting, controlling, and removing security threats on computer systems, and thus are in the same field of endeavor. *Gladstone*, Abstract, 2:36-3:65, 5:10-65; ’243 Patent, Abstract, 1:42-45, 2:7-26. A PHOSITA also would have recognized *Gladstone* is directed at solving similar problems to

those of the '243 Patent, including providing pestware identification and response that is not reliant on virus definitions generated based on previous encounters with the pestware, allowing the system to respond to new pestware in an improved manner. *Gladstone*, 2:36-3:65; '243 Patent, 1:63-2:3.

2. Muttik

49. *Muttik* (Ex. 1005) is directed to a system and method “determining whether software is likely to exhibit malicious behavior by analyzing patterns of system calls” or “application program interface (API)[ ] calls[.]” *Muttik*, Abstract, 1:8-12, 1:43-45. In an example, *Muttik*’s system monitors the following API calls: “1. {system call to modify the registry key(s) responsible for launching applications at startup}[;] 2. {wildcard—any number of intervening system calls}[;] 3. {system call to write an executable file with a name used in step 1}[;] 4. {wildcard—any number of intervening system calls}[;] 5. {system call to open a port for listening}[.]” *Id.*, 5:6-13. *Muttik*’s system then “assign[s] weights to system calls[.]” e.g., “positive for suspicious activity, and negative for” non-malicious activity. *Id.*, 5:14-17. The total weights are “compared against a threshold value” such that “[i]f the total weight equals or exceeds this threshold value, the system can report the code as suspicious.” *Id.*, 5:18-21. In the above example, if “the weights for items 1, 3 and 5 above are, 20, 20 and 30, respectively” and the threshold is 50, “the system will indicate that the code is suspicious[.]” *Id.*, 5:22-27.

50. A PHOSITA would have recognized that each of *Muttik* and the '243 Patent are related to the fields of detecting, controlling, and removing security threats on computer systems, and thus are in the same field of endeavor. *Muttik*, 1:8-12 (the “present invention relates to systems for detecting malicious computer software”), 1:66-2:11, 3:43-52; '243 Patent, Abstract, 1:42-45, 2:7-26. A PHOSITA also would have recognized *Muttik* is directed at solving similar problems to those of the '243 Patent, including providing a security system which does not rely on virus definitions to detect security threats. *Muttik*, Abstract (describing monitoring system calls to detect malware), 1:8-12, 1:66-2:11, 3:43-52, 4:32-33, 4:59-5:27; '243 Patent, 1:63-2:3, 5:42-67 (describing monitoring API call activity to detect malware), claims 1, 6, 12.

3. *Pantuso*

51. *Pantuso* (Ex. 1006) is directed to a system and method that determines the source (such as an IP address) of pestware activity, which is then reported to a “central intrusion activity watch service.” *Pantuso*, 2:26-45. For example, *Pantuso* discloses “personal firewalls” installed on user computers which monitor information relating to intrusion activity. *Id.*, 3:16-23, 4:21-33. This information is output to a central server, and there, the stored information is heuristically analyzed to ascertain intrusion activity” so that the source (e.g., IP address) of the activity is identified, to provide the opportunity to “correct any infected machines[.]” *Pantuso*,

2:1-34, 3:46-48, 4:47-54, 5:11-56 (describing initiating a “trace” to identify the source of the intrusion activity). The intrusion activity may be additionally or alternatively transmitted to other networked computer systems to “notify the public of the source of the intrusion activity.” *Pantuso*, 2:38-45, 6:8-20, Figs. 3-4.

52. A PHOSITA would have recognized that each of *Pantuso* and the ’243 Patent are related to the fields of detecting, controlling, and removing threats to computer systems. *Pantuso*, 1:8-10 (the “present invention relates to intrusion detection scanning methods”), 3:16-23, 4:21-33; ’243 Patent, Abstract, 1:42-45, 2:7-26. A PHOSITA also would have recognized *Pantuso* is directed at solving similar problems to those of the ’243 Patent, including providing pestware protection that does not require the use of virus definitions, enabling the systems and methods to protect against unknown threats, and thus are in the same field of endeavor. *Pantuso*, 2:1-5 (describing identifying intrusion activity “heuristically”), 2:29-43, 4:47-54, claims 2, 11, 22; ’243 Patent, 1:63-2:3, 3:65-4:7 (describing heuristic analysis), 4:40-62 (same), claims 1, 6, 12.

#### 4. English

53. SPA04 *English* (Ex. 1007) is directed to a system and method for detection and removal of “malware” such as spyware, viruses, or worms. *English*, Abstract, 1:13-19. In embodiments, *English*’s system exploits an “Internet cache maintained by the computer system’s Web browser to determine the source URL”

of particular files. *Id.*, 5:1-23, Fig. 2. “If a user downloads a file from the Internet, this cache area will effectively ‘log’ the URL of the download.” *Id.* *English* states that the browser’s cache acts as a “URL access log” that is “effective for determining the exact source URL of a spyware payload.” *Id.*

54. A PHOSITA would have recognized that each of *English* and the ’243 Patent are related to the fields of detecting, controlling, and/or removing security threats on computer systems, and thus are in the same field of endeavor. *English*, 1:13-19 (the “present invention relates generally to...detecting, removing[,] [] preventing[,]” and “determin[ing] the source of malware”), 1:66-2:11, 3:43-52; ’243 Patent, Abstract, 1:42-45, 2:7-26. A PHOSITA would have also recognized *English* is directed at solving similar problems to those of the ’243 Patent, including providing a security system which does not rely on virus definitions to detect security threats. *English*, Abstract (describing searching an Internet cache to determine the URLs that might be the source of malware), 1:13-19, 2:58-67, 4:11-32, 5:1-23, Fig. 2; ’243 Patent, 1:63-2:3, 9:26-52 (describing searching a cache to determine the source of pestware), claims 1, 6, 12.

**F. Opinions Regarding Ground 1: Claims 1-3, and 5-14 are rendered obvious by Gladstone in view of Muttik or Gladstone in view of Muttik in further view of Pantuso**

1. Claim 1

- (a) *1[P]. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:*

55. *Gladstone* describes a computer system performing a computerized method from software stored on computer-readable medium that identifies the “root cause” of computer activity due to unwanted pestware-related/“malicious” software. *Gladstone*, 5:42-61. In these methods, *Gladstone* utilizes a “security system” comprising “security agents” which “monitor and record processing behavior that results in an undesired processing operation” along with “recorded processing operations that led up to [the] undesired operation or problem to identify the root cause of the failure.” *Id.* *Gladstone* explains that in embodiments, its method comprises steps of detecting operation of a sequence of processing operations, correlating the operations in a security history with outcomes associated with such processing, identifying a security violation by the processing operations, and disallowing those steps in the future. *Gladstone*, 3:66-4:11, 7:44-63, 8:46-9:11. Fig. 3.

56. I note that the '243 Patent describes examples of “pestware” including “trojans, spyware, and adware.” '243 Patent, 1:43-54. Further, the '243 Patent equates “pestware” to “malware” and “spyware” or at least indicates malware and spyware are a type of pestware. *Id.* A PHOSITA would have understood “pestware,” as described by the '243 Patent, includes unwanted software with malicious functions, such as stealing information (e.g., “spyware”), presenting unwanted advertisements (e.g., “adware”), and/or interrupting the normal operation of the

computing system, which would include Trojans and other types of malicious software. This understanding coincides with known in the art descriptions of “malware” in *Gladstone* and other prior art references, such as *English*. Namely, *Gladstone* describes “**malicious** software programs” including “viruses, worms, **Trojan horses**, and the like,” as well as “denial-of-service attacks, a buffer overflow operations, execution of malformed application data, and execution of malicious mobile code.” *Gladstone*, 1:5-11, 1:54-2:20. Similarly, *English* explains the term “malware” is used “to connote any software that may be installed onto a computer without the user’s full consent or awareness, including software that may gather information from the computer, sometimes without the user’s knowledge. Malware may present a privacy, security or productivity risk to the user’s computer system.” *English*, 1:25-31. Based on these descriptions, a PHOSITA would have recognized that the software identified by *Gladstone* as “malware” teaches at least one or more types of “pestware” as described by the ’243 Patent because it is unwanted software with malicious intent that may cause issues with privacy or system performance. *’243 Patent*, 1:43-54.

57. Furthermore, I also understand that Patent Owner has explained in the litigation that “‘pestware’ is broader than and is not limited to ‘a trojan, spyware or adware program’.” Ex. 1008 (*Responsive Markman Brief*), 11. Thus, *Gladstone’s*

processes disclose identifying an origin of activity on a computer that is indicative of pestware under PO's understanding of this claim limitation as well.

