

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETSKOPE, INC.,

Petitioner,

v.

FORTINET, INC.,

Patent Owner.

PTAB Case No. IPR2026-00474

U.S. Patent No. 11,449,623

**DECLARATION OF PAUL D. MARTIN, PH.D. IN SUPPORT OF
PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO.
11,449,623**

TABLE OF CONTENTS

I.	INTRODUCTION	1
A.	QUALIFICATIONS	2
1.	Professional Background	2
2.	Teaching.....	2
3.	Research.....	3
4.	Patents.....	8
5.	Industry	8
6.	Curriculum Vitae	12
B.	MATERIALS REVIEWED	12
C.	LEVEL OF ORDINARY SKILL IN THE ART.....	14
D.	SUMMARY OF MY OPINIONS.....	15
II.	OVERVIEW OF THE TECHNOLOGY.....	16
A.	PRIORITY DATE OF THE CLAIMS.....	16
B.	OVERVIEW OF RELEVANT TECHNOLOGY	17
1.	Cryptography Background.....	17
2.	Cryptographic Controls for File Access	20
3.	Risk-Based Scoring Systems	22
C.	THE '623 PATENT	26
D.	THE CHALLENGED CLAIMS	27
III.	UNPATENTABILITY OF THE '623 PATENT CLAIMS	28
A.	LEGAL STANDARDS.....	28

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

1.	Obviousness	28
B.	GROUND 1: COMBINATION OF CHENG AND BLECKMANN RENDERS CLAIMS 1-15 OBVIOUS	30
1.	Cheng	30
2.	Bleckmann	33
3.	Motivation To Combine.....	36
4.	Claim 1:.....	41
5.	Claim 2:.....	73
6.	Claim 3:.....	74
7.	Claim 4:.....	77
8.	Claim 5:.....	78
9.	Claim 6:.....	80
10.	Claim 7:.....	82
11.	Claim 8:.....	83
12.	Claims 9-15:.....	85
C.	GROUND 2: COMBINATION OF CHENG, BLECKMANN AND KIRTI RENDERS CLAIMS 2, 4, AND 10-13 OBVIOUS.....	95
1.	Motivation to Combine	96
2.	Claim 2:.....	100
3.	Claim 4:.....	101
4.	Claim 10-13	102
D.	GROUND 3: COMBINATION OF CHENG, BLECKMANN, AND VAN DIJK RENDERS CLAIMS 3, 9-13, AND 15 OBVIOUS	102

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

1.	Motivation to Combine	104
2.	Claim 3:.....	106
3.	Claims 9-13, 15:.....	106
E.	GROUND 4: COMBINATION OF FORD AND VAN DIJK RENDERS CLAIMS 1-15 OBVIOUS	107
1.	Motivation to Combine	109
2.	Claim 1:.....	110
3.	Claim 2:.....	126
4.	Claim 3:.....	127
5.	Claim 4:.....	135
6.	Claim 5:.....	136
7.	Claim 6:.....	138
8.	Claim 7:.....	139
9.	Claim 8:.....	140
10.	Claims 9-15	142
F.	GROUND 5: COMBINATION OF FORD, VAN DIJK, AND KIRTI RENDERS CLAIMS 2 AND 10-13 OBVIOUS	146
1.	Motivation to Combine	146
2.	Claims 2, 10-13:.....	149
G.	GROUND 6: COMBINATION OF FORD, VAN DIJK, AND BLECKMANN RENDERS CLAIMS 1-15 OBVIOUS	150
1.	Motivation to Combine	150
2.	Claim 1	152

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

H. GROUND 7: COMBINATION OF FORD, VAN DIJK,
BLECKMANN AND KIRTI RENDERS CLAIMS 2 AND 10-
13 OBVIOUS 154

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

LIST OF APPENDICES

Appendix A *Curriculum Vitae* of Paul Martin, Ph.D.

I. INTRODUCTION

1. I, Paul Martin, have been retained by Petitioner Netskope, Inc. (“Petitioner”) to investigate and opine on certain issues relating to United States Patent No. 11,449,623 (“the ’623 patent”) in its Petition for *Inter Partes* Review (IPR2026-00474) of that patent. The Petition requests that the Patent Trial and Appeal Board (“PTAB” or “Board”) review and cancel claims 1-15 of the ’623 patent. I have analyzed the claims of the ’623 patent in numerical order.

2. The opinions set forth in this declaration are based on my personal knowledge, my professional judgment, and my analysis of the materials and information referenced in this declaration and its exhibits.

3. If called upon to testify, I could and would testify to the truth of the following.

4. The company for which I work, Harbor Experts, is being compensated at the rate of \$775 per hour for time that I spend on this case. Harbor Experts is also being reimbursed for my reasonable and customary expenses. I receive no other forms of compensation related to this case. My compensation does not depend on the outcome of this *inter partes* review or the co-pending district court litigation, and I have no other financial interest in this post-grant review.

5. I understand that the ’623 patent has been assigned to Fortinet, Inc.

6. This declaration is based on the information currently available to me.

To the extent that additional information becomes available, I reserve the right to continue my investigation and study, which may include a review of documents and information that may be provided, as well as testimony from depositions that have not yet been taken.

A. QUALIFICATIONS

1. Professional Background

7. I am the Chief Scientist at Harbor Experts, Inc. and a part-time Lecturer in the Department of Computer Science at Johns Hopkins University. I hold B.S., M.S.E., and Ph.D. degrees from Johns Hopkins University, with all degrees, including my doctorate, being in computer science.

2. Teaching

8. I am a part-time lecturer in the Department of Computer Science at Johns Hopkins University. I currently teach classes on computer and network security and applied cryptography, and C and C++ programming, developer tools and Linux environments. In the past I have taught classes on the topic of hardware hacking, including analyzing, modifying, and repairing computer hardware and embedded devices and vulnerability analysis and exploitation. I also occasionally substitute teach classes on network security and cryptography.

9. My classes cover a diverse array of topics including hardware and software security design, analysis and reverse engineering for vulnerability assessment; hardware and software-based attacks on computer components including RAM and CPUs; applied cryptography; computer architecture; computer networking; and component-level repair and modification. My classes also utilize hardware and software emulation and virtualization techniques in order to present students with a variety of real-world environments in which to learn and perform hands-on projects.

3. Research

10. In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University. In fall 2011, I began working towards my Ph.D. in computer science, also at Johns Hopkins University, and I began researching computer security and privacy systems in order to both design novel technologies for securing computing systems and to also bridge the interface gap between users and their technology. As such, my research focused not only on developing technical solutions to novel security and privacy systems but to also presenting these solutions in a way that non-technical users could understand. Part of my research also focused on non-deterministically generating virtualized computer networks in order to provide malware education environments for students. I also developed an emulator for analyzing malware code segments as part of a student

project with the NSA. This emulator was integrated into an IDA Pro plugin and was able to observe how binary instruction snippets taken from malware samples modified their computing environment.

11. During my tenure as a Ph.D. student at Johns Hopkins, I was fully funded as a research assistant and/or teaching assistant throughout all of my semesters. I was a member of the Upsilon Pi Epsilon computer science honor society, as well as its treasurer for the 2014-2015 school year. I was also a member of the Johns Hopkins chapter of the Association for Computing Machinery. I earned an award for outstanding teaching assistant in the Computer Science department for the year 2014-2015. I co-instructed a short course called, “Introduction to Hardware Hacking,” with a colleague, Dr. Michael Rushanan, which was the highest-rated course in the computer science department (based on student reviews) during the winter session in which it was offered. In this course, we offered lessons on a variety of topics including modifying game consoles and device firmware; electronics repair; binary analysis and modification, network traffic analysis; and web-based vulnerability assessment and exploitation.

12. During my time as a student at Johns Hopkins, I also participated in numerous kinds of service to the department. I represented the university as a student speaker at numerous open houses and admitted student days to help introduce prospective students to the computer science department. I was selected

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

to speak to the external advisory board for the computer science department to provide insight into the student experience in the department. I served the department as the faculty liaison czar for several semesters, in which I attended and documented faculty meetings, which I then summarized for the students in the department. I also mentored and supervised a high school student on a year-long student project in software design and I supervised a variety of undergraduate research assistants on some of my research projects.

13. I finished my Ph.D. by successfully defending my dissertation, entitled “Securing Medical Devices and Protecting Patient Privacy in the Technological Age of Healthcare,” on February 12, 2016, at the age of 26. My doctoral thesis tells the story of a secure healthcare practice of the future in which technology is seamless to use for healthcare providers while providing a much higher standard of security than is typical today. It focuses on the juxtaposition of usability and security with an emphasis on simplicity, automation, and error-proofing of security controls.

14. During my doctorate and afterward, I have produced, peer-reviewed, and published research in areas such as fingerprinting, anomaly detection, multifactor authentication, and embedded systems security. In many of these cases, I focused not only on designing novel security systems but also on designing usable web-based security systems for controlling them and understanding their

data output. In fact, some of my research has formed the basis for commercial products and services. For example, in my work on integrated audit and access control, which was funded in part by Accenture Labs, I developed a Hadoop-based application to perform large-scale statistical analysis of audit logs from an electronic medical record system. As part of this work, I also designed a web application to automatically produce human-readable reports and graphs for use in consulting. Accenture subsequently patented this technology.

15. Similarly, in my research at Applied Communication Sciences in 2013, I designed and implemented a web-based traffic visualization dashboard and analysis system for field area smart grid networks that could be used to quickly gain an understanding of the current state of a SmartGrid network as well as to detect unexpected anomalies in the network. This dashboard was able to aggregate and visualize multiple data streams in realtime. Applied Communication Sciences subsequently patented this work and continued to build on the project. To my knowledge, they sold and/or still sell this product as part of their SecureSmart Managed Security Service product offering.

16. I have worked on and published two research projects related to improving the quality and ease-of-use of authentication technologies, especially in healthcare settings. In one project, I and my co-authors designed an indoor location tracking system consisting of unspoofable Bluetooth Low Energy beacons. These

beacons were placed around a building and mapped to a backend such that a user could report which beacons he or she was within range of in order to be used as a secondary authentication mechanism for accessing patient medical records. In the way that we designed and envisioned the system, a doctor would log into a mobile device which would connect to a web-based backend. As the doctor walked past patient rooms, he or she would be automatically presented with medical records of nearby patients. In another project, I and my co-authors designed an authentication bracelet that would receive a Kerberos ticket upon login to a modified computer terminal through use of low-energy electrical signals transmitted over the wearer's skin. Upon use of other terminals throughout the hospital, this Kerberos ticket could be sent back over the wearer's skin to the custom contact on the terminal in order to allow the user to login without a password. The bracelet was also designed to immediately lose the cryptographic secret upon being removed from the user.

17. My recent research has focused primarily on embedded systems security with an emphasis on binary analysis, anomaly detection and automated security enforcement. In one case, I designed a security system that can be soldered directly to the CPU of embedded devices in order to perform control-flow integrity for purposes of profile building and enforcement. In another case, I designed a system to automatically discern name and version information from binaries on embedded devices in order to build a software profile of the platform configuration

of the device which can then be cross-referenced with a vulnerability database. I have also written a patent on this specific technique.

18. In 2023 and 2024, I served as a member of the program committee for the IEEE Symposium on Security and Privacy. As a member of this committee, I peer reviewed research that was submitted for publication at the Symposium, including research on cryptographic protocols, memory forensics, cryptographic side channel attacks, cryptographic password vaults, differential privacy, computational theory, memory module design, and hardware security.

4. Patents

19. I am a named inventor on six U.S. patents. A full listing of these patents can be found on my attached vita.

5. Industry

20. I began working in the software industry in 2008, when I obtained my first independent consulting client—Brandeis University. I created a program for their computer repair shop's ticketing system to interface with a label printer. This enabled the computer repair shop to automatically print labels associated with tickets in order to easily identify customers' devices.