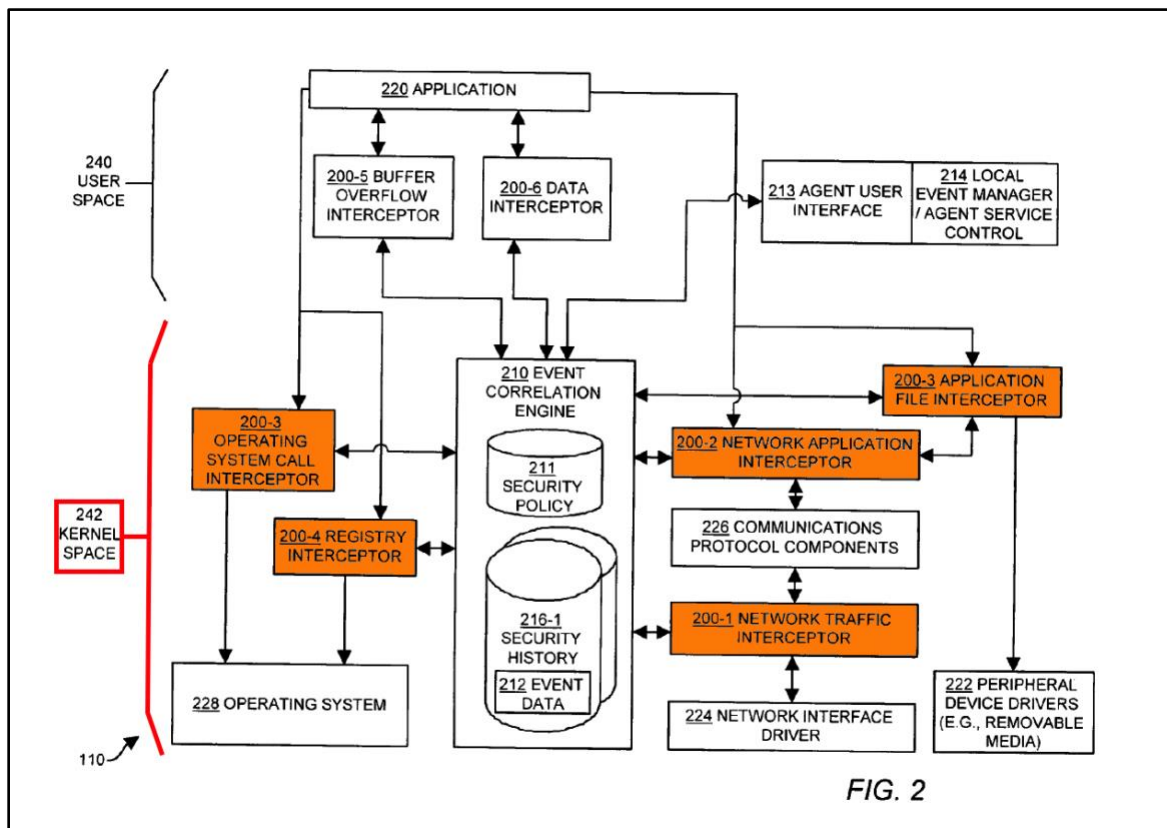
58. *Gladstone*, therefore, discloses a “method” for identifying the origin of activity indicative of “pestware,” as claimed. For example, *Gladstone*'s methods can be used to monitor network packet data from communication session attempts. *Id.*, 7:64-8:5. Here, the security agents monitor event data, “includ[ing] specific information concerning the packet, such as an Internet Protocol (IP) address identifying a computer system or network device from which the packet originated[.]” *Id.* In another example, the security agents monitor “a file system access attempt made by an application 220 for access to a file (e.g., via a system call or [a] device driver call to access the file on [a] disk)[.]” *Id.*, 8:6-13. Here, *Gladstone*'s system identifies “the identity of the application 220” along with the “specific file to be accessed, and the type of access requested [by] the file.” *Id.* For the reasons discussed below in limitation 1(d), it is my opinion that it would have been obvious for a PHOSITA to also identify the source where application 220 came from (i.e., the URL or IP address where application 220 was downloaded from) in *Gladstone*'s methods. *Infra*, Claim 1(d) (also describing combination with *Pantuso* to identify the origin of pestware).

- (b) *[1(a)] monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and*

*storing a history of at least a portion of the API calls in an activity log;*

**“monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware”**

59. Gladstone’s methods utilize a plurality of interceptors 200 (which represent the claimed “drivers”), including interceptors which operate solely in the kernel space 242, as highlighted orange below in annotated Figure 2.



Gladstone, Fig. 2<sup>1</sup>. Gladstone’s interceptors “watch over and monitor processing operations performed by various software and hardware components within the host

<sup>1</sup> All annotations added unless noted otherwise.

computer system which that security agent protects.” *Gladstone*, 3:26-32. For example, the file interceptor 200-3 is configured to identify processing activities performed by applications 220, such as when the application 220 accesses a particular file via an “operating system call.” *Id.*, 7:19-22, 8:6-13; *see also id.*, Fig. 5 (steps 500-504). Similarly, the network traffic interceptor 200-1 is configured to monitor “processing operations related to an inbound connection to a Web server...in order to detect the related sequence of processing operations that the inbound Web server connection attempt triggers[.]” *Gladstone*, 3:32-53, 7:17-19, 7:64-67. These are merely examples given by *Gladstone* of envisioned drivers operating at the kernel level (thus “*kernel mode drivers*”) that monitor computer activity for potential security violations, such as those due to pestware (e.g., viruses, worms, spyware, Trojans, or adware).

60. A PHOSITA would have understood that these kernel-mode interceptors are “kernel mode drivers.” For instance, based on my extensive experience with malware security systems and computing systems in general, I understand “drivers” to generally refer to software used to interface between computer components (e.g., generally, software that communicates). *Gladstone’s* kernel level interceptors teach the claimed kernel mode drivers because they operate in the kernel space and communicate information regarding computing activity—such as communicating API calls from an application accessing a file to *Gladstone’s*

threat detection system. More specifically, a PHOSITA would have recognized *Gladstone's* interceptors require kernel-mode access to be able to determine what operations an application 220 is performing, such as monitoring API calls made on the device. Without the drivers (interceptors), *Gladstone's* monitoring method would be unable to communicate with the aspects of its security system, including communications concerning what requests have been received or applications downloaded.

61. These kernel-mode interceptors also fit within characterizations for a kernel-mode driver as discussed in the specification of the '243 Patent. The '243 Patent explains that “the activity monitor 116 is realized by a kernel-mode driver” such that it logs “API calls in the activity log” related to pestware processes. '243 Patent, 5:42-56. Like the '243 Patent, as discussed above, *Gladstone's* interceptors “watch over and monitor processing operations performed by various software and hardware components within the host computer system which that security agent protects” and log such processing operations. *Gladstone*, 3:26-32. This includes, for example, processing activities performed by application 220, such as when the application 220 accesses a particular file via an “operating system call” (i.e., API call). *Id.*, 7:19-22, 8:6-13.

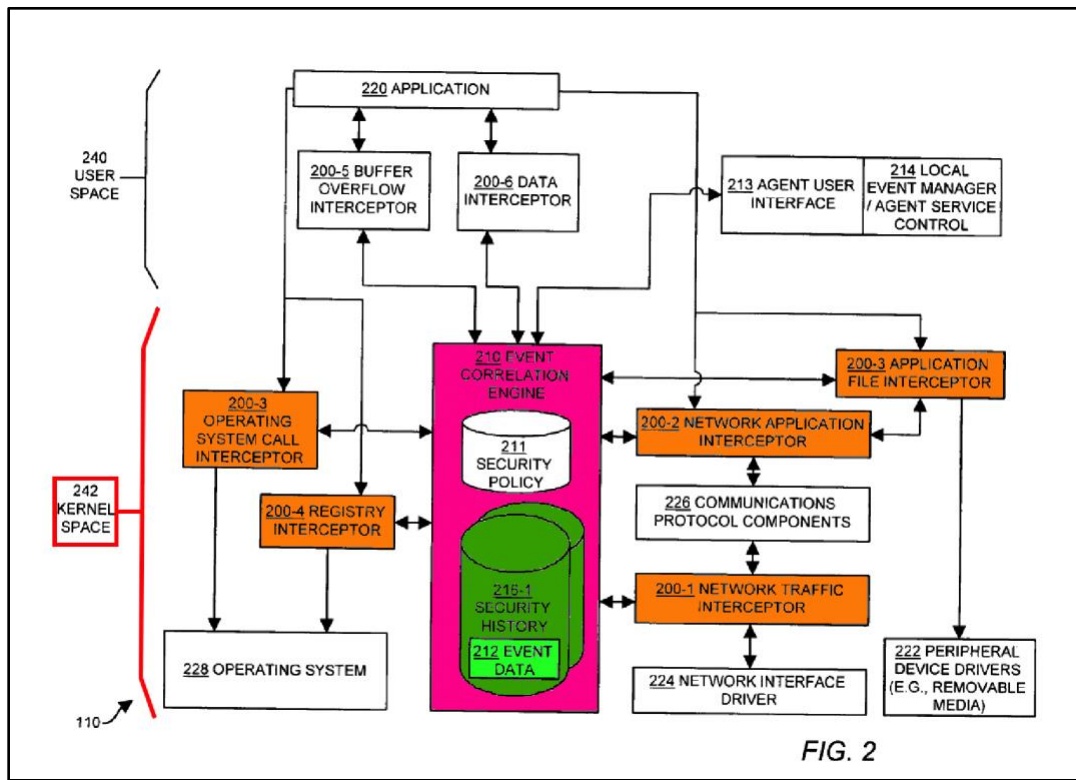
**“monitoring API calls”**

62. In the case of file interceptor 200-3 monitoring “operating system calls” to access particular files, a PHOSITA would have recognized that *Gladstone* is describing the well-known process by which applications perform Application Programming Interface (API) calls to request that the operating system provide the application 220 with the desired file. For instance, *Device Drivers for Windows* (Ex. 1010), a manual for the Windows operating system, supports that these operating systems calls are API calls. *Device Drivers for Windows* provides that applications accessing a Dynamic Link Library (DLL) via system calls is an example of an “API function call” operating at the kernel level. *Device Drivers for Windows*, p. 13 (“...when a DLL associated with the legacy applications requires hardware access, it calls the kernel-mode driver directly using a Win32 API function call ***DeviceIoControl()***...”). This description is consistent with the description in *Gladstone*, which teaches that “interceptors 200 can be installed and executed by using, for example, windows registry keys that create dependencies on standard MS Windows dynamically linked libraries (dlls) so that the interceptor dlls 200 are loaded along with the appropriate windows dlls that they monitor. The interceptors can thus serve as wrappers to monitor processing operations of all calls made to any specific computer components.” *Gladstone*, 6:51-61. Similarly, *Muttik* reaffirms that a PHOSITA would have recognized *Gladstone*’s monitoring of system calls as a form of monitoring API call activity. *Muttik*, 1:43-45 (“system calls (or application

program interface (API) calls)"). Thus, since *Gladstone's* interceptors serve as "wrappers to monitor processing operations of all calls made to any specific computer components," a PHOSITA would have recognized that *Gladstone's* interceptors teach monitoring API calls (such as those performed via DLL calls) via drivers (interceptors 200) operating at the kernel level (i.e., *kernel mode drivers*). *Gladstone*, 6:59-7:26, Fig. 2

**"storing a history of at least a portion of the API calls in an activity log"**

63. Data regarding activity stored by the interceptors 200 (including API calls) is collected in one or more activity logs—i.e., security history 216. *Gladstone*, 6:2-8, 7:10-43, 8:1-13, 9:28-34, 11:56-67, Fig. 4 (depicting event record), Fig. 5 (steps 505-507). Specifically, event data 212, such as data described above regarding API call activity, is reported by *Gladstone's* interceptors 212 to a correlation engine 210, which records it as a record of computer activity; a method that parallels the description of the '243 Patent of an "activity log" in which information related to computer processes is stored. *Gladstone*, 7:10-16, 8:14-37, 9:28-65; *243 Patent*, 5:18-29. Security history (or histories) 216 is illustrated below in dark green, storing the event data 212 in light green:



*Gladstone*, Fig. 2. Specific examples of the types of data stored within *Gladstone*'s activity log(s) include historical information such as an indication of a specific security violation produced during an event, a detected processing instruction and/or program identity causing the event, a timestamp, *procedure call or sub-routine information*, file names of data to be accessed, and/or dynamically linked library (dll) information. *Gladstone*, 12:1-24.

- (c) *[1(b)] analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;*

64. I note that limitation 1(b) recites a step of analyzing computer activity “heuristically.” The ’243 Patent describes embodiments with exemplary heuristics such as applying weights to determine the likelihood that computer activity is attributable to pestware. *’243 Patent*, 4:45-62. This description is consistent with known understanding of “heuristic” analyses to entail, such as applying weights to computer activity used to detect patterns in the activity indicative of pestware. Indeed, *Pantuso* affirms this general understanding, characterizing a process performed “heuristically” by stating “[a]s an option, this may be accomplished **heuristically**...For example, the information may be analyzed for patterns that are indicative of intrusion activity.” *Pantuso*, 4:47-54.

65. As discussed above, *Gladstone* teaches a system employing rule-based methods for determining activity indicative of pestware from actions (e.g., API calls) detected and recorded by interceptors at the kernel level. *Supra*, Claim 1(a). While *Gladstone* describes heuristic rule-based methods for determining the presence of pestware in a host computer and mitigating such pestware, *Gladstone* does not expressly discuss applying a heuristic which utilizes weighting factors for comparison to a threshold. However, *Muttik* discloses this.

66. *Muttik* describes a computer method for detecting pestware by monitoring API calls, which (1) “records system calls (API calls) generated by code[;]” (2) applies “comparison rules” to compare the record of API calls against profiles of calls generated by known malicious code; and (3) “determines if the record of [API] calls indicates that code [] is likely to exhibit malicious behavior.” *Muttik*, 4:25-44, Fig. 3. Specifically, *Muttik*’s pestware detection algorithm assigns weights to API calls which are compared against a threshold to determine the likelihood of malicious behavior.

comparison unit 204 can be configured to **assign weights to system calls**. **Weights can be positive for suspicious activity**, and negative for activity which is more likely to be present in non-malicious code. **The system can keep a count of the total weight, which is compared against a threshold value**. If the total weight equals or exceeds this threshold value, the system can report the code as suspicious.

*Muttik*, 5:15-21 (emphasis added). As a specific example, *Muttik* lays out an algorithm by which weights are applied to potential computer processes (activity), then a determination of likely pestware is established if the sum of the weights of activities actually detected surpasses a threshold level. *Muttik*, 4:59-5:27; *see also id.*, Fig. 2 (“Decision 212” “OK or malicious”). Specifically, *Muttik*’s system monitors the following API calls:

1. {system call to modify the registry key(s) responsible for launching applications at startup}
2. {wildcard—any number of intervening system calls}

3. {system call to write an executable file with a name used in step1}
4. {wildcard—any number of intervening system calls}
5. {system call to open a port for listening}

*Muttik*, 5:6-13. Items 1 and 3 are weighted at 20, while Item 5 is weighted at 30 and the threshold for pestware activity is set at 50. *Muttik*, 5:22-27. Thus, performance of steps 1, 3, and 5 sums to a total weight of 70, surpassing the threshold and qualifies as pestware activity. *Muttik*, 4:59-5:27.

67. Based on *Muttik*'s description of a process in which rules are applied assigning weights to computer processes to determine pestware activity patterns, a PHOSITA would have recognized that *Gladstone* as modified by *Muttik* teaches the claimed limitation of "analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware." A PHOSITA would have been motivated to include *Muttik*'s pestware analysis using a heuristic weighting approach into *Gladstone*'s pestware identification method to potentially prevent new pestware processes the first time they are encountered ("on-the-fly," as described by *Muttik*), in addition to blocking pestware previously encountered. *Muttik*, 4:12-16, 4:25-44. A PHOSITA would have recognized *Gladstone*'s event correlation engine would have been modified to perform the

heuristic weighting and threshold comparison steps pursuant to *Muttik*, rendering obvious a “heuristics module.”

68. Specifically, a PHOSITA would have found it obvious to modify *Gladstone*’s event correlation engine to incorporate functions from *Muttik*’s comparison unit 204, in order to perform *Muttik*’s weighted threshold analysis for API call activity. Indeed, this would simply be applying a known heuristic technique (i.e., *Muttik*’s weighted threshold heuristic) in *Gladstone*’s system which already employs heuristic rule-based analyses. This modification would have had the desirable improvement of, when possible, preventing a need to shut down and reboot after the first encounter with pestware, as in *Gladstone*, which would have resulted in possible downtime and exposure to process exceptions, faults, system crashes, security policy violations or any other type of unwanted operation. *Gladstone*, 14:32-42.

69. Moreover, *Muttik*’s heuristic analysis would successfully operate within *Gladstone*’s disclosed methods. For instance, in *Gladstone*’s native pestware security process: First, security agents detect a sequence of processing operations (e.g., API call activity by kernel-level interceptors) and record this information in a security history. *Supra*, Claims 1[Pre]-1(a); *Gladstone*, Figs. 5 and 6. Then, the system executes these processing operations, recovers from the undesired outcome, stores the outcome in the security history, and sends this security history to a

management center to identify what caused this outcome such that an updated policy can be received to prevent this outcome in the future. *Gladstone*, Figs. 6-8. A PHOSITA would have understood that *Gladstone's* identify, execute, recover, and prevent framework disadvantageously exposes the system to undesirable processing events. When modified by *Muttik*, *Gladstone's* modified system would identify pestware activity on a first encounter pursuant to *Muttik*, preventing execution of unwanted pestware and the need to potentially recover from a system crash as described above.

70. *Muttik* provides other benefits for its techniques which would also motivate the combination. *Id.*, 2:40-54 (describing “a number of advantages[,]” including generating fewer false alarms); *see also id.*, 1:59-63 (*Muttik* expressly explains its methods detect malicious software “without exposing the computer system to potentially malicious actions of the software”). A PHOSITA would have been additionally motivated by these express benefits to implement *Muttik's* weighting process in *Gladstone's* system.

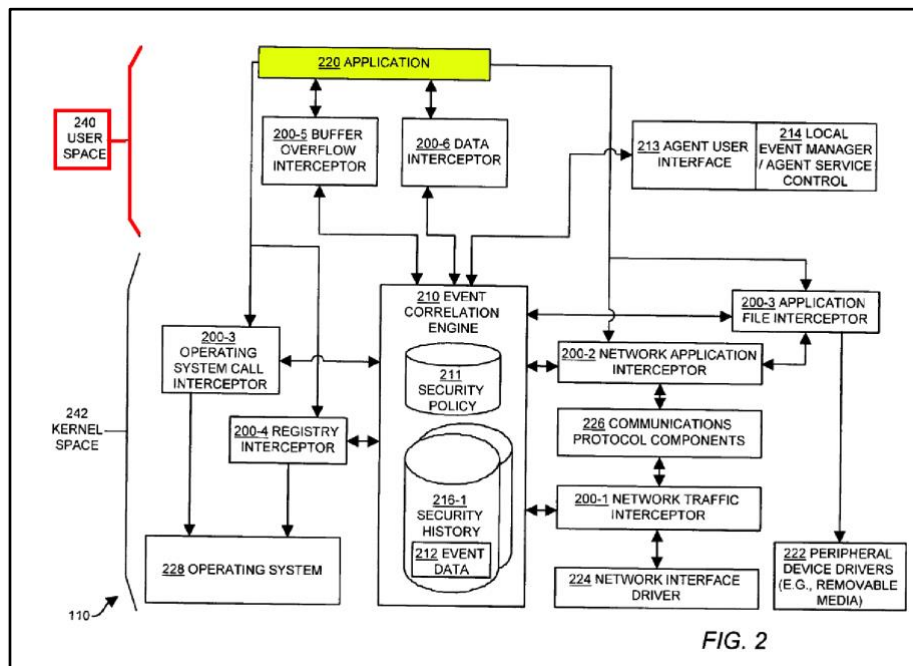
71. The combination would have been well within the skills of a PHOSITA to incorporate *Muttik's* heuristic weighting analysis of computer activity (including API calls) into *Gladstone's* pestware security methods that also seek to detect and mitigate pestware by monitoring API call activity. Modifying the *Gladstone* system using *Muttik's* weighting and threshold heuristic analysis would have provided a