21. Shortly after finishing my engagement with Brandeis University, I began working for the Johns Hopkins University Digital Research and Curation Center as a student programmer. There, I created a batch importer for a digital

archiving system called DSpace in order to enable hundreds of digitally archived works per week to automatically be added to the repository. I next ported a web interface for statistics tracking and visualization to the same digital archiving system in order to allow library staff to more easily visualize and understand data about how the digital archiving system was being used through a common web-based interface.

22. In 2009, I began working for a security consulting company called Independent Security Evaluators in Baltimore, Maryland. I worked on a wide variety of security and privacy projects including projects to test and break the DRM scheme of a magazine distribution application for iOS and Android (at the behest of the developer of said application), projects to test implementation code for cryptographic secret splitting, projects to assist with fuzz testing for security vulnerabilities of a variety of software applications, software development projects to automate testing of antivirus and antimalware solutions, and a variety of other security-related projects. Of note, I designed automation systems to create and restore virtualized snapshots of Windows machines on which I tested antivirus software on actual malware samples as part of a project for Consumer Reports. I worked for ISE throughout the semesters and summers until August 2011. In 2010, I also designed a security architecture for a large-scale digital curation system

meant to be a major inter-university initiative to create a successor to existing digital curation systems that could be used for decades.

23. In spring 2011, I completed my bachelor's in computer science at Johns Hopkins University, and I also retained an independent consulting client, the University of Michigan, for whom I performed a penetration test and security assessment of a cloud-based research system that they planned to deploy.

24. In February 2016, I joined Harbor Labs full-time as a research scientist. In 2018, I was promoted to Director of Firmware Security. In December 2023, I was promoted to Vice President of Applied Research and Technology. In October 2024, the division of Harbor Labs that I managed became Harbor Experts. I became Chief Scientist at Harbor Experts during this time. At Harbor Experts, I manage client engagements related to all of the analysis work that Harbor Experts performs. I also lead Harbor Experts' research projects.

25. A substantial portion of my role at Harbor Experts is in managing source code review engagements. As part of this work, I have reviewed software systems of varying sizes, often totaling in the millions or billions of lines of code. I have reviewed products in the security space, television-based set top boxes, network appliances, numerous web-based enterprise systems, email management systems, telephony products, embedded system bootloaders, social network platforms, virtualization platforms, and countless other products.

26. Prior to joining Harbor Experts, I was also the technical and development lead for a firmware security analysis engine for a product developed at Harbor Labs called Firmware IQ. Firmware IQ is designed to analyze the firmware of embedded devices for security vulnerabilities in an automated fashion. In one configuration of the product, a developer uploads a firmware image to a web-based portal which uses a broker to forward the firmware to an engine for analysis. The engine unpacks the firmware, breaks it into its constituent components, and then performs more than a hundred automated security checks in order to find vulnerabilities in the firmware image. The results are then reported through JSON to a web-based presentation system which displays them in an interactive fashion. Since Firmware IQ, I have devoted a substantial portion of my time to incorporating lessons learned from analyzing large numbers of firmware images into my own Linux distribution, which I am currently in the process of releasing. This distribution is intended to address several gaps in the current market and will provide improved stability, reliability, and performance relative to existing Linux distributions.

27. A more detailed list of my engagements can be found on my attached vita.

6. Curriculum Vitae

28. A copy of my curriculum vitae (CV) is attached as Appendix A to this declaration.

B. MATERIALS REVIEWED

29. My opinions expressed in this declaration are based on documents and materials identified in this declaration, including the '623 patent and its prosecution history, the prior art references and background materials discussed in this declaration, and the other references specifically identified in this declaration. I have considered these materials in their entirety, even if only portions are discussed here. The following is an exemplary list of the materials on which I based my opinion.

Exhibit No.	Description
1001	U.S. Patent No. 11,449,623
1002	Prosecution History of U.S. Patent No. 11,449,623 (the "'623 Prosecution History")
1005	U.S. Patent Application Publication 2013/0232543 A1 ("Cheng")
1006	U.S. Patent Application Publication 2009/0144813 A1 ("Bleckmann")
1007	U.S. Patent 8,978,159 ("Van Dijk")
1008	U.S. Patent 10,063,654 ("Kirti")
1009	International Patent Application 2015/164521 A1 ("Ford")

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

Exhibit No.	Description
1010	U.S. Pat. Pub. No. 2019/0319945 (“Levy”)
1011	U.S. Pat. Pub. No. 2004/0221172 (“Stamos”)
1012	Reserved
1013	Archived capture of webpage from Cisco.com titled ‘What Is Encryption?’ (Internet Archive Wayback Machine: https://www.cisco.com/site/us/en/learn/topics/security/what-is-encryption.html), captured Sep 14, 2026
1014	Archived capture of webpage from Okta.com titled ‘RSA Encryption: Definition, Architecture, Benefits & Use’ (Internet Archive Wayback Machine: https://www.okta.com/identity-101/rsa-encryption/), captured Sep 14, 2026
1015	Archived capture of webpage from csrc.nist.gov titled ‘Policy Based Access Control (PBAC)’ (Internet Archive Wayback Machine: https://csrc.nist.gov/glossary/term/policy_based_access_control), captured Sep 14, 2026
1016	Archived capture of webpage from csrc.nist.gov titled ‘Risk Adaptive (Adaptable) Access Control’ (Internet Archive Wayback Machine: https://csrc.nist.gov/glossary/term/risk_adaptive_adaptable_access_control), captured Sep 14, 2026
1017	Archived capture of webpage from Microsoft.com titled ‘Risk-based access policies’ (Internet Archive Wayback Machine: https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-policies), captured Sep 14, 2026
1018	Archived capture of webpage from csrc.nist.gov titled ‘A Survey Of Access Control Modules’ (Internet Archive Wayback Machine: https://csrc.nist.gov/csrc/media/events/privilege-management-workshop/documents/pvm-model-survey-aug26-

Exhibit No.	Description
	2009.pdf), captured Sep 14, 2026
1019	Archived capture of webpage from ibm.com titled ‘What is machine learning?’ (Internet Archive Wayback Machine: https://www.ibm.com/think/topics/machine-learning), captured Sep 14, 2026

30. I have also relied on my own experiences in encryption, network security technologies, client-server architectures, and computer systems security.

C. LEVEL OF ORDINARY SKILL IN THE ART

31. I am not an attorney and offer no legal opinions. I have been informed about certain aspects of the law for purposes of my analyses and opinions.

32. I understand that in analyzing questions of invalidity, the perspective of a person having ordinary skill in the art (“POSITA”) is often implicated, and the Court may need assistance in determining that level of skill.

33. I understand that the claims and written description of a patent must be understood from the perspective of a POSITA. I have been informed that the following factors may affect the level of skill of a POSITA: (1) the educational level of the inventor; (2) the type of problems encountered in the art; (3) the prior-art solutions to those problems; (4) the pace of innovation; (5) the sophistication of the technology; and (6) the educational level of active workers in the field. A person of ordinary skill in the art is also a person of ordinary creativity in the art.

34. Based on my experience in network security system design, as well as my reading of the '623 Patent, it is my opinion that a person of ordinary skill with respect to the subject matter of the '623 Patent at the time of the alleged priority date of the '623 Patent in March 2019 would have had at least a B.S. degree in computer science, computer engineering, or electrical engineering (or equivalent experience) and/or would have had at least two years of practical experience in analyzing or implementing network security, data access controls, or key management. This definition is flexible, and additional educational experience in computer science could make up for less work experience and vice versa.

35. I am at least a person of ordinary skill in the art and was so on the date to which the '623 Patent claims priority. As shown by my qualifications and my curriculum vitae attached as Appendix A, I am aware of the knowledge and skill possessed by a person of ordinary skill in the art at the time of the priority date of the '623 Patent. In performing my analysis, I have applied the standard set forth above.

D. SUMMARY OF MY OPINIONS

36. I have reviewed and analyzed the '623 patent.

37. Based on my review and analysis, it is my opinion that claims 1-15 of the '623 patent are invalid based on the following grounds:

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

Ground	Basis	Reference(s)	Challenged Claims
1	§103	Cheng and Bleckmann	1-15
2	§103	Cheng, Bleckmann, and Kirti	2, 4, 10-13
3	§103	Cheng, Bleckmann, and Van Dijk	3, 9-13, 15
4	§103	Ford and Van Dijk	1-15
5	§103	Ford, Van Dijk, and Kirti	2, 10-13
6	§103	Ford, Van Dijk, and Bleckmann	1-15
7	§103	Ford, Van Dijk, Bleckmann, and Kirti	2, 10-13

II. OVERVIEW OF THE TECHNOLOGY

A. PRIORITY DATE OF THE CLAIMS

38. I have been informed that a U.S. patent application may claim the benefit of the filing date of an earlier patent application if the earlier patent application sufficiently discloses the invention claimed in the later-filed U.S. patent application. I have also been informed that priority is determined on a claim-by-claim basis so that certain claims of a patent may be entitled to the priority date of an earlier-filed patent application even if other claims of the same patent are not entitled to that priority date.

39. I have also been informed that a patented claim is invalid if the claimed invention was patented, described in a printed publication, or in public

use, on sale, or otherwise available to the public before the effective filing date of the claimed invention, or the claimed invention was described in an issued patent or in an application for patent published or deemed published and that was effectively filed before the effective filing date of the claimed invention.

40. I understand that the claims of the '623 Patent are entitled to a priority date of March 22, 2019, which is the date on which the application for the '623 Patent was filed.

B. OVERVIEW OF RELEVANT TECHNOLOGY

1. Cryptography Background

a. Symmetric Key Cryptography

41. Cryptography is the study and application of mathematical techniques used to protect information from unauthorized access, disclosure, alteration, or misuse. It is a fundamental component of modern information security and is commonly employed to secure electronic communications and data exchanged between individuals, computer systems, networks, and other entities. The primary purpose of cryptography is to provide mechanisms that allow information to be securely stored and transmitted while preventing unauthorized parties from accessing or understanding the protected information.

42. Cryptography consists of two general methods for altering the readability of information: encryption and decryption. Encryption is the practice of

converting readable information into unreadable information through use of a “key;” decryption is the inverse. A POSITA would refer to readable information as plaintext and encrypted information as ciphertext.

43. In cryptographic terms, the “key” is the value or piece of information that determines how the cryptographic algorithm transforms the plaintext into ciphertext. Humans have used “keys” to encrypt communications since antiquity to prevent intercepted messages from being understood. For example, Julius Caesar was reputed to have encoded letters he wrote using a cipher that today would be called a shift cipher. A shift cipher encrypts a message in text by replacing each letter in the original message with a substitute letter that follows the original letter by a fixed number of positions in the alphabet. The value of that fixed number is called the “shift.” For example, applying a shift cipher with a shift of 3, one would replace every ‘A’ in the original message with a ‘D’ in the encrypted message, and every ‘B’ with an ‘E,’ and so forth.

44. For a shift cipher like the above, the key is the numerical value of the shift, e.g., a key of 3 in the shift cipher above. During decryption, the key is used to determine the corresponding reverse transformation needed to recover the original plaintext. If an incorrect key is used for the shift cipher above, e.g., a key of 5, then the incorrect key could not be used to successfully decrypt the ciphertext into the correct plaintext. Of course, for an encryption algorithm as primitive as shift

cipher, it would be fairly straightforward to guess the value of the key through trial and error because the key can only take 25 possible values. Modern cryptographic algorithms are therefore much more sophisticated than the shift cipher described above.

45. The combination of encryption, decryption, and key generation algorithms comprise a cryptosystem. There exist two types of cryptosystems: symmetric and asymmetric.¹

46. **Symmetric (shared) key cryptosystems** use the same private key for encryption and decryption. An obvious issue with symmetric cryptosystems is the challenge of securely distributing the shared secret key between the parties involved in encryption and decryption. The key must be exchanged or established without allowing an unauthorized party to intercept or obtain it. Since the security of the communication depends on keeping the key secret, any compromise of the key can undermine the confidentiality of the encrypted communication.