desirable ability to prevent execution of pestware and would have required simple software modifications to hardware already present, leading a PHOSITA to a reasonable expectation of success. An administrator of the system would have been able to set this threshold at any desired level, further motivating the combination. For instance, an administrator may raise the threshold, tightening security during times of particular threat, or lower the threshold, relaxing security to reduce any false positives. Such a combination would have constituted improving a known system (*Gladstone's* system performing its pestware-identification method) using a known technique (*Muttik's* weighted heuristic with threshold comparison), requiring only software reprogramming within the skill of a PHOSITA without undue experimentation. The modified *Gladstone/Muttik* system and method would then operate as normal, storing event data related to identified API call pestware processes in security history and transmitting a report of such to a management center for analysis, updating its security policy to prevent future executions of the pestware activity.

- (d) *[1(c)] identifying, based upon the activity, an object residing on the computer that is a suspected pestware object*

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

73. As I described above, *Gladstone* teaches its system and method “rapidly identifies malicious attacks[,]” by storing event data 212 in security history 216. *Supra*, Claim 1(a); *Gladstone*, 3:13-17, 7:17-24. This event data includes, for example, information identifying an application 220 and/or the processes application 220 executes (i.e., *an object residing on the computer that is a suspected pestware object*) accessing a particular file via an operating system API call. *Supra*, Claim 1(a). As seen below in Fig. 3, code for application 220 resides in the user space of computer system 110, and thus resides “on the computer,” as claimed.



*Gladstone*, Fig. 3 (annotated). A PHOSITA would have understood that an application 220 constitutes an “object” consistent with the ’243 Patent’s specification. See, e.g., ’243 Patent, 8:5-22 (describing “objects” as including both

files and processes, an understanding widely accepted to PHOSITAs at the time of the '243 Patent); *see also id.*, 3:49-64 (describing tracing the information in N files to the “source of pestware 122, 124” where one or more of the N files can be associated with one or more applications or can be “generated from an application”), Fig. 1 (“Pestware File 124”). This is also consistent with the '243 Patent's file history. *See, e.g.*, '243 FH, 85-86, 138-139, 178-179 (rejections mapping prior art “unwanted software application” to the claimed “object”). Similarly, the API processes originating from application 220 would also reside on the computer as executable code. Thus, *Gladstone/Muttik's* method monitors computer activities for API calls indicative of pestware. *Supra*, Claim 1(b). The modified method then identifies, based on the monitored computer activity, the object(s) (application file 220 and/or processing operations (processes) originating from the application file 220) responsible for the API call activity. Of course, since the application 220 is on the computer, the processes being performed by the application regarding the computer, such as API calls, would have also been understood by a PHOSITA to have resided “on the computer,” as claimed.

74. Further, application 220 and/or processing operations (processes) originating from the application file 220 are a “suspected pestware object” as claimed. For the purposes of my opinions herein, I have been informed to apply PO's plain and ordinary meaning to this limitation. I understand that in litigation, PO

contends that “‘suspected’ referring to pestware” is a well-understood concept and requires no construction. Ex. 1008 (*Responsive Markman Brief*), 14-15. Namely, PO suggests a “‘suspected pestware object’ is simply the object identified based upon the activity”—referring to the monitored activity in the limitations above. *Id.* PO points to examples in the specification which it contends support its interpretation. *Id.*, 7-8 (citing related ’932 Patent, 4:58-66 and characterizing disclosure as “identifying a suspected pestware object by analyzing activity based on weighted factors associated with pestware activity and determining that one or more of the weighted factors exceeds a threshold”). PO contends that “[a] POSITA would understand that activities that exceed the threshold may be...‘suspected’ of pestware.” *Id.*, 17. I express no opinion on the correctness of PO’s arguments. I express no opinion regarding the correctness of PO’s interpretation.

75. Under PO’s interpretation, *Gladstone’s* modified system identifies application 220 as a “suspected pestware object.” Namely, *Gladstone* in view of *Muttik* utilizes the same process of weighting factors for API call activity and comparing to a threshold as PO identifies to determine if an object is a “suspected pestware object.”

- (e) *[1(d)] accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular*

*externally networked source that the suspected pestware object originated from; and*

76. As I explained previously, *Gladstone* discloses identifying an object (application 220 or its processes) residing on the computer that is suspected of being a pestware object based on activity, including, e.g., API call activity. *Supra*, Claim 1(a)-1(c). Information identifying the application and/or processing operations conducted by the application are stored as event data 212 in security history 216. *Id.*

77. *Gladstone* also describes additional embodiments where its security system monitors computer activity for pestware, such as by monitoring network packet data from communication session attempts. *Gladstone*, 7:64-8:5. Specifically, *Gladstone* may record “specific information concerning the packet, such as an Internet Protocol (IP) address identifying a computer system or network device from which the packet originated” in security history 216’s event data. *Gladstone*, 7:64-8:5. In another example, upon detecting buffer overflow pestware activity, *Gladstone*’s system is able to “detect an overflow and can map it to a recently received URI (URL) that caused the fault.” *Gladstone*, 9:18-21. In each of these, this source data would be stored in security history 216. Indeed, *Gladstone* explains that its network traffic interceptor 200-1 “resides between a TCP driver 221 and the network interface card 224” and “looks at packets coming from the network.” *Id.*, 6:42-61. By looking at these network packets, a PHOSITA would

have understood this interceptor is examining IP address and URL metadata associated with these packets, and such data would be stored as event data in security history 216. *Id.*, 7:64-8:5. A PHOSITA would have recognized each of these disclosures, in which a record of the address or location on a network from which pestware activity originated is stored in security history 216, an externally networked source of pestware is identified. *Gladstone*, 7:64-8:5, 9:18-21. This understanding of a PHOSITA is consistent with the specification and File History of the '243 Patent, which expressly lists URLs, Web sites, and/or IP addresses as the originating sources of pestware. '243 Patent, 3:41-45, 3:59-60; '243 FH, 167.

78. I note that while *Gladstone* discloses identifying the origin of the pestware (e.g., IP address and URL), these disclosures come from separate embodiments from the application file access embodiment described above. In my opinion, it would have been obvious to a PHOSITA to modify the processes in *Gladstone's* application file access embodiment with features from its other embodiments, such as determining the IP address or URL from where pestware objects (e.g., application 220) originated.

79. For example, one of *Gladstone's* stated goals is to inhibit the spread of "malicious programs" (pestware) to "other computers within a network or data center by exploiting vulnerabilities of computer's operating system or resident application programs." *Gladstone*, 1:14-19, 2:21-32. One approach to achieve this

goal is to report event data regarding malicious software attacks experienced by one computer to other computers on a network “in order to spread the knowledge of the behavior or processing pattern that the malicious attack attempted to perform...so that other computer systems will not be vulnerable to the attack.” *Gladstone*, 3:56-65. A PHOSITA would have recognized that each of the types of event data expressly described by *Gladstone* in separate embodiments regarding pestware activity would have been valuable, useful information to disseminate to other networked computers to help prevent pestware activity on those computers and throughout the system. Though *Gladstone* presents these embodiments as separate examples, a PHOSITA would have recognized that, prior to the '243 Patent, it was well-known to download applications from remote locations using IP addresses, where the applications would then have been installed locally on a computing device, and to track the locations these downloads occurred from. For example, *Dixon* (Ex. 1012) expressly describes a computerized system and method for “real-time, reputation-based Web services” that provides “enhanced security for users of computer devices.” *Dixon*, ¶¶ 4-6. *Dixon* illustrates that it was known that particular URLs, Web sites, or addresses may be advantageously identified as known sources of “spyware, malware, or other unwanted content,” and should be avoided. *Dixon*, ¶ 90. *Dixon*’s solution specifically disseminates information regarding such externally networked pestware sources using a “reputation service host” that collects

information regarding the pestware sources and warns users of potential danger of interacting with such a source. *Id. Kronenberg* (Ex. 1011) and *English* (Ex. 1007) each additionally provide further support that it was well-known prior to the '243 Patent to identify a source of a downloaded file by its IP address and/or URL, and to store such information for future use. *Kronenberg*, ¶¶ 7, 28-31, Fig. 3; *English*, 5:1-23, Fig. 2. *Kronenberg* is clear on the benefits of sharing such information regarding the reputation of networked sources, envisioning that these networked sources may even be blocked upon future attempts to download pestware. *Kronenberg*, ¶¶ 10, 31. Moreover, *Kronenberg* notes certain sources can be “white list[ed]” and therefore catalogued as safe, providing a basis for approval from downloads from that particular source location. *Id.*, ¶ 31. Similarly, *Hartrell* (Ex. 1014) shows it was known in the art to record IP addresses and/or URLs as part of monitored data in a security system. *Hartrell*, 4:10-15.