47. On the other hand, **public key (asymmetric) cryptosystems** use a key pair consisting of two unique keys: a private key and a public key. These keys are mathematically bound such that a plaintext encrypted with the public key can only be decrypted with the corresponding private key. For example, a public key of

¹ Ex-1013.

the entity Bob may be uploaded to a publicly accessible server on the Internet. If and when the entity Alice wants to communicate securely with Bob, she would download his public key and encrypt her message to him using this public key. She then transmits this ciphertext to Bob, who is the only holder of the associated private key, and thus is the only entity that can decrypt the message. Like the symmetric cryptosystem, the private key must be kept secret by Bob because its loss breaks secure communication afforded by encryption. An example asymmetric cryptosystem that would have been known by a POSITA at the time is RSA.²

2. Cryptographic Controls for File Access

a. Policy-Based Controls

48. Protecting files and other information resources from unauthorized disclosure is a common and important security requirement. To this end, many organizations and entities have researched and created cryptographic file protection systems that facilitate the online distribution of digital content while also restricting the usage of said content to be in accordance with a set of narrowly defined and sanctioned policies.

49. Specifically, encryption alone cannot reliably enforce access for only a defined period. In a system that only utilizes encryption to regulate file access,

² Ex-1014.

once a user is granted the ability to decrypt a file (meaning that the user is given the decryption key to an encrypted file), that capability to decrypt the file may persist indefinitely unless additional controls are imposed. Therefore, achieving finite-duration access usually requires policy-based mechanisms that define a specific cutoff point and revoke or restrict access once that period expires, such as at the end of an individual's employment with an organization.³

50. A POSITA would be familiar with Policy-Based Access Control (PBAC)⁴, a mechanism that controls access by applying predefined policies that specify the conditions under which a user may access a particular resource. These policies may consider attributes such as user identity, role, clearance, operational need, risk, heuristics, but usually require the policies to be predefined and continuously maintained as users, resources, and circumstances change. "For example, if an employee of an organization is granted access to sensitive company data, when that employee leaves the organization, his/her access must be revoked by altering the file access control policy. Similarly, when an employee joins the organization, policies must be added for the new employee."⁵

³ Ex-1001, 1:46-58.

⁴ Ex-1015.

⁵ Ex-1001, 1:63-2:1.

51. In addition, heuristic approaches can be used in RBAC to infer appropriate roles and access permissions from observed user behavior, organizational patterns, or existing access assignments. These methods can help identify likely roles of an accessing user, or potential risks associated with an action, then recommend access decisions when explicit role definitions are incomplete or difficult to maintain. Under these circumstances, RBAC may be implemented with other access control mechanisms like Risk Adaptive Access Control.

3. Risk-Based Scoring Systems

a. User Behavioral-Based Systems

52. A POSITA would be familiar with Risk Adaptive Access Control (or generally “risk-based access control”),⁶ a mechanism that evaluates access requests according to the level of risk associated with a user, resource, and access context, rather than relying solely on predefined permissions. National Institute of Standards and Technology (NIST), as an example, has been trying to define and standardize Risk-Adaptive Access Control since at least 2009.⁷ A risk score can be derived from factors such as user behavior, device characteristics, location, access

⁶ Ex-1016. *See also* Ex-1017.

⁷ Ex-1018 (NIST publicly circulated a Risk-Adaptive Access Control working draft in connection with its 2009 Privilege Management Workshop).

history, and the sensitivity of the requested resource, with higher-risk requests subject to additional verification or restricted access.

53. User behavioral-based risk scoring systems provide a mechanism for evaluating access requests based on deviations from a user's established patterns of activity. Rather than treating authorization as a static decision determined solely by predefined roles or permissions, these systems incorporate behavioral attributes such as "history of general file access by the user, current location of the user, history of location of the user, time of access request, time when the user typically accesses a file, whether the user is accessing from [sic] a trusted location or an untrusted location, behavior of the user's peer group as determined by either a list obtained from a directory services server or as measured by behavior of multiple users associated with the enterprise."⁸ A risk score can then be assigned to a user or access request by comparing current activity against a behavioral baseline. Access decisions may subsequently be made according to predefined risk thresholds, allowing normal behavior to proceed while triggering additional verification, restricting access, or denying requests that exhibit elevated risk.

54. A key advantage of behavioral-based scoring is its ability to provide more adaptive access control in environments where user behavior and security

⁸ Ex-1001, 6:7-16.

conditions change over time. Heuristic techniques can be used to identify user behavior that differs significantly from expected patterns.

55. Another key advantage of behavioral-based scoring is that it can support continuous security monitoring by evaluating user behavior. This allows security systems to detect emerging risks in real time and respond before potentially harmful activity causes significant damage.⁹

b. **Machine Learning-Based Scoring**

56. Machine learning (ML) is a type of artificial intelligence (AI) that allows computers to “learn” the patterns of training data and, subsequently, make accurate inferences about new data.¹⁰ Instead of following only specific instructions, a machine learning system identifies patterns in data and uses those patterns to make predictions or decisions.

57. For example, a machine learning system can be trained on information regarding historical user behavior to “learn” normal behavior.¹¹ This type of

⁹ *Id.*, 3:13-26.

¹⁰ Ex-1019.

¹¹ Ex-1018: “RAdAC [Risk-Adaptive Access Control] also takes a probabilistic, heuristic approach to determine whether the access should be granted under the circumstances. The heuristics include a historical record of access control decisions and **machine learning**.” (Emphasis added.).

machine learning system contributes to implementing Risk Adaptive Access Control systems discussed in the section above. As also discussed above, historic user behavior that could be used as training data may include “history of general file access by the user, current location of the user, history of location of the user, time of access request, time when the user typically accesses a file, whether the user is accessing from [sic] a trusted location or an untrusted location, behavior of the user’s peer group as determined by either a list obtained from a directory services server or as measured by behavior of multiple users associated with the enterprise.”¹²

58. Then, the machine learning system can be employed to analyze a new file access request at issue to “determine a measure of abnormality or deviation from normal user behavior.”¹³ The machine learning system then helps organizations to identify unusual or potentially risky activity and take appropriate action.

59. The measure of abnormality or deviation, generated by the machine learning system regarding a new file access request, can be represented by a numerical value, score, probability, or other indication of risk. For example, a

¹² Ex-1001, 6:7-16.

¹³ *Id.*, 8:20-43.

relatively low risk score can indicate that the file access request is substantially consistent with historical behavior of the user, while a relatively high risk score can indicate that the file access request differs from historical behavior in one or more respects.¹⁴ The risk score can be based on multiple characteristics of the file access request. For example, an access request “at 3:00 a.m. through a network other than the enterprise network” may receive an elevated risk score from the machine learning system; “[a]lternatively, when the user accesses the file during working hours using the enterprise network, the activity can be viewed as relatively normal and be assigned a low risk score.”¹⁵

C. THE '623 PATENT

60. The '623 patent concerns “[s]ystems and methods for a machine-learning driven fine-grained file access control approach.” Ex-1001 at 2:66-67.

61. The patent describes a network architecture that obtains and stores information regarding historical network users’ behavior by observing file access requests. This architecture includes a management server, a permission server, and an analytics server residing within an enterprise network, connected to client machines. Files within the enterprise network are stored in encrypted form to

¹⁴ *Id.*, 12:48-57.

¹⁵ *Id.*

prevent access without validation of a user's rights to access the file. When a user initiates a file access request, the system determines a risk score for the user based on a plurality of factors, including the user behavior information and observed data from the request. *Id.* at 14:14-62.

62. Based on the resulting risk score, access is permitted or denied by returning or withholding the decryption key. The patent discloses a three-tier, two-threshold access scheme: if the risk score is less than a first threshold, the permission server provides full access by returning the decryption key; if the risk score falls between the first and second thresholds, the permission server provides limited access by returning the decryption key with limitations, the only such disclosed being directing the user to access the file through a lower-risk channel (via VPN); and if the risk score exceeds the second threshold, the permission server blocks access entirely by withholding the decryption key. *Id.* at 6:16-24.

D. THE CHALLENGED CLAIMS

63. I understand that claim terms generally are construed in accordance with the ordinary and customary meaning they would have to a POSITA at the time of the invention in light of the claim language, the specification, and the prosecution history. I understand that dictionaries and other extrinsic evidence may be considered as well, though such evidence is typically regarded as less

significant than the intrinsic record in determining the meaning of the claim language.

64. For all terms of the challenged claims of the '623 patent, I have afforded them their ordinary and customary meaning in light of the intrinsic evidence at the time of the invention on March 22, 2019.

III. UNPATENTABILITY OF THE '623 PATENT CLAIMS

A. LEGAL STANDARDS

1. Obviousness

65. I am informed and understand that a patent cannot be properly granted for subject matter that would have been obvious to a person of ordinary skill in the art at the time of the alleged invention, and that a patent claim directed to such obvious subject matter is invalid under 35 U.S.C. § 103. It is also my understanding that in assessing the obviousness of claimed subject matter, one should evaluate obviousness in light of the prior art from the perspective of a person having ordinary skill in the art at the time the alleged invention was made (and not from the perspective of either a layman or a genius in that art). It is my further understanding that the question of obviousness is to be determined based on:

- The scope and content of the prior art;

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

- The difference or differences between the subject matter of the claim and the prior art (whereby in assessing the possibility of obviousness one should consider the manner in which a patentee and/or a Court has construed the scope of a claim);

- The level of ordinary skill in the art at the time of the alleged invention of the subject matter of the claim; and

- Any relevant objective factors (the “secondary indicia”) indicating nonobviousness, including evidence of any of the following: commercial success of the products or methods covered by the patent claims; a long-felt need for the alleged invention; failed attempts by others to make the alleged invention; copying of the alleged invention by others in the field; unexpected results achieved by the alleged invention; praise of the alleged invention by the alleged infringer or others in the field; the taking of licenses under the patent by others and the nature of those licenses; expressions of surprise by experts and those skilled in the art at the subject matter of the claim; and whether the patentee proceeded contrary to accepted wisdom of the prior art.

- Any relevant objective factors (the “secondary indicia”) indicating obviousness: independent invention of the claimed invention by others before or at about the same time as the named inventor thought of it; and other evidence tending to show obviousness.

**B. GROUND 1: COMBINATION OF CHENG AND BLECKMANN
RENDERS CLAIMS 1-15 OBVIOUS**

1. Cheng

66. Cheng is directed to “controlling access to data, and more particularly to providing server control for access to client data on a mobile device.” Ex-1005, [0004].

67. Cheng discloses a data protection system that processes requests from mobile devices for data items, such as files, and corresponding decryption keys by using a policy decision module to determine whether a user is currently eligible to access an encrypted data item. The policy decision module determines eligibility based on an accumulated authentication score representing the level of confidence that the authenticated user of the mobile device is its current user, that score compared to a minimum score required for access. The module includes a risk engine that assesses the likelihood that a data item may be leaked or misused, based on the sensitivity score of the data item, the access history, and the deviation of the most recent access patterns from longer-term access patterns in the access history. If the request for data item and the corresponding decryption key includes authentication or context information, the authentication and context history store may first be updated. *Id.*, [0063], [0064], [0067].

300

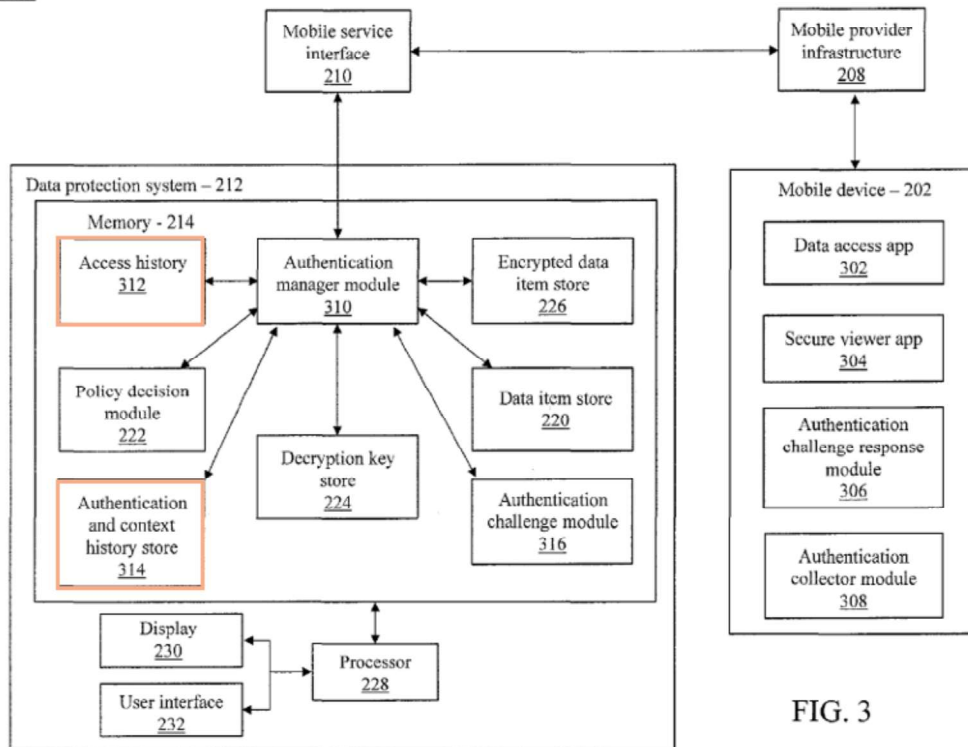
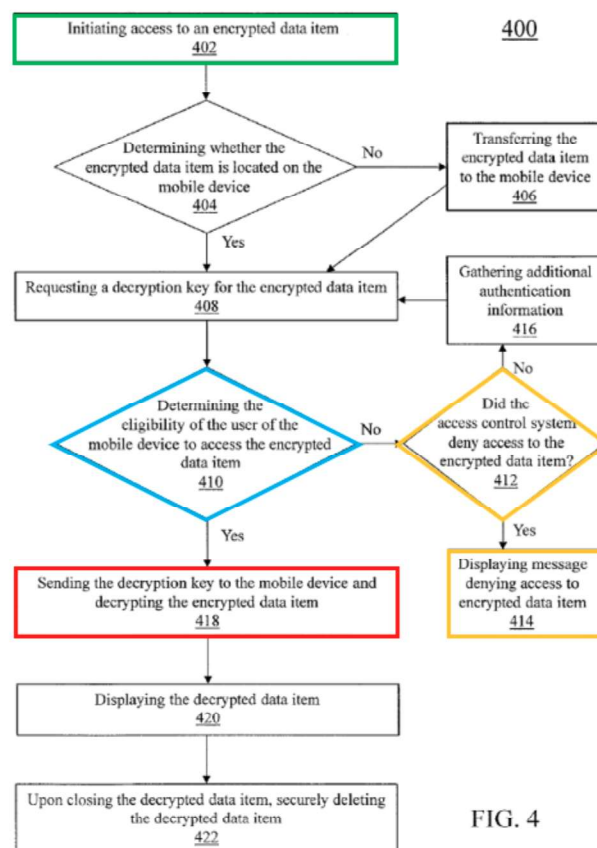


FIG. 3

Id., Fig. 3 (orange outlining added).

68. Cheng discloses a server-based data protection architecture in which encrypted data items are stored on a server and can be transferred to a mobile device. Users request access from the server to the encrypted data item, the server evaluates the request against a confidence score derived from authentication history, access history, and current device context; the server then permits or denies access by returning or withholding the appropriate decryption key. Ex-1005, [0060]-[0063], [0068].

69. If access is not initially permitted, reduced access to the file may be granted, more authentication information may be requested, or the request may be outright denied. *Id.*, [0064]-[0068]. Cheng discloses multiple ways that reduced access may be performed, including creating multiple files with various redactions, released either with their own decryption key or a single decryption key, passwords, and invertible and non-invertible obfuscation techniques. *Id.*, [0044]-[0046].



Id., Fig. 4 (colored outlining added).

70. Cheng additionally discloses a risk engine that evaluates the likelihood of data leakage based on deviation of recent access patterns from historical norms, a graduated access framework in which a decryption key corresponding to an appropriate level of redaction may be sent based on the user's confidence level and device context, and a continuous authentication mechanism in which background-collected authentication information is used to update the accumulated authentication score. *Id.*, [0024], [0028], [0029], [0067], [0069], [0079]. Though Cheng describes certain aspects of its invention as “preferred embodiments,” a POSITA would recognize that combining like-embodiments is straightforward for a POSITA and would not have demanded any ingenuity. *See id.*, [0097] (“Having described preferred embodiments of a system and method to provide server control for access to mobile client data (which are intended to be illustrative and not limiting), it is noted that modifications and variations can be made by persons skilled in the art in light of the above teachings. It is therefore to be understood that changes may be made in particular embodiments disclosed which are within the scope of the invention.”).

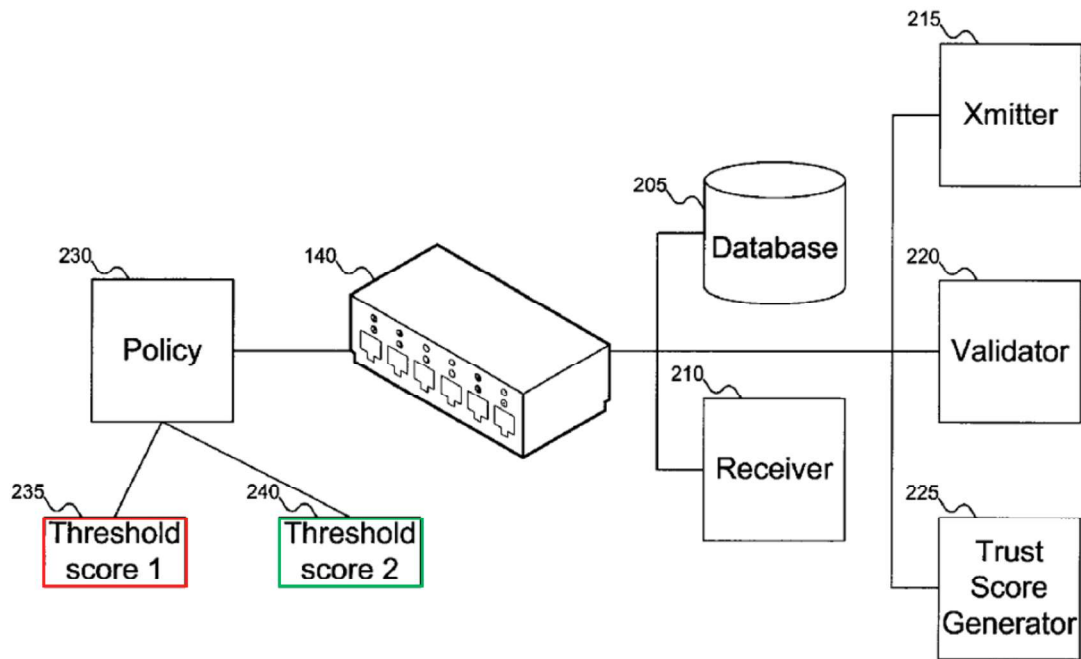
2. Bleckmann

71. Bleckmann discloses a system for controlling access to network “resource[s]” by generating a trust score for a requesting computer system and comparing that score against a policy to determine the appropriate level of access.

Ex-1006, Abstract. The system discloses an integrity validator (140) between an external network (110) and an internal network (135) to validate computer systems outside the organization but are requesting access to internal resources. *Id.*, Fig. 1, [0019].

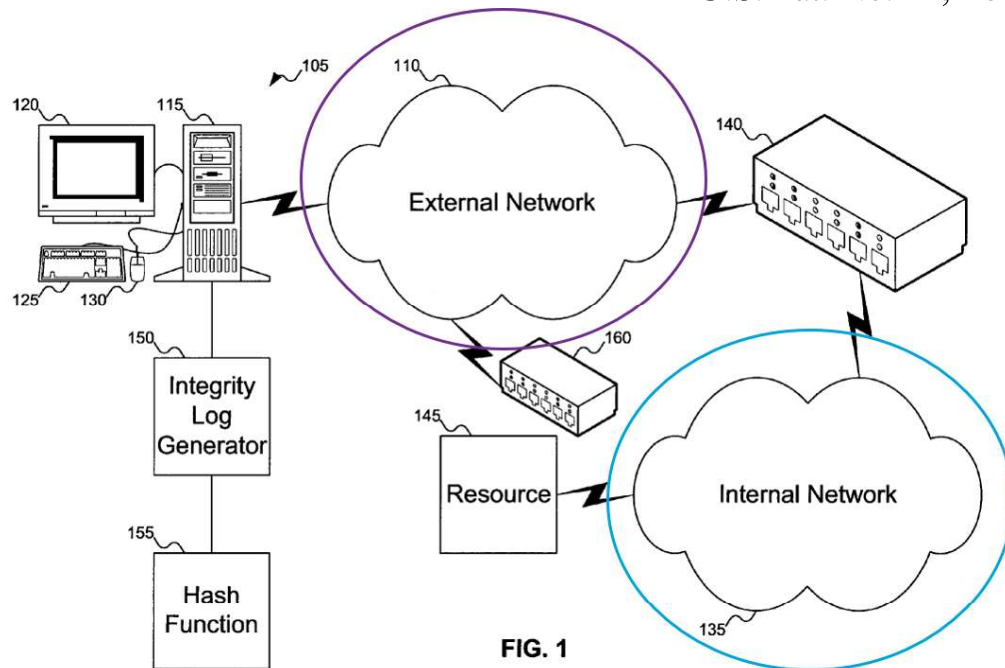
72. The system's validator component (220) compares those received signatures against a database of known-valid signatures and returns an indication of which are valid and which are not. *Id.*, [0038]. The trust score generator (225) then produces a trust score based on which signatures were validated, with several possible weighting schemes: for example, the ratio of validated modules to total modules, a scale from 0 to 1000, or a scheme that weights critical modules more heavily than others. *Id.*, [0039].

73. Bleckmann's policy (230) may include a single threshold score or two threshold scores governing three distinct access outcomes: if the trust score is at least as high as the first threshold score (235), the computer system is granted full access to the resource; if the trust score is below the second threshold (240), the computer system is denied access; and if the trust score is less than the first threshold but at least as high as the second threshold score, the computer system is granted partial access to the resource. *Id.*, [0043].



Id., Fig. 2 (colored outlining added).

74. Bleckmann's integrity validator operates regardless of how the resource is sent or requested to the device: whether it is encrypted or unencrypted and whether the request arrives over a standard or VPN-secured channel. The policy may also describe different access rules for different resources on the same network, and where the integrity validator serves multiple organizations, it can store and enforce separate policies for each. *Id.*, [0032], [0044].



Id., Fig. 1 (colored outlining added).

3. Motivation To Combine

75. A POSITA would have been motivated to combine Cheng and Bleckmann with a reasonable expectation of success for several reasons.

76. First, Cheng and Bleckmann are analogous art because they both generally relate to resource access mechanisms based on a confidence or trust score. Both are directed to server-based systems that compute a score reflecting a requester's trustworthiness or risk and that score, compared against one or more thresholds, to determine the degree of access a requester is permitted to protected resources.

77. In other words, both Cheng and Bleckmann teach systems that compute a score reflecting the trustworthiness or eligibility of a requester and use that score to gate access to protected data or network resources. *See, e.g.*, Ex-1005, [0028], [0079], [0089], [0095]; Ex-1006, [0039], [0043], Figs. 2, 8. Both Cheng and Bleckmann try to solve the same general problem, namely, the need for dynamic, score-driven access control to protected resources that provides finer-grained access decisions than rigid, binary approaches. Both consider both the risk of the user accessing a file and how the file is transferred to the user. *See, e.g.*, Ex-1005, [0006]-[0008], [0024], [0027]; Ex-1006, [0003]-[0007], [0032], [0039]-[0044].