80. Based on these well-known understandings and motivations, it would have been obvious to a PHOSITA to transmit information to other computers regarding all event data monitored and stored in *Gladstone* relating to pestware activity – including information pertaining to the source of the downloaded application and information pertaining to API calls performed by the application after installation. Therefore, in my opinion, it would have been obvious to modify *Gladstone* to store event data including the identity of a pestware application 220,

processing operations by that particular application 220, and the source from which the particular application 220 was downloaded in security history 216. A PHOSITA would have recognized that this modification would have furthered *Gladstone's* express goal of inhibiting the spread of “malicious programs” (pestware) to “other computers within a network or data center by exploiting vulnerabilities of computer’s operating system or resident application programs.” *Gladstone*, 1:14-19, 2:21-32.

81. Storing this record in security history 216 would have enabled the system to track the malicious networked source (e.g., Web site, IP address, or URL) from which the application 220 responsible for the pestware activity was received, such that the system would then be able to report the poor reputation of this externally networked source to other computers. In *Gladstone's* software, each of these event data types are stored in native hardware components. Because, as shown by the prior art, security risks stemming from downloading applications from externally networked sources and methods of disseminating the identity of such externally networked sources of pestware to other computers within a network to mitigate risk were each well-known, a PHOSITA would have had a reasonable expectation of success applying these well-known concepts in *Gladstone's* methods/system. A PHOSITA would have recognized the modification to be combining techniques and methods already-present in the prior art according to

known methods described expressly by *Gladstone* to predictably yield a system that records a networked source from which applications potentially identified as pestware were previously received.

82. In further support, *Pantuso* provides another example of this well-known procedure for inhibiting pestware, teaching a “central intrusion activity watch service” that “works to notify the public of the source” (such as the IP address) of pestware activity via electronic transmission. *Pantuso*, 5:50-52, 6:8-16. Since each of the embodiments described are performed by the same system (*Gladstone*’s), each would have utilized the same hardware, and thus combination would have only required simple reprogramming within the skill of a PHOSITA without undue experimentation, further yielding a reasonable expectation of success. Combining *Gladstone*’s methods of storing event data of two types, each relevant to pestware activity, would have constituted combination of prior art elements according to known methods (each expressly described in *Gladstone*), yielding a predictable result of a stored record of a networked source from which applications potentially identified as pestware were previously received.

**accessing, in response to the identifying an object...**

83. As I discuss below in Claim 1(e), *Gladstone* in view of *Muttik* or alternatively, in further view of *Pantuso* performs the steps of generating and transmitting a report to a “central intrusion activity watch service” via a network

(e.g., via email) in response to identified pestware activity. *Infra*, Claim 1(e). A PHOSITA would have recognized that in generating and transmitting a report in response to identifying the activity, *Gladstone's* modified method would have accessed the event data 212 in security history 216 regarding the identified pestware activity, commensurate with *Gladstone's* express embodiments.

84. For example, it would have been obvious to “mark” the source of where application 220 was downloaded from as a source of malware in response to identifying a pestware object, just as *Gladstone's* system marks sequence of processing operations that are the root cause of a failure. *See, e.g., Gladstone*, 11:42-49, 12:45-47. Indeed, a PHOSITA would have recognized that a result of combining the embodiments from *Gladstone* in which pestware is detected based on API call activity and associated with a previously-stored externally networked source, the system would need to “mark” the IP address (or Website, URL, URI, etc.) as a source of malware, providing additional data to *Gladstone's* management center 160 for updating a security policy and informing other devices of security risks and violations, including the pestware sources. The system must access the security history to “mark” this source as the source of pestware.

**Combination with *Pantuso***

85. Additionally or alternatively, it would have been obvious to modify *Gladstone's* and *Muttik's* methods to implement a “trace,” or “any other feasible

technique” as disclosed in *Pantuso* to determine the source of pestware in response to identifying pestware. Indeed, each of *Gladstone*, *Muttik*, and *Pantuso* generally relates to systems which address threats in compromised systems, and share similar countermeasures to identify threats using either signature-based or behavior-based techniques, or both. Specifically, *Pantuso* teaches a system and method that identifies pestware by determining “an Internet Protocol (IP) address associated with the source” of detected pestware activity by performing a “trace” to identify the source of the pestware activity (e.g., intrusion) or “any other feasible technique.” *Pantuso*, 1:25-33, 5:11-56, 6:8-20. A PHOSITA would have recognized that *Gladstone* itself teaches “recording traces” from attacks, leading to a reasonable expectation of success for the modification, using only hardware already present and software modification within the skill of a PHOSITA without undue experimentation. *Gladstone*, 7:38-43. *Pantuso*’s system monitors computer activity, analyzing it using a “heuristic” to detect and inhibit activity potentially due to pestware, such as viruses, worms, and/or Trojan horses. *Pantuso*, 1:25-33, 1:57-2:5, 4:15-20. *Pantuso*’s system logs information regarding computer activity events, including information such as “applications associated with the selected event[,]” “the associated Internet Protocol (IP) address[,]” and includes a “plurality of tools for processing” an event, including “Trace this Event.” This is shown in annotated Figure 5 below:

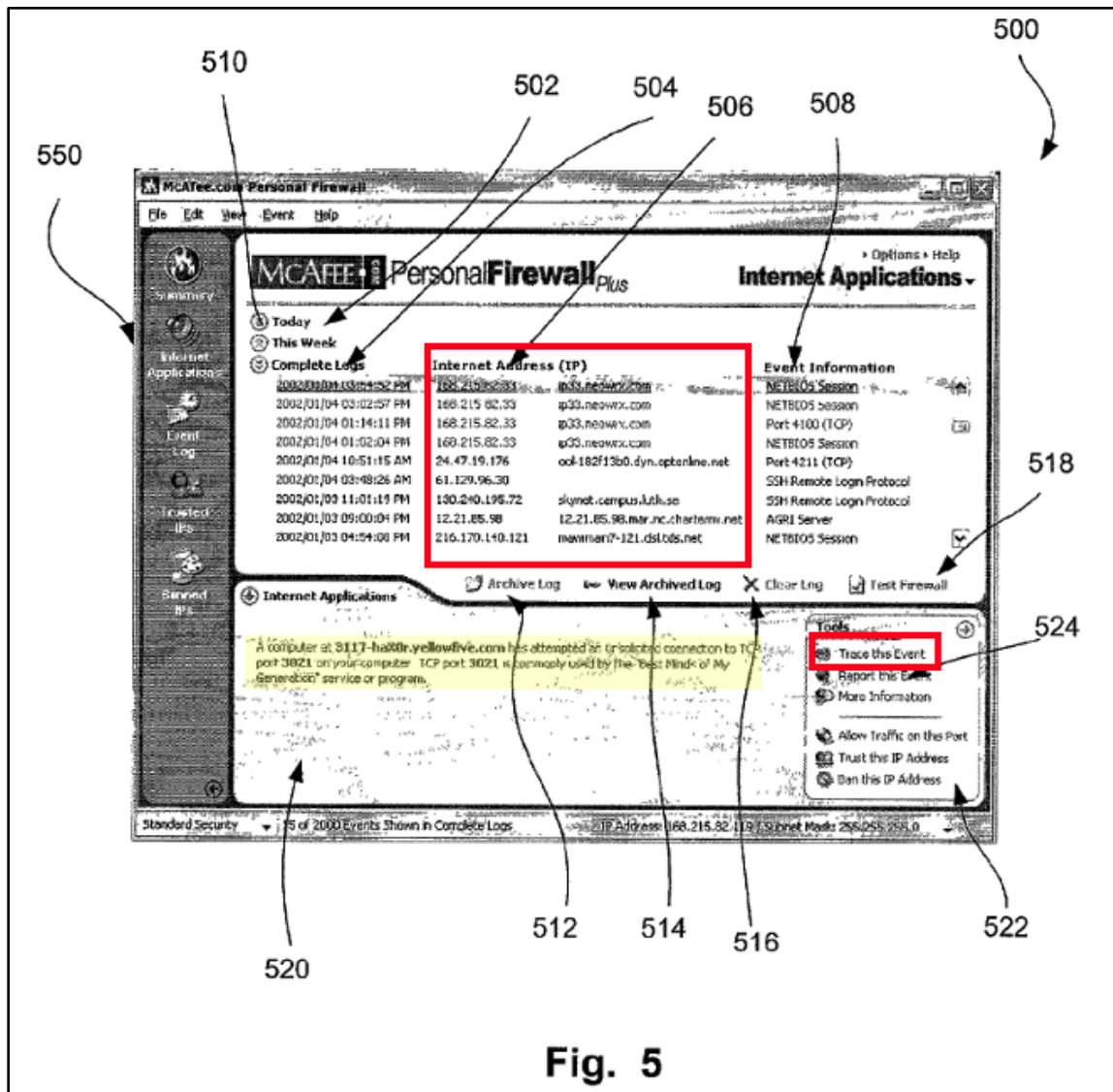


Fig. 5

*Pantuso*, Fig. 5. A PHOSITA would have found it obvious to modify the systems and methods of *Gladstone* and *Muttik* to utilize any of *Pantuso*'s trace techniques to identify the externally networked source of pestware, such as the IP address of a downloaded application 220. Specifically, each of *Pantuso*'s tracing tools ("Report this Event," "Trust this IP Address," "Ban this IP Address," "Trusted IPs," and/or "Banned IPs") would have been desirably incorporated into the *Gladstone* pestware

identification system and method to enable the system to track, block, avoid, and/or share sources of pestware with other networked entities. *Pantuso*, Fig. 5.