78. A POSITA would have been motivated to apply Bleckmann's multi-threshold access control framework to Cheng's score-based data protection system to advantageously provide tiered, granular access to protected data items—including full access, limited access, and denial of access—based on a computed score rather than a single binary grant-or-deny decision. Users present varying degrees of risk depending on context and authentication history, and a system capable of granting only limited access in intermediate-risk scenarios provides both greater security, greater flexibility, and greater usability than one forced to make an all-or-nothing determination.

79. Cheng acknowledges this tension, explaining the tradeoff between security and usability and the limitations of existing approaches that do not “sufficiently address both security and usability of a mobile device.” Ex-1005, [0007].

80. Bleckmann addresses this by disclosing a policy that includes two threshold scores: if the trust score is at least as high as the first (higher) threshold score, the computer system is granted full access to the resource; if the trust score is less than the first threshold but at least as high as the second (lower) threshold, the computer system is granted partial access; and if the trust score is smaller than the second threshold, the computer system is denied access to the resource. Ex-1006, [0043].

81. In applying these teachings to Cheng, Cheng’s policy decision module 222, as modified with Bleckmann’s two-threshold framework, would compare the accumulated authentication score of the user to a first threshold score and a second threshold score, returning a decryption key for full access when the score meets or exceeds the first threshold, returning a decryption key and providing only limited access, including access only by VPN, when the score falls between the two thresholds, and withholding the decryption key entirely when the score falls below the second threshold.

82. Moreover, a POSITA would have further been motivated to incorporate Bleckmann's multi-tiered threshold framework into Cheng's data protection system because it enables context-sensitive, fine-grained access control to protected data items—a recognized design goal explicitly pursued by Cheng itself.

83. When access to files is enabled from outside an enterprise network, or remotely, there is a threat of unauthorized third-party access. This includes Man In The Middle (MITM) attacks where a bad actor operates a proxy between the service provider and the network, intercepting and decrypting the connection between an employee and the enterprise network to capture login credentials and view sensitive files being transmitted. A POSITA armed with this knowledge would be motivated to prevent these attacks and increase file protection.

84. A POSITA would understand that providing access within certain restrictions, including the use of a VPN, would increase protection for the transfer of a file where there is increased security concern, including when the user resides outside the enterprise network.

85. Granting limited access when a risk score is intermediate, rather than forcing a binary choice between full access and outright denial, better serves users in moderate-risk contexts and increases file protection. Where releasing a

decryption key provides access to the file, a POSITA would have been motivated to add restrictions on top of a binary grant/deny system.

86. Cheng contemplates this outcome in the context of redaction-based systems, explaining that “the data protection system may send only one decryption key that only allows access to a version that is appropriate for the current device context (e.g., only allowing access to a highly redacted version of the data item in a device context that is considered insecure like an airport).” Ex-1005, [0029].

87. A POSITA implementing this graduated-access concept in Cheng would have looked to Bleckmann for a concrete mechanism for restricting access short of full denial, including the VPN-gated restricted-access option Bleckmann discloses for computer systems that are not directly connected to the internal network.

88. Because Cheng already teaches a policy decision module that compares an accumulated authentication score to a minimum required authentication score to determine whether to send a decryption key to the requesting device (*Id.*, [0028], [0079], [0089], [0095]), implementing Bleckmann’s two-threshold framework in Cheng’s data protection system would have been a straightforward modification.

89. Similar to Cheng’s policy decision module, which already compares a computed score to a threshold to control whether a decryption key is provided,

Bleckmann teaches applying the same score-to-threshold comparison using two threshold scores to produce three distinct tiers of resource access: full access, partial access, and denial. Ex-1006, [0043].

90. A POSITA would have understood that Cheng’s policy decision module 222 could be implemented with two threshold scores—a first, higher threshold governing full access and a second, lower threshold governing partial access—consistent with Bleckmann’s express teachings regarding threshold score 235 and threshold score 240. Thus, a POSITA would have found it straightforward and advantageous to apply Bleckmann’s two-threshold access control teaching to Cheng’s data protection system, and would have known such a combination, yielding the “first threshold” and “second threshold” limitations of the ’623 patent claims, would predictably work and provide the expected functionality.

4. Claim 1:

1[a]: “A method comprising: obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;”

91. Cheng discloses or renders obvious a method (e.g., “methods for protecting sensitive data items”) comprising: obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network (e.g., obtaining and

storing, by “server 206,” including a “data protection system 212,” “access history” information in “access history 312”) by observing file access requests initiated by the plurality of users (e.g., a “request to access the protected data item”). Ex-1005, Abstract, [0006], [0010], [0052]-[0053], [0065].

92. Cheng discloses methods for “server-based protection before the transfer of data item from a server to a mobile device” where server 206 and data protection system 212 limit “the risk of loss of sensitive data on a mobile device by exercising control over the authentication needed to access the data.” *Id.*, [0037], [0053].

93. Based on Cheng’s disclosures, a POSITA would recognize or find it obvious that data protection system 212 can be a component of server 206. Cheng is architected towards monitoring and manipulating the data exchanged between server 206 and mobile device 202; data protection system 212’s functionality is thus naturally associated with server 206’s data processing. *See, e.g., id.*, [0025] (“a data item may be protected before being transferred from a server to a mobile device using the data protection system.”).

94. To the extent Cheng does not explicitly disclose data protection system 212 as a component of server 206, it would have been obvious to a POSITA. Cheng describes that “the mobile service interface 210 may also modify data items transferred from the server 206 to the mobile device 202 according to

the data protection system 212” then states “It should be understood that the functions and components of the data protection system 212 may be integrated into one or more systems. In one embodiment, the data protection system 212 may be implemented as a plug-in for an existing mobile platform infrastructure. ... Other implementations of the data protection system 212 are also contemplated.” *Id.*, [0052], [0053]. Cheng further states “The present principles provide **server-based** protection **before** the transfer of a data item from a server to a mobile device.” *Id.*, [0037] (emphasis added). A POSITA would recognize “existing mobile infrastructure” as including server 206 such that data protection system 212 could reside as a component of server 206.

95. Cheng’s methods include obtaining and storing user “access history” by such employees in “**access history 312**” and “**authentication and context history 314**.” *Id.*, Fig. 3, [0006], [0009]-[0011], [0053], [0065]-[0068]. *See also id.*, [0063] (emphasis added) (“The authentication manager module 310 processes the request for the decryption key by using the policy decision module 222 to **determine whether a user is currently eligible to access the encrypted data item.**”).

96. Cheng suggests or renders obvious one or more servers are associated with an enterprise network. “In accordance with the present principles, systems and methods for protecting sensitive data items and server and context based access control of these sensitive data items are provided.” *Id.*, [0024]. Cheng describes its

disclosures in the context of enterprise systems. “Over the last few years, work environments have changed from an office-centric model to an increasingly mobile model in which *employees access enterprise data remotely through various channels from a wide range of devices*. In addition to access from laptops that connect to enterprise networks through encrypted channels, such as virtual private networks (VPNs), employees are increasingly using other mobile devices, such as smartphones or tablet computers. Such mobile devices create a significant risk of data loss due to accidental loss or theft.” *Id.*, [0006] (emphasis added). Cheng does not limit server 206 to any particular architecture, and provides examples of servers typically associated with enterprise networks: “The server 206 is a computing apparatus that provides service to a client device, and is not limited to any architecture, location or operating environment. For instance, server 206 may include, e.g., an email server, calendar server, etc. It is noted that the present principles may be applicable to the transfer of any data item that can be monitored and manipulated between a mobile device 202 and server 206.” *Id.*, [0049]. It would have been obvious to a POSITA that Cheng’s server system was associated with an enterprise network.

97. Cheng’s data protection server maintains two behavioral data stores populated by observing prior user activity: an *access history store 312*, used “to determine which encrypted data items were accessed in the past from the mobile

device,” and an authentication and context history store 314, used “to determine the most recent context for the mobile device.” *Id.*, [0065].

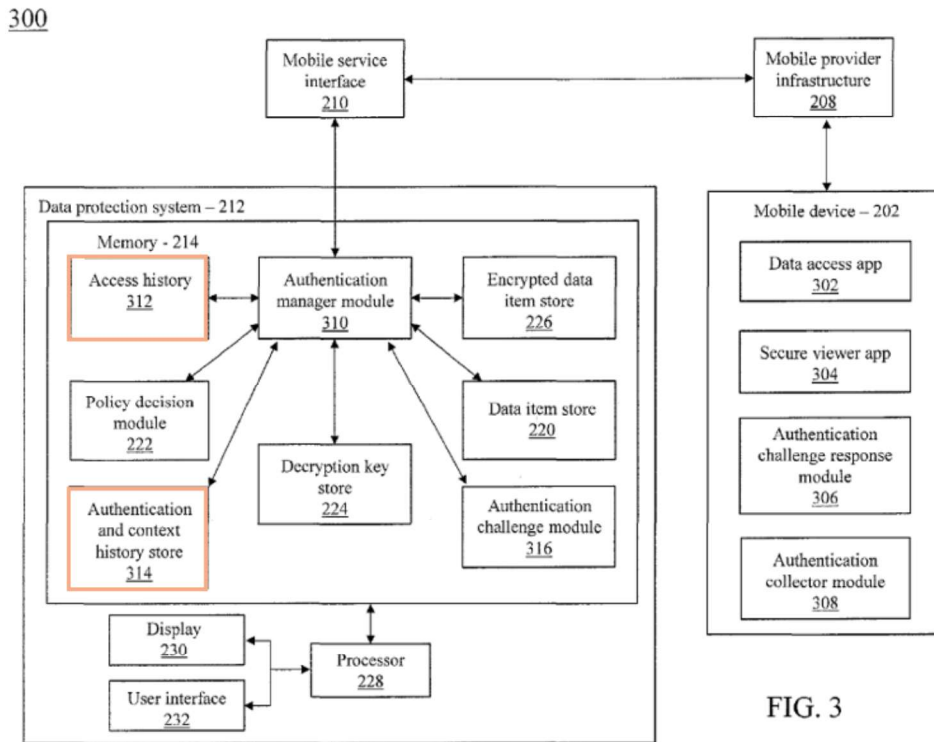


FIG. 3

Id., Fig. 3 (orange outlining added).

98. The obtaining and storing of this historical behavioral information is done in connection with processing each request to access a protected data item: “responsive to a request to access the protected data item,” the data protection system determines a level of confidence based on “one or more of a context of the client device, an authentication history of the client device, and an access history of the user of the client device.” *Id.*, [0010]-[0011].

99. That confidence level may be “determined based on the history of data access (e.g., based on volume, topic, average sensitivity, etc.) or the current context of the device (e.g., current location, nearby devices, etc.). For instance, the history may be used to determine if the data accessed or current context of the mobile device 202 is unusual. The **access history 312** may be used to determine which encrypted data items were accessed in the past from the mobile device 202. The **authentication and context history store 314** may be used to determine the most recent context for the mobile device 202.” *Id.*, [0065].

100. The behavioral history captured in those stores encompasses a wide range of contextual factors, including “the current location of the mobile device [], the history of previous locations of the mobile device [], the history of previous compromises of the mobile device [], the ownership status of the mobile device [], the operating system of the mobile device [], the applications installed on the mobile device [], the current patch level of the mobile device [], the presence of known or suspected malware on the device, and the security status of the networks which the device is connected to,” as well as user-specific factors including “the history of the user’s access to data of known sensitivity” and “the aggregated sensitivity score of all data items accessed by the user.” *Id.*, [0066].

101. Cheng discloses or renders obvious obtaining and storing, by one or more servers of an enterprise network, information regarding historical user

behavior for a plurality of users by observing file access requests those users initiate, satisfying limitation 1[a].

102. To the extent Cheng does not disclose or suggest obtaining and storing, by one or more servers associated with an enterprise network, historical behavior information *for a plurality of users*, it would nonetheless have been obvious to a POSITA to implement Cheng's disclosed **access history 312 and authentication and context history 314** across the plurality of users that Cheng expressly contemplates.

103. Cheng is not directed to single-user deployment; it describes its solution in the context of "an increasingly mobile model in which employees access enterprise data remotely through various channels from a wide range of devices," expressly framing the invention as addressing data protection needs across an organization's employee population. Cheng, [0006]. Nothing in Cheng's architecture limits the **access history 312 or authentication and context history 314** to tracking only one user. *Id.*, [0049]-[0053].

104. To the contrary, Cheng discloses that its policy decision module 222 evaluates eligibility using stored history so that the system can distinguish an authorized user's typical behavior from anomalous access, a determination that is only meaningful, and only usable to detect deviation from a user-specific baseline, when the server maintains a discrete historical record for each of the multiple

employees accessing the enterprise's data. *See id.*, [0064]-[0067]. A POSITA implementing Cheng's data protection system would have extended Cheng's history-tracking mechanism to maintain a corresponding history record for each user in that population, using ordinary, well-understood techniques for associating stored records with a user identifier already necessary to Cheng's own authentication and eligibility determinations. *Id.*, [0028] (comparing "the accumulated authentication score of the user" against "a minimum authentication score to determine the eligibility of the user").

105. This extension amounts to applying Cheng's known access-history and policy-decision mechanism to each of the multiple users Cheng's own background section identifies as the source of the mobile data protection problem, yielding the predictable and expected result of a server that maintains historical behavioral information for a plurality of users rather than one.

106. A POSITA would have had a reasonable expectation of success in this straightforward extension because Cheng's per-device data stores ([access history 312](#) and [authentication and context history 314](#)) already operate independently for each accessing device and require no architectural modification to be replicated across the enterprise's user population.

1[b]: "receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access

request relates to a file stored within the enterprise network in encrypted form;”

107. Cheng discloses or renders obvious receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network (e.g., a “request to access the protected data item”) in encrypted form (e.g., “stored in the encrypted data item store 226”).

108. Cheng discloses that server 206 may initiate the file transfer process in response to a request from the mobile device. *Id.*, [0050]. The data item “may be protected before being transferred from a server to a mobile device using the data protection system.” *Id.*, [0025]. “The data protection system 212 may apply appropriate protections on data items transferred from the server 206 to the mobile device 202.” *Id.*, [0052]. *See also id.*, [0024] (“A server, such as a data protection system, may be utilized to ensure protection of the data item while also providing an opportunity to increase usability of the mobile device.”). The data protection system “appl[ies] appropriate protections” on data items, e.g., files, including “encrypting the data items” in an “encrypted data item store.” *Id.*, [0056], [0059].

109. As described by Cheng, “In one embodiment, *initiating the transfer of a data item may include a request from the mobile device 202 due to* one or more of, e.g., *a user request...*” Cheng, [0050] (emphasis added). When the policy

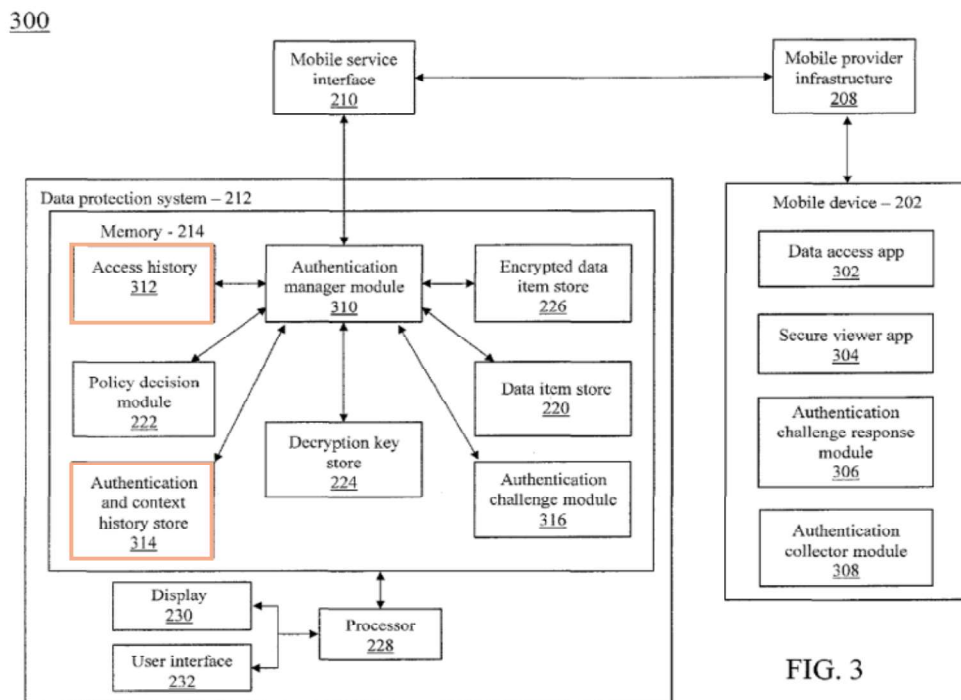
decision module determines that a data item requires protection, “appropriate protections are applied on the data items,” and “[i]n a preferred embodiment, protecting data items includes encrypting the data items.” *Id.*, [0056]; *see also id.*, [0059].

110. Encrypted data items are stored on encrypted data item store 226. *Id.*, [0061]. The encrypted data item store 226 and decryption key store 224 are part of the data protection system 212. *See id.*, [0059]. Data items are stored on server 206, then the data protection systems 212 modified these data items as necessary for use, applying “appropriate protections” including encryption. *Id.*, [0049], [0052]. The data protection system of Cheng may be a part of an enterprise network and server, as described in [0006] and [0025]. Thus, the requested files may reside on an enterprise network server before transfer to the mobile device.

111. Cheng also discloses or suggests that data items stored on server 206 are stored in encrypted form before additional protection is applied by data protection system 212. “In block 102, upon initiating the transfer of a data item from a server to a mobile device, a sensitivity score of the data item may be determined.” *Id.*, [0039]. This sensitivity score includes the current level of encryption on the data item before being further protected by the data protection system. *See, e.g., id.*, [0041] (“In still other embodiments, upon initiation of transfer of a data item, a current protection level of the data item may be

determined, such as, e.g., whether the data item is currently already protected (e.g., encrypted or redacted)"). *See also id.*, [0054].

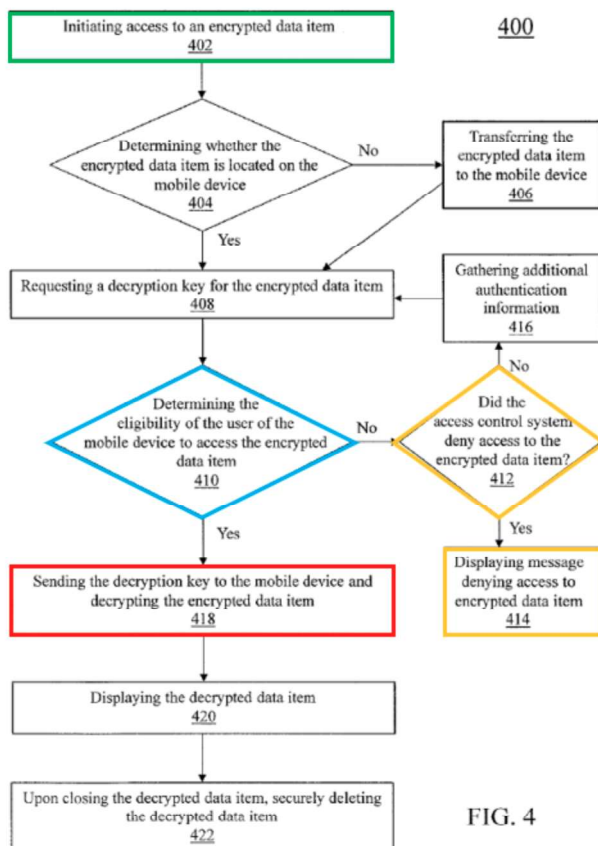
112. Cheng's data protection system 212 includes encrypted data item store 226 and decryption key store 224 maintained within the data protection system. Access history 312 and authentication and context history store 314 also reside within the data protection system, along with the authentication manager module 310 and policy decision module 222 that govern access decisions. *Id.* [0061]-[0064].



Id., Fig. 3. (orange outlining added).

113. Figure 4 illustrates the flow beginning with “Initiating access to an encrypted data item” at block 402, proceeding through “[d]etermining eligibility of

the user” at block 410 and either “[s]ending the decryption key to the mobile device” at block 418 or denying access and displaying a denial message at blocks 412 and 414. Figure 6 illustrates the data protection system’s receipt of the decryption key request at block 602, determination of whether the request includes authentication or context information at block 604, and the subsequent access determination at blocks 608 and 612.



Id., Fig. 4 (colored outlining added).

114. Figure 6 illustrates the data protection system’s receipt of the decryption key request at block 602, determination of whether the request includes

authentication or context information at block 604, and the subsequent access determination at blocks 608 and 612.

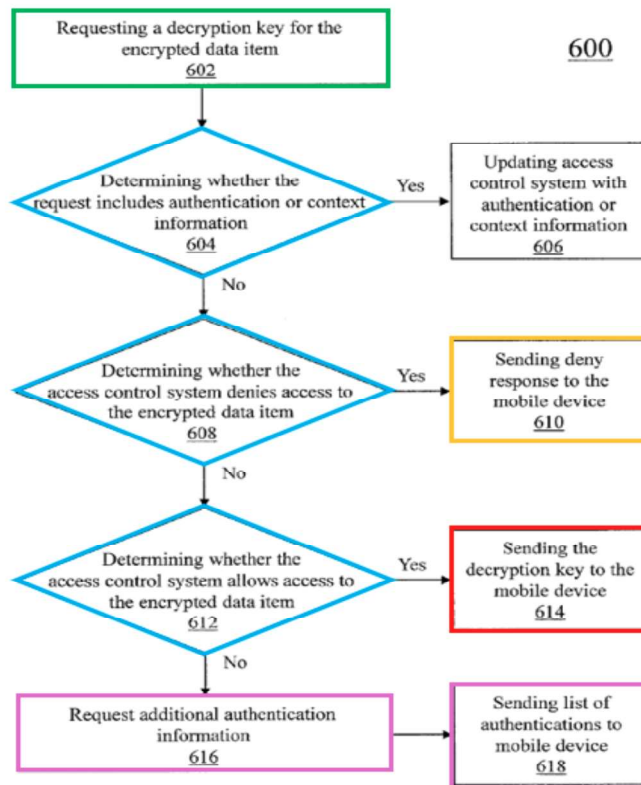


FIG. 6

Id., Fig. 6 (colored outlining added).

115. Cheng discloses that the policy decision module evaluates the request and determines eligibility “responsive to a request to access the protected data item.” *Id.*, [0010]-[0011], [0014], [0064]. As discussed in limitation 1[a], the user’s file access request is the triggering event for the entire access control process. Upon initiation of the file access request, a level of confidence is determined that

“is based on one or more of a context of the client device, an authentication history of the client device, and an access history of the user of the client device. An authentication manager module is configured to provide access to the protected data item to the client device in accordance with the level of confidence, such that a level of confidence needed to access the protected data item is based upon a sensitivity score of the protected data item.” *Id.*, [0014].

116. Cheng describes protection methods of the files requested, including the use of encryption and decryption keys. “If the policy decision module 222 determines that the data item does need protection, appropriate protections are applied on the data items. In a preferred embodiment, protecting data items includes encrypting the data items. However, it is noted that other implementations of protecting data items are also contemplated. For example, applying appropriate protections on data items may include redaction, password access, etc.” *Id.*, [0056].

117. Cheng describes that the “secure mobile migration manager module 216” would “encrypt the data item by determining an encryption key. It should be appreciated that the present principles are not limited to determining an encryption key, but may be implemented using other forms of protection, such as a redaction function, obfuscation function, or similar instruction.” *Id.*, [0057].