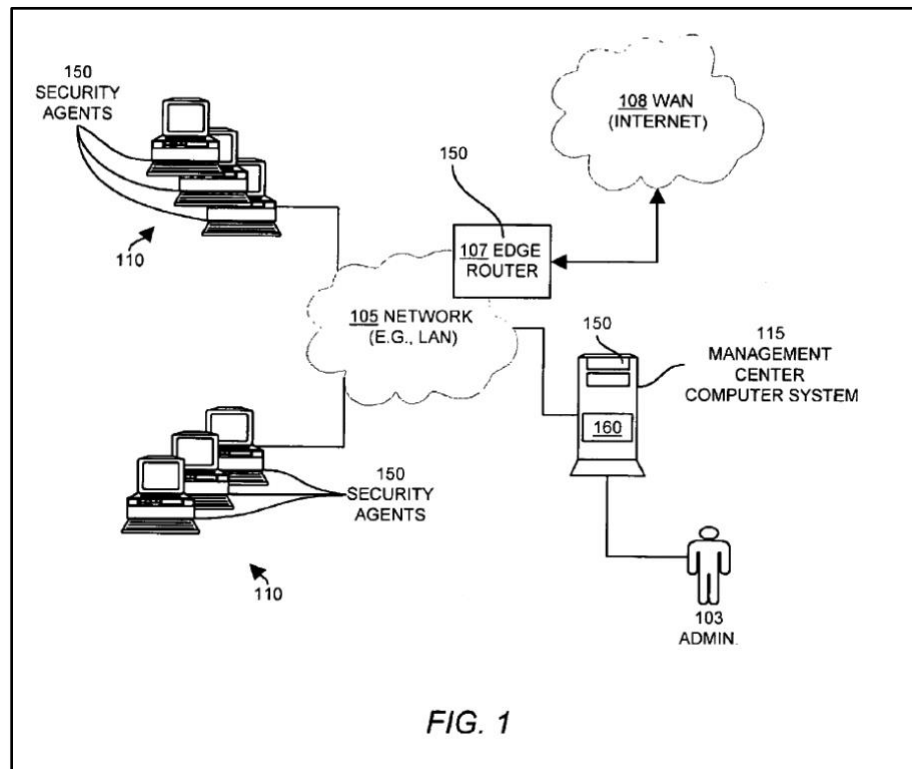
86. Each of *Hartrell*, *English*, and *Kronenberg*, described above, teach known methods of identifying and reporting the sources of pestware and mitigating pestware's impact on computing systems, illustrating that such techniques were well-known to PHOSITAs prior to the '243 Patent, leading to a reasonable expectation of success for the combination. Specifically, *Kronenberg* provides an example in which certain pestware source web sites may be whitelisted or blacklisted, allowing or preventing access or downloads, as discussed above. *Kronenberg*, ¶ 31. In another example, *Costea* (Ex. 1013) teaches yet another system and technique for "tracing the spread of computer malware" that identifies the "source" of the malware using event information from a "minidump" stored in memory. *Costea*, Abstract, 3:8-18, 5:48-62, 8:38-58, 9:1-10, Fig. 4. Information relating to the pestware activity is transmitted to a server that maintains a database of crashes due to pestware, useful in confirming the spread of malware in a communication network. *Costea*, 2:33-47. Since *Gladstone* itself already teaches storing an IP address associated with the externally networked source of pestware, a PHOSITA would have found it obvious to store this same event data in the application file access embodiment for the reasons described above such that a trace could be performed to identify this particular source as the source of malware,

pursuant to *Pantuso. Gladstone*, 8:1-5. And just as above, a PHOSITA would have recognized that in generating and transmitting a report in response to identifying the activity, *Gladstone's* modified method would have accessed the event data 212 in security history 216 regarding the identified pestware activity.

87. Again, as before, a PHOSITA would have been motivated to perform this modification to further *Gladstone's* expressly-stated goal of inhibiting the spread of “malicious programs” (pestware) to “other computers within a network or data center by exploiting vulnerabilities of computer’s operating system or resident application programs.” *Gladstone*, 1:14-19, 2:21-32. Further, a PHOSITA would have recognized generating and transmitting a report in response to identifying pestware activity would have involved accessing security history 216 and the event data 212 stored therein to include this information in such a report. Such a report would reflect the cumulative monitored event data 212 relating to the monitored potential pestware activities. As explained above, a PHOSITA would have only needed to add known software features to hardware already present in *Gladstone* using programming skills available to a PHOSITA by adding *Pantuso's* tracing functionality to *Gladstone's* event correlation engine.

- (f) *[1(e)] reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.*

88. As I explained above, it would have been obvious to a PHOSITA to modify *Gladstone's* pestware identification method to store the externally networked source of suspected pestware (i.e., IP address or URL) in security history 216 in response to identifying a pestware object (application 220 and/or processes initiated by application 220). Indeed, a PHOSITA would have understood that connection 105 may not always be available, such that monitored and generated data, including the source of suspected pestware, would need to be stored to prevent data loss during times when a network connection fails, and that such data would naturally be stored in security history 216. Further, *Gladstone* additionally teaches transmitting this event data stored in security history 216 to a management center computer system 115 comprising a management center application 160. *Gladstone*, 6:13-15, 10:41-64, 12:56-13:8, 15:16-19, Fig. 7 (step 515). This architecture is reproduced below:



*Gladstone*, Fig. 1. The “management center 160 acts as a central repository for all event log records generated by the security agents 150” that analyzes the security history and updates a security policy to prevent future instances of this particular pestware on computers on the network. *Gladstone*, 6:16-18, 15:20-16:39. Since *Gladstone*’s management center 160 may be “remote” from the computer systems 110 (in contrast to processing occurring “locally” on the computers to which it is networked), a PHOSITA would have recognized *Gladstone*’s management center 160 teaches an “externally networked entity,” as claimed. *Gladstone*, 14:55-58, 10:41-49, 11:42-49. Specifically, a PHOSITA would have recognized that management center computer system 115 may be separated from host computer

systems 110 by a firewall, underpinning the understanding that the local computer system and management center 160 computer systems are separate and remote. *Gladstone*, 5:24-26. During prosecution, the Applicant explained generally that the entities are externally networked when they are connected via a “network,” and thus a PHOSITA would have understood *Gladstone*’s management center 160 is “externally networked” for the same reason. *’243 FH*, 63-76, 158-169.

89. Further, a PHOSITA would have considered *Gladstone*’s management center 160 to be a “pestware research entity” because it is described as “perform[ing] a correlation operation between security histories containing event data 212 for multiple computer systems 110,” confirming the presence of concurring data in security histories from multiple computer systems and marking it as violating a security policy. *Gladstone*, 6:8-15, 10:41-49, 11:42-49, 11:63-67, 15:26-16:10, Fig. 7. *Gladstone*’s management center then transfers an updated security policy back to the computer systems to prevent future pestware attacks of this type. *Id.* Thus, in this way, *Gladstone*’s system reports event data to its management center, which “researches” the pestware attacks at an “externally networked location.”

#### **Combination with *Pantuso***

90. Additionally or alternatively, *Pantuso* teaches a similar pestware identification system and method in which computer operations are monitored heuristically to identify and respond to activity due to pestware (viruses, worms,

Trojan horses). *Pantuso*, 1:25-33, 1:57-2:5, 4:15-20, Fig. 3. *Pantuso* expressly envisions its computerized method may provide, in response to identifying such activity, “an Internet Protocol (IP) address associated with the source” of the pestware activity. *Pantuso*, 6:8-20. *Pantuso* teaches reporting the source of the intrusion activity to a “central intrusion activity watch service” in an electronic message (e.g., email) that may be connected via a web interface (i.e., via the Internet). *Pantuso*, 6:8-20, Figs. 3,5. *Pantuso*’s central intrusion activity watch service constitutes an “externally networked pestware research entity” because it is (1) connected via the Internet to the computer system being monitored (thus, “externally networked”) and (2) researches the source of pestware for distribution to “notify the public of the source of the intrusion activity.” *Pantuso*, 6:8-20.

91. A PHOSITA would have found it obvious to combine the methods described by *Gladstone/Muttik* and *Pantuso* to provide reports to management center 160 or another externally networked pestware research entity, desirably enabling the pestware research entity to receive reports from and provide service to computers that are not close geographically and/or on the same local area network (LAN) as the first computer system experiencing the pestware activity. A PHOSITA would have recognized that, like a biological infection, protection against pestware is more effective the wider its coverage reaches, motivating the PHOSITA to include *Pantuso*’s external pestware research entity and furthering *Gladstone*’s express goal

of inhibiting the spread of “malicious programs” (pestware) to other computers by “exploiting vulnerabilities of the computer’s operating system or resident application programs.” *Gladstone*, 1:14-19, 2:21-32. A PHOSITA would have a reasonable expectation of success for the combination at least because *Pantuso*’s method is so similar to that of *Gladstone/Muttik* (which is already connected to the Internet) and would require only reprogramming of software, using only hardware already present and skills available to a PHOSITA. Such a modification would have constituted improving a known system (*Gladstone*’s pestware security system) via a known technique (*Pantuso*’s event data reporting to a research entity at an externally networked location), to achieve the benefit of increased awareness of sources of pestware distributed to vulnerable computer systems.