118. Cheng describes how the encrypted file may be transferred from the server to the device. “Upon initiating access to the encrypted data item, the

application initiating the access (i.e., data access app 302 or secure view app 304) may determine whether the encrypted data item is stored on the mobile device 202. For example, the encrypted data item may already be stored on the mobile device 202 if the user had previously viewed the encrypted data item or if the encrypted data item was transferred by a background process (e.g., data sync). If the encrypted data item is not currently stored on the device, the application initiating access (i.e., data access app 302 or secure viewer app 304) requests transfer from the authentication manager module 310 of the data protection system 212. The encrypted data item store 226 may provide the encrypted data item to the mobile device 202 where the encrypted data item was not already transferred to the mobile device 202, such as when a link was sent to the mobile device 202 instead of the encrypted data item.” *Id.*, [0060].

119. Cheng discloses or renders obvious receiving, by one or more servers, a file access request initiated by a first user of a plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form, satisfying limitation 1[b].

1[c]: “responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and”

120. Cheng discloses or renders obvious responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user (e.g., “responsive to a request to access the protected data item, determining a level of confidence”) based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request (e.g., based on “one or more” factors including “an access history of the user”; the “sensitivity score of the protected data item” being requested and the “method of authentication”; and a “context” of the request, “the time of last successful authentication,” and “confidence in that method of authentication”). *Id.*, [0010]-[0011], [0014]-[0015], [0027], [0065]. *See* 1[b].

121. Cheng discloses that “responsive to a request to access the protected data item,” the authentication manager module 310 in the data protection system 212 “determine[s] a level of confidence” for the user that is used to determine whether the user is “eligib[le]” to “access” the requested item. Ex-1005, [0010]-[0011], [0014]-[0015]. Cheng’s “level of confidence” is an “accumulated authentication score.” *Id.*, [0010], [0064]. *See also id.*, [0079] (“In [block 410](#), it is [determined whether a user is currently eligible to access the encrypted data item](#). In a preferred embodiment, user eligibility may be based on a minimum authentication score. Each authentication option may be given a score, with the

accumulated authentication score of the user reflecting the level of confidence that the data protection system has in the user's identity.”).

122. Cheng discloses the level of confidence is based on information regarding historical user behavior. “The level of confidence is based on one or more of a context of the client device, an authentication history of the client device, and an access history of the user of the client device.” *Id.*, [0010]. “The context of the mobile device 202 may include one or more of the following: the current location of the mobile device 202, the history of previous locations of the mobile device 202, the history of previous compromises of the mobile device 202, the ownership status of the mobile device 202 (e.g., corporate owned or personally owned), the operating system of the mobile device 202, the applications installed on the mobile device 202, the current patch level of the mobile device 202, the presence of known or suspected malware on the device, and the security status of the networks which the device is connected to.” *Id.*, [0066]. “The context of the user may include one or more of the following: the management status of the user, the business role of the user, the history of the user's access to data of known sensitivity, the aggregated sensitivity score of all data items accessed by the user, the history of the user in experiencing the loss or theft of devices, and the history of the individual in accessing the device.” *Id.*

123. Cheng discloses the level of confidence is based on the file access request, e.g. the sensitivity score of the protected data item. “In accordance with the level of confidence, access to the protected data item is provided to the client device using the data protection system such that a level of confidence needed to access the protected data item is based upon a sensitivity score of the protected data item.” *Id.*, [0011]. *See also id.*, [0067] (“In an embodiment, the risk may be based on one or more of the likelihood that the data item may be leaked or misused, the potential damage of such leakage or misuse, etc. The likelihood may be based on one or more of the sensitivity score of the data item”).

124. Cheng discloses the level of confidence is based on observed data determined based on the file access request, e.g., a method of authentication. “[T]he level of confidence may be determined based on the time of last successful authentication of the user through the mobile device 202 or the method of authentication, such as password or biometric authentication. In another embodiment, the level of confidence may be determined based on the confidence of the authentication method (e.g., the confidence of a fingerprint identification, voice recognition or facial recognition), the trust in the authentication method itself (e.g., based on the difficulty to achieve a false positive authentication by exploiting weaknesses in the authentication method), or sensitivity score of the data item.” *Id.*, [0065].

125. Cheng discloses its “level of confidence” may be represented by an “authentication score” that includes historical user behavior (e.g., “time of last successful authentication of the user” and “**access history 312**”). *Id.*, [0064]-[0067]. The level of confidence takes into account the file access request, including assigning a sensitivity score based on the file/type that is requested ([0065]), and it analyzes data from the file access request including “trust in the authentication method itself” ([0092]) and other “authentication information provided by the mobile device” ([0064]). Based on this level of confidence, “authentication manager module 310 processes the request for the decryption key by using the policy decision module 222 to determine whether a user is currently eligible to access the encrypted data item.” *Id.*, [0063].

126. Cheng discloses or renders obvious the limitation of claim 1[c].

1[d]: “based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key”

127. Cheng discloses or renders obvious based on the risk score (e.g., “[b]ased on the level of confidence” including an “authentication score”), permitting or denying, by the one or more servers, access to the file (e.g., “determine whether access to the encrypted data item is allowed.”) by returning a decryption key for the file or withholding the decryption key (e.g., “If access is allowed, the authentication manager module 310 retrieves the decryption key...and

sends it to the mobile device”; “send a message ... indic[a]ting that access is denied” if “access is not allowed”). *Id.*, [0064], [0068]. *See* 1[c].

128. Cheng discloses that, depending on level of confidence, the system permits or denies access to the file. “Based on the level of confidence, the policy decision module 222 may determine whether access to the encrypted data item is allowed.” *Id.*, [0068]. “If the policy decision module 222 allows access, the appropriate decryption key may be transferred from the decryption key store 224 to the mobile device 202. If the policy decision module 222 denies access, the authentication manager module 310 may send a message to the mobile device 202 indic[a]ting that access is denied until the context (e.g., location) changes.” *Id.*, [0073].

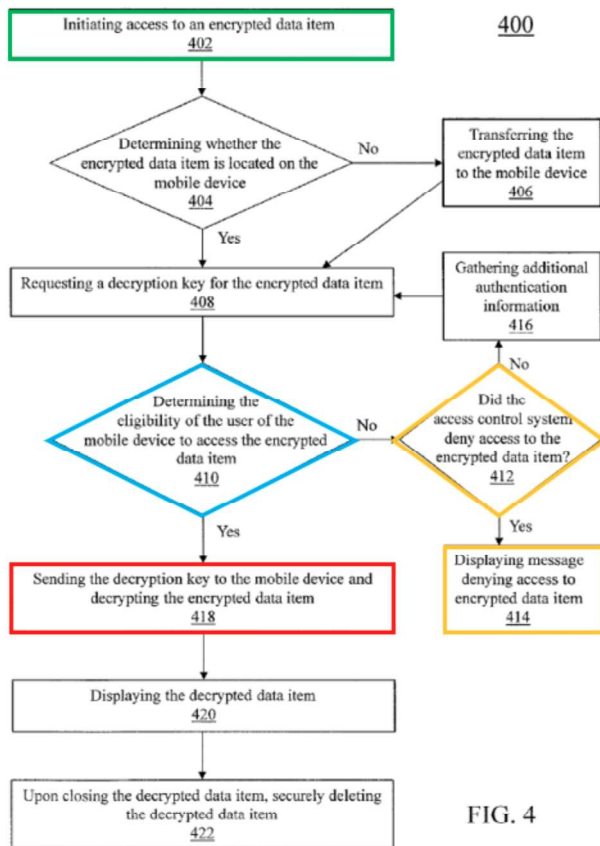


FIG. 4

Id., Fig. 4 (colored outlining added).

129. “The authentication manager module 310 processes the request for the decryption key by using the policy decision module 222 to determine whether a user is currently eligible to access the encrypted data item. Based on the determination of the policy decision module 222, *the appropriate decryption key may be sent to the mobile device 202.*” *Id.*, [0063] (emphasis added). If the authentication score exceeds a “minimally required authentication score,” then the system “send[s] a decryption key” to the user for the “protected data item.” *Id.*,

[0029], [0095]. If the authentication score does not satisfy this threshold, then the system “send[s] a message...indic[a]ting that access is denied.” *Id.*, [0073].

130. Cheng discloses or renders obvious the limitation of claim 1[d].

1[e]: “wherein said permitting or denying comprises when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;”

131. Cheng discloses or renders obvious wherein said permitting or denying (*see* 1[d]) comprises: when the risk score is less than a first threshold (e.g., when the “level of confidence” does not require “a redacted version” when “compared to a minimally required authentication score”), returning the decryption key and providing full access to the file (e.g., “send a decryption key to the mobile device for accessing the protected data item”). Ex-1005, [0028]-[0029].

132. Cheng discloses “The accumulated authentication score of the user may be compared to a minimum authentication score to determine the eligibility of the user in the current context.” *Id.*, [0028]. This accumulated authentication score, or level of confidence, dictates whether full access is granted to decrypt a file: the accumulated authentication score must meet the minimum threshold for the full (e.g., unredacted) decryption key is sent for full access to the data item. *Id.*, [0028]-[0029].

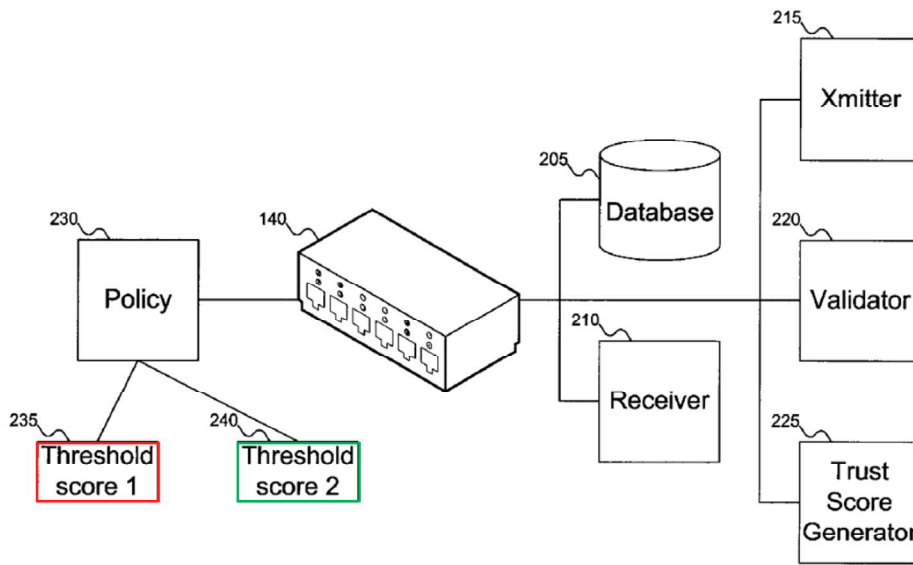
133. Cheng discloses comparing its level of confidence to a minimum threshold (e.g., minimally required authentication score) for full access. “The

accumulated authentication score may be compared with the minimum authentication score to determine whether a user is eligible to access the encrypted data item.”*Id.*, [0079]. “If the user was found to be eligible, a decryption key may be sent to the mobile device.” *Id.*, [0080]. “In block 418, a decryption key may be sent to the mobile device to decrypt the encrypted data item.” *Id.*, [0081]; *see also* [0087], [0095].

134. To the extent Cheng does not disclose or suggest this element, it would have been obvious in light of Bleckmann.

135. Bleckmann discloses Threshold score 1, i.e. a first threshold. “In one embodiment, policy 230 includes threshold score 235. To be granted access to the resource, the computer system should have a trust score at least as high as threshold score 235.” Ex-1006, [0042].

136. A file is one resource considered by Bleckmann. *Id.*, [0019] (“Resource 145 could be any type of resource: for example, a network drive, directory, or file, or a web page, to name some examples.”).



Id., Fig. 2 (colored outlining added).

137. In the combination Cheng and Bleckmann, a POSITA would find it obvious to implement Bleckmann's **Threshold score 1** with Cheng. Cheng discloses a "minimum authentication score." *Id.*, [0072]. Bleckmann's **Threshold score 1** provides a POSITA with an explicit value to input as the minimum authentication score, such that Cheng's authentication manager module 310 compares the current level of confidence against this explicit score. *See id.*

138. A POSITA would have been motivated to incorporate this teaching of Bleckmann into Cheng for the reasons I discussed in the Motivation to Combine section.