92. As discussed above regarding limitation 1(a), information regarding activity of suspected pestware is stored in event data 212 of security history 216. *Supra*, Claim 1(a). “Event data 212 can include things such as the identification of new connection requests made to the network interface driver 224... an application 220 accessing a particular file via an operating system call[.]” *Gladstone*, 7:17-24. Further, the security histories may contain a wide variety of relevant information, such as an indication of a specific security violation produced during the event, a detected processing instruction and/or program identity causing the event, a timestamp, procedure call or sub-routine information, file names of data to be

accessed, and/or dynamically linked library information. *Gladstone*, 12:1-24. A PHOSITA would have recognized that any or all of this information would have enabled a pestware research entity (e.g., *Gladstone's* management center 160) to research if the source is specifically a source of pestware. Specifically, the particular information envisioned by *Gladstone* being included in its transmission to management center 160 would have been utilized by the management center to “perform a correlation operation between security histories containing event data 212 for multiple computer systems 110.” A PHOSITA would have found it obvious to confirm the source is the source of pestware to ensure accuracy and accurately mitigate the spread of pestware prior to transmitting a report of pestware sources to other vulnerable computing systems to avoid false positives, leading to a loss of faith in the system and potential uninstallation and/or disuse. Thus, any or all of the types of event data collected and transmitted (e.g., a specific security violation produced, procedure call or sub-routine information, file names of data to be accessed, dynamically linked library information, etc.) would have enabled the externally networked pestware research entity (e.g., *Gladstone's* management center 160 and/or *Pantuso's* central intrusion activity watch service) to research whether the particular externally networked source (e.g., web site and/or URL from which application 220 was downloaded) is indeed a pestware source.

2. Claim 2 –...wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

93. As I discussed above, *Gladstone* in view of *Muttik*, or *Gladstone* in view of *Muttik* and *Pantuso* discloses a system and method that identifies the externally networked source of pestware—where such source is an IP address and/or URL. *Supra*, Claim 1(d).

94. I have been informed that in litigation, PO advances that “unrecited group members” may fall within the scope of this claim—meaning that sources of pestware not expressly mentioned above may be considered. In my opinion, it would have been obvious to a PHOSITA to additionally or alternatively store any other known sources of pestware. For example, this could include other network sources or computer-readable media sources. Indeed, it would have been obvious for *Gladstone*’s modified system to store other commonly known sources of potential pestware files to enhance coverage and reporting. These known sources are described in, for example, *Kronenberg*, disclosing sources “external to the computer system” from which events may originate, such as email clients storing attachments, web browsers storing downloaded files, and “special-purpose software retrieving files from network sources using any protocol, or installation of a software program on the computer system from a computer-readable media source.” *Kronenberg*, ¶ 0020, Fig. 2.

3. Claim 3 —...wherein the identifying includes accessing an activity log that includes information that relates the activity to the suspected pestware object.

95. As I discussed above, *Gladstone* teaches a pestware identification system that stores event data, including data from when an application makes calls to the operating system (i.e., API calls), related to potential pestware activity as part of security history 216. *Supra*, Claim 1(a). A PHOSITA would have recognized that security history 216 comprises an “activity log” as claimed. For example, API call activity is recorded in security history 216. *Id.* Additional information relevant to the event is also stored in security history 216, such as “the **identity of the application 220, the identity of the specific file to be accessed, and the type of access requested[.]**” *Gladstone*, 8:6-13, 7:15-24 (further describing storing information regarding an application 220 “accessing a particular file via an operating system call and report[ing] this as event data 212”). This stored data relates this API call activity to the suspected pestware application that performed it—specifically, application 220 in this example.

96. Furthermore, a PHOSITA would have understood or found obvious, based on these descriptions, that *Gladstone*’s method modified by *Muttik* would have “accessed” security history 216 when identifying application 220 as a suspected pestware object. For instance, *Gladstone*’s modified system would access security history 216 to apply weights to the recorded API call activity (as expressly described

in *Muttik*) and to identify application 220 as suspected pestware when the sum of the recorded weighted activities exceeds a threshold. As described above, the modified method then is able to trace the externally networked source of the pestware.

4. *Claim 6(c) – a research portion configured to access, in response to a prompt from the heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is configured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received; and*

97. As I discussed above regarding claims 1(c)-1(d), *Gladstone* modified by *Muttik* discloses a method and system which identifies an application 220 as a suspected pestware object on a computer. A PHOSITA would have recognized that in the modified *Gladstone/Muttik* system that *Gladstone*'s event correlation engine, modified to perform the steps described by *Muttik* for heuristic weighting and threshold comparison, teaches or at least includes a “research portion” that identifies application 220 as suspected pestware if the weighted factors exceed the threshold. This is consistent with the '243 Patent's disclosure. *243 Patent*, 2:62-65 (each module can be implemented as software in a single software package), 5:57-67 (“several functions may be consolidated into a single module”). I have been informed that PO interprets the “research portion” to refer to software, leading a PHOSITA to the understanding that *Gladstone/Muttik*'s heuristic event correlation

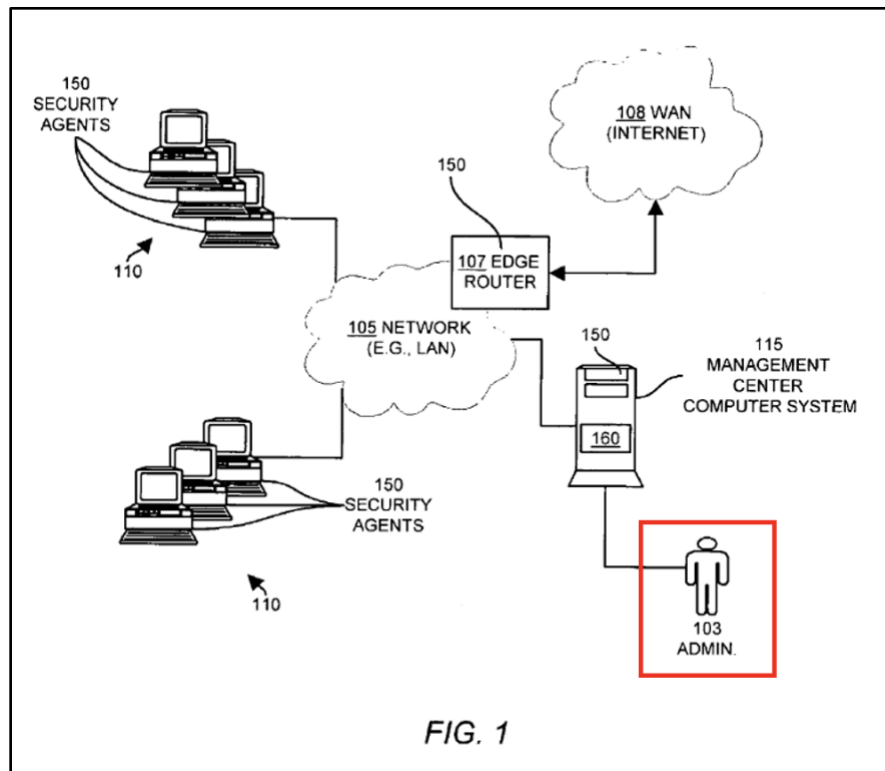
engine renders this limitation obvious. Ex. 1008 (*Responsive Markman Brief*), 40 (“‘research portion’ claim language refers to software”).

98. Additionally or alternatively, a PHOSITA would have found it obvious to include an independent “determination mechanism” (i.e., “research portion”) as taught by *Muttik* in *Gladstone*’s event correlation engine for determining if an application 220 “is likely to exhibit malicious behavior based upon” the sum of observed weighted activities comparison to a threshold. A PHOSITA would have had a reasonable expectation of success for this minor modification because it would have only required reprogramming of *Gladstone*’s already-present components to perform steps expressly described by *Muttik*, using skills available to a PHOSITA without undue experimentation.

99. The modified system would monitor and record API call computer activity, transmitting it to the security history 216 associated with the event correlation engine, which then performs the steps described by *Gladstone* and *Muttik* which includes analyzing the event data for pestware activity by “accessing” the stored data. A PHOSITA would have recognized that in doing so, the research portion is accessing each of the first set of recorded information (related to API call activity) and second set of recorded information (related to the source of the application 220). *Supra*, Claim 1(a). For example, *Gladstone* discloses that “[e]vent data 212 stored within a single security history 216 will contain **a set of records**

containing event data 212 that are reported from each interceptor 200 for a predetermined period of time of operation of the computer system 110.” *Gladstone*, 8:19-26. A PHOSITA would have understood this data to include information reported from the interceptors such as data relating to operating system calls by application 220 to access a particular file. When modified to also store the source of pestware activities, this data would also be stored in this “set of records.” In this way, the “set of records” contains a first and second set of recorded information, including event data reported from the interceptors and the sources of pestware.

100. It would have been obvious to a PHOSITA to modify the research portion to access these first and second sets of recorded information stored in one or more records upon an administrator request for source information. First, *Gladstone* discloses its networking environment connects an administrator to its system’s network components:



*Gladstone*, Fig. 1. The “administrator 103 uses the management center application 160 to create and distribute security policies to each computer system 110 to be protected.” *Id.*, 6:39-41, 13:24-38. To have the most up-to-date security policy or to determine the source of a particular event, it would have been obvious to enable the administrator to request updated event and source information. Indeed, the management center 160 is already in communication with security agent 150 (comprising the event correlation engine—i.e., heuristics module). *See, e.g., Gladstone* 11:4-9 (noting management center 160 can send “instruction[s]” to security agents 150). An administrator would therefore request report information of a particular event from the heuristics module, including source data, which would

prompt the research portion to access this data to generate such a report. This would provide additional data to an administrator for manual analysis. For example, as described in my opinions above, an administrator could use the “Trace this Event” or “Report this Event” tools described in *Pantuso* to perform such a request. *See, e.g., Pantuso*, 6:51-55 (noting the report icon may be selected to “transmit intrusion activity information to the central server for analysis in a manual fashion”). Such a modification would enhance administrator control over the system, providing detailed source information upon request to further mitigate detected pestware. A PHOSITA would have had a reasonable expectation of success making this modification for the reasons described in my opinions above concerning the combination with *Pantuso*, including because it would require simple programming changes to already present hardware in a network communication system already capable of the requisite communications.

101. Therefore, an administrator in *Gladstone’s* modified system would “prompt” the research portion of the event correlation engine to access this stored data to formulate a report, as described in my opinions below concerning limitation 6(d).

5. Claim 6(d) – a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware.

102. As I discussed above regarding claim 1(e), *Gladstone's* modified system or *Gladstone* as further modified by *Pantuso* discloses transmitting a report of the security history event data regarding a suspected pestware object to a remote management center 160 or central intrusion activity watch service to enable these entities to research whether the externally networked source is a source of pestware. A PHOSITA would have recognized that the security history 216 containing the relevant event data 212 teaches the claimed “report that identifies the externally networked source of the file” because *Gladstone* directly characterizes this step of its method as “reporting” event data. *Gladstone*, 10:54-64. A PHOSITA would have further recognized that the portions of *Gladstone* (or *Gladstone* in view of *Pantuso*) responsible for transmitting this report teach the claimed “reporting portion.” I have been informed that PO also interprets the “reporting portion” to refer to software, leading a PHOSITA to the understanding that *Gladstone/Muttik's* heuristic event correlation engine renders this limitation obvious. Ex. 1008 (*Responsive Markman Brief*), 43 (“reporting portion” “refers to software”).

103. Additionally or alternatively, a PHOSITA would have found it obvious, based on the disclosures of *Gladstone* and *Pantuso*, to transmit a “report” summarizing the event data related to the pestware activity to the remote management center 160 or central intrusion activity watch service, as disclosed by *Pantuso*. *Pantuso*, 5:58-60 (“a summary of the information relating to the intrusion activity associated with the source may be generated”), 6:8-13. This would further *Gladstone’s* goal of preventing dissemination of pestware through a network pursuant to *Pantuso’s* description of transmitting “a summary of the information relating to the intrusion activity associated with the source.” *Pantuso*, 5:58-60, 6:8-13. A PHOSITA would have appreciated a reasonable expectation of success making this simple modification to generate a “summary” or “support” as means to output the monitored security information to the remote management center 160 or central intrusion activity watch service.

6. *Claim 7 –...wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file.*

104. As I discussed above regarding claim 1(a), *Gladstone’s* pestware identification system and method monitors computer activity related to API calls, storing it in security history 216. *Gladstone* specifically states that information

stored may include “**process or program identities**, program counter information, procedure call or sub-routine information, file names of data to be accessed, dynamically linked library information, and so forth,” such that a PHOSITA would have understood that *Gladstone*’s system stores the identity of the particular process that performed the API call activity, as claimed. *Gladstone*, 12:7-12. *Gladstone* elaborates, explaining that the method “monitor[s] and record[s] processing behavior that results in an undesired processing operation” along with “recorded processing operations that led up to [the] undesired operation,” further indicating to a PHOSITA that the “identity” of the pestware-suspected process would have been stored as part of the identification of the events that “led up to the desired operation.” *Gladstone*, 5:42-61. Further, *Gladstone* is clear that the stored information includes “the identity of the specific file” that the application 220 accessed. *Gladstone*, 8:6-13, 7:15-24. Thus, a PHOSITA would have recognized that *Gladstone* teaches storing (1) an API call to access a file, (2) the identity of that accessed file, and (3) the identity of the application performing the API call. In this way, *Gladstone* stores a relation between each API call and at least one file. Namely, with respect to this “relation” between the API call and at least one file, *Gladstone* stores data related to the API call request to access a file, which includes information concerning the request and the file’s identity.

7. Claim 9 –...wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer.

105. As I discussed above, *Gladstone* teaches that event data regarding API call activity and the sources of pestware applications are each stored in security history 216 on a computing device. *Supra*, 6(c)-6(d). A PHOSITA would have recognized or at least found it obvious due to the well-known and widely-used nature of hard drives that the computing device would have stored the security history 216 on the hard drive of the computing device, and thus storing “on a file storage device of the computer.” *Gladstone* expressly articulates its system includes any requisite software and circuitry to perform the methods described, which a PHOSITA would have understood would have included a hard drive. *Gladstone*, 4:13-46. This is consistent with well-known hardware storage in computing systems. For example, *Kronenberg* illustrates that it was well-known to a PHOSITA to store pestware monitoring software and its monitored data on the hard disk drive of a computing device. *Kronenberg*, [0046]. A PHOSITA would have further understood or found obvious that each of these types of event data, regarding API call activity and pestware sources, would have been stored in the *same* security history file 216 on the hard drive of the computer system, such that this data is stored in the same “log file.” Indeed, it would have been obvious to store these two types of data relevant to

the same monitored activity in a common record to avoid unnecessary references between elements of different files.

**G. Opinions Regarding Ground 2: Gladstone in View of Muttik and English, or Alternatively, Gladstone in View of Muttik, Pantuso, and English renders Claims 1-8 and 10-14 Obvious**

1. Claim 4 —...wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the file

106. My opinions above in Ground 1 regarding the limitations of claims 1-3, 5-8, and 10-14 are incorporated by reference. As explained in the Petition, Ground 1 proposes rejections to claimed embodiments that store data regarding monitored potential pestware activities (e.g., application 220 making API calls to access a file) and the sources of the pestware (e.g., IP address or URL where the application was downloaded from) in the **same** storage component (e.g., security history 216). *See, e.g., '243 Patent*, Claim 9 (claiming activity information and source information stored in the same log file in a file storage device); claims 5, 11, and 14 (claiming source information stored in a variety of storage components, including in an “activity log,” the same log that stores other activity information claimed in independent claims 1, 6, and 12). Ground 2 captures other claimed embodiments which store activity information and source information in **separate** logic-based locations. *See, e.g., '243 Patent*, Claim 4 (claiming source information stored in a

browser cache compared to activity information stored in an “activity log” in claims 1, 6, and 12).

107. In Ground 2, a PHOSITA would have been motivated to modify *Gladstone’s* modified methods/system to store pestware source information in a browser cache, as disclosed by *English*, to facilitate source identification particularly when the source originates from Internet downloads.

108. For example, *English* teaches a system and method utilizing “native browser functionality” including a “cache area” that “log[s] the URL” of downloaded applications that may turn out to be pestware. *English*, 5:8-12. *English’s* system and method stores the source website of pestware, such as a “malware payload” or “spyware payload,” in an Internet browser’s cache “to determine the URLs that might be the source of the malware.” *English*, Abstract, 1:13-19, 1:57-2:13, 2:58-67, 4:11-32, 5:1-23, Fig. 2.

109. A PHOSITA would have recognized that *Gladstone’s* similar pestware identification system and method would have been modified using skills available to a PHOSITA, such as reprogramming of software in already-present hardware, to store event data 212 in a security history 216 comprising a browser cache as disclosed by *English. Gladstone*, 8:14-26; *English*, 5:1-23. This modification would have leveraged the well-known structure of a browser cache to “enable the user to

prevent re-installation of the malware” by tracing the source of pestware, motivating the combination. *English*, 1:30-37.

110. A PHOSITA would have had a reasonable expectation of success for the combination at least because *English* and *Gladstone* perform such similar methods of pestware identification using similar hardware, requiring only reprogramming well within the skill of a PHOSITA to store visited URLs in a browser cache and to access the browser cache when determining a source, a step already performed in *Gladstone*. A PHOSITA would have recognized the combination as combining a known technique (storing historical download source information in a browser cache, per *English*) into a known system (the modified *Gladstone* pestware identification system) ready for improvement to yield the predictable result of a system using its browser cache as at least part of security history 216.

111. With respect to this modification, a PHOSITA would have known that anti-virus programs typically have higher privilege levels than other common end-user applications, such as (1) a privilege allowing for determination of the threat level posed by or to various software entities and (2) the privilege to read the code and/or execution state of software entities, which would include a browser cache. Thus, a PHOSITA would have been successful modifying *Gladstone* to implement well understood processes to access and store a browser cache, as disclosed by

*English*, because these high privileges for Gladstone's security system would enable the system to read the code and/or execution state of a browser cache.

112. Additionally or alternatively, a PHOSITA would have found it obvious, based on *Gladstone's* explanation that security history 216 can be divided into individual components 216-1 through 216-X, to store the security history comprising event data in a separate logic location dedicated to storage of such data for simplicity and convenience of organization of the computer system's memory. Under such a configuration, activity data would be stored in a first dedicated logic-based storage location within security history 216, and source data (e.g., URLs visited) would be stored in a second logic-based storage location within security history 216.

#### IV. CONCLUSION

113. 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: June 22, 2023

By:   
\_\_\_\_\_  
Dr. Markus Jakobsson

# CV and Research Statement

Markus Jakobsson  
[www.linkedin.com/in/markusjakobsson](http://www.linkedin.com/in/markusjakobsson)  
[www.markus-jakobsson.com](http://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](http://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](http://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/](http://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.