139. Cheng, alone or in combination with Bleckmann, discloses or renders obvious the limitation of claim 1[e].

1[f]: “when the risk score is greater than a second threshold, withholding the decryption key; and”

140. Cheng discloses or renders obvious when the risk score is greater than a second threshold, withholding the decryption key (e.g., “send a message...indic[a]ting that access is denied” if “access is not allowed”). Ex-1005, [0068], [0073]

141. Cheng discloses that when the accumulated confidence score is below a certain authentication threshold (i.e., risk is sufficiently high), the decryption key is withheld entirely.

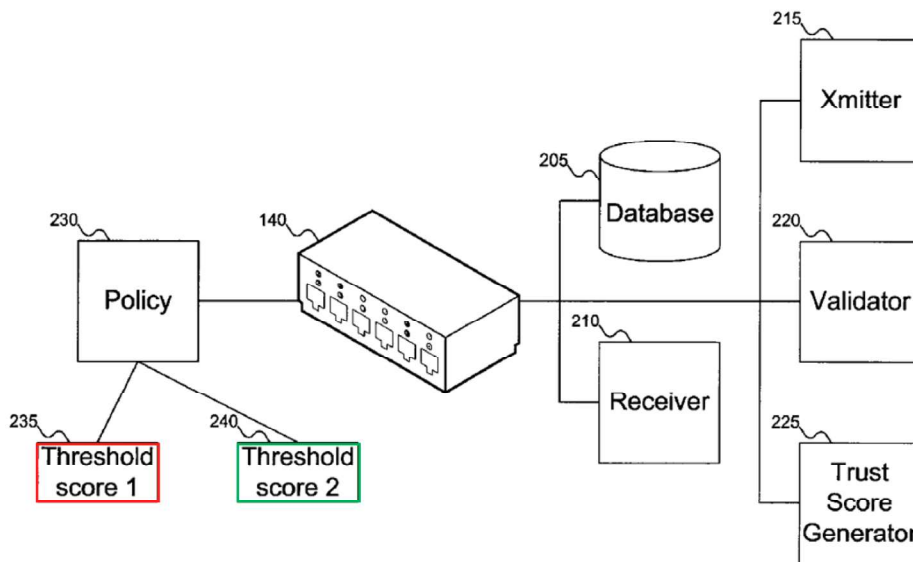
142. Cheng discloses preventing access and withholding the decryption key when the level of confidence is not sufficiently high. “In block 410, it is determined whether a user is currently eligible to access the encrypted data item. In a preferred embodiment, user eligibility may be based on a minimum authentication score. ... The accumulated authentication score may be compared with the minimum authentication score to determine whether a user is eligible to access the encrypted data item.” *Id.*, [0079]. “If the user was not found to be eligible, in block 412, it is determined whether the data protection system denied access to the encrypted data item or needs additional authentication. If the server denied access to the encrypted data item, in block 414, a message may be displayed.” Cheng, [0080]. “If the policy decision module 222 denies access, the

authentication manager module 310 may send a message to the mobile device 202 indic[a]ting that access is denied until the context (e.g., location) changes.” *Id.*, [0073].

143. To the extent Cheng does not disclose or suggest a second threshold different from the first threshold, a POSITA would have understood or at least found it obvious to implement the disclosures of Cheng with a separate second threshold. Cheng discloses limited access beyond simple access/denied options. *See, e.g., id.*, [0029] (emphasis added) (“In a preferred embodiment, the data protection system may send a decryption key to the mobile device for accessing the protected data item *or for accessing a redacted version of the data item.*”); *see also infra* 1[g]. Therefore, a POSITA would have understood or found it obvious to implement a first, a second, or even additional thresholds to determine different levels of limited access. Cheng further discusses embodiments where a range of authentication scores may be used; a POSITA would have understood or found it obvious to implement multiple thresholds to address different ranges and scores. Ex-1005, [0028], [0064] (e.g., “Each authentication option (e.g., simple pass code, full password, biometrics, etc.) may be assigned a score.”). Therefore, a POSITA would have found it obvious to implement Cheng with two separate threshold levels.

144. But even if Cheng alone does not disclose or render obvious this limitation, it would have been obvious over Bleckmann.

145. Bleckmann discloses **Threshold score 2**, i.e. a second threshold. “For example, in FIG. 2, policy 230 is shown as including two threshold scores 235 and 240.” Bleckmann further discloses that “if the trust score for the computer system is smaller than **threshold score 240**, the computer system can be denied access to the resource.” Ex-1006, [0043].



Id., Fig. 2 (colored outlining added).

146. In the combination Cheng and Bleckmann, a POSITA would find it obvious to implement Bleckmann’s Threshold score 2 with Cheng. Cheng discloses a comparing its authentication score against baseline values and discloses denying access. Ex-1005, [0072], [0080]. Bleckmann’s Threshold score 2 provides

a POSITA with an explicit value to input, such that Cheng's authentication manager module 310 compares the current level of confidence against this explicit score and may determine the if denial criteria is met.

147. A POSITA would have been motivated to incorporate this teaching of Bleckmann into Cheng for the reasons I discussed in the Motivation to Combine section.

148. Cheng, alone or in combination with Bleckmann, discloses or renders obvious the limitation of claim 1[f].

1[g]: “when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.”

149. Cheng discloses or renders obvious when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file. (*e.g.*, when “level of confidence” is between the unredacted item's “sensitivity score” and the “lower” sensitivity score of a “redacted version,” provide the “key” and provide access to a “redacted version”). Ex-1005 [0058]. *See* 1[d]-1[f].

150. Cheng discloses providing limited access to the file by creating redacted versions. The policy decision module 222 determines, based on the level of confidence, which version the user is granted access, if at all. Ex-1005, [0074], [0026]. Cheng describes various levels of access to files, including levels of

redaction: “Each individually protected data item of the aggregate protected data item may be protected as appropriate to allow access according to different contexts (*e.g., a heavily redacted version permissible to be viewed everywhere and a lightly redacted version that may only be viewed in locations with some level of access control*).” *Id.*, [0046] (emphasis added). *See also id.*, [0074] (“[T]he policy decision module 222 may determine that a redacted version of the data item should be displayed based on the level of confidence in the user’s identity and the current context of the mobile device (*e.g., in a public location with a high risk of unauthorized access by “shoulder surfing,” where a third-party observes the mobile device 202 screen while the authorized user is viewing the data item*).”).

151. Cheng provides a decryption key for each version of limited access. *Id.*, [0029]. Cheng discloses “the policy decision module 222 may determine that a redacted version of the data item should be displayed based on the level of confidence”. *Id.*, [0074]; *see also id.*, [0081] (“In one embodiment, the decryption key may be sent to the mobile device according to a level of redaction of the data item.”).

152. To the extent this limitation is not met because Cheng describes decryption keys unique to each version, utilizing a single decryption key is disclosed by Cheng. While Cheng describes a single decryption key for each file, it also discloses “In some embodiments, encryption keys may be reused according to

a predefined arrangement. For example, encryption keys may be assigned by data item type, by time period, *or the same encryption key may be used for all data items.*” *Id.*, [0057] (emphasis added). Using a single decryption key further would have been obvious to a POSITA. Using a single encryption key for all versions of the file would simplify key management—there’d be only a single key to manage access to the file as opposed to needing to generate and maintain separate keys for each different version.

153. Additionally, to the extent a second threshold is not disclosed or suggested, it would have been obvious to a POSITA. Cheng discloses providing limited access to files, including redacted versions. *See id.*, [0046], [0074]. This is an access tier that falls between denying access to a file and providing unlimited access. If there were only a binary grant/deny option, it would have been obvious that a single threshold existed. Because three tiers of access are described by Cheng, it is obvious that two thresholds are disclosed or suggested.

154. Additionally, to the extent providing a redacted version of a file is not providing “limited access,” that would have been obvious in light of other disclosures in Cheng. Cheng considers other protection techniques for intermediate access other than redacted versions each with a unique decryption key. *Id.*, [0044]. Other well-known access control methods known before the ’623 patent include

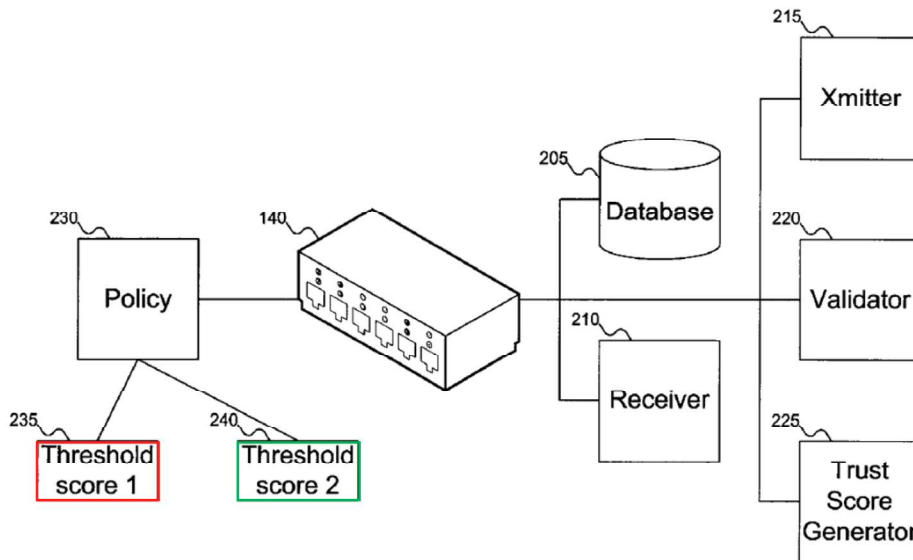
redirecting a user's connection through a virtual private network or requiring a user to access a file through a specific terminal.

155. To the extent Cheng does not disclose or suggest this limitation, it would have been obvious in light of Bleckmann.

156. Bleckmann describes that “policy 230 can include multiple threshold scores. For example, in FIG. 2, policy 230 is shown as including two threshold scores 235 and 240. If the trust score for the computer system is at least as high as **threshold score 235**, then the computer system can be granted full access to the resource. If the trust score for the computer is less than **threshold score 235** but at least as high as **threshold score 240**, then the computer system can be granted partial access to the resource. And if the trust score for the computer system is smaller than **threshold score 240**, the computer system can be denied access to the resource.” Ex-1006, [0043].

157. Further, Bleckmann discloses the same functionality as the '623 patent for providing limited access to a file when the risk score is between the two thresholds. The '623 patent describes providing limited access once along with releasing the decryption key as: “when the risk score is moderate, the user can be directed to access the file through a lower risk channel, e.g., a virtual private network (VPN); and when the risk score is high, the user can be blocked from accessing the file.” Ex-1001, 6:20-24.

158. Bleckmann describes the same function of releasing a resource given concern of its environment. Describing a computer system not directly connected to an internal network, and therefore less secure, Bleckmann discloses “resource 145 might be requested over a virtual private network (VPN) used to secure access to resources. A person skilled in the art will recognize other ways in which access to resource 145 can be managed.” Ex-1006, [0032].



Id., Fig. 2 (colored outlining added).

159. In the combination Cheng and Bleckmann, a POSITA would find it obvious to implement Bleckmann’s Threshold score 1 and Threshold score 2 with Cheng. Cheng discloses intermediate levels of file access. *See* Cheng, [0074], [0081]. Bleckmann’s threshold scores provide a POSITA with explicit values for Cheng’s authentication manager module 310 to compare against the current level

of confidence to determine which outcome, allow, deny, or intermediate access, results.

160. A POSITA would have been motivated to incorporate this teaching of Bleckmann into Cheng for the reasons I discussed in the Motivation to Combine section.

161. Cheng, alone or in combination with Bleckmann, discloses or renders obvious the limitation of claim 1[g].

5. Claim 2:

“The method of claim 1, wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine learning,”

162. Cheng discloses or renders obvious the method of claim 1, wherein said determining, by one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning. (*see* claim [1]; *e.g.*, evaluating the “history of data access” and determining if the data accessed or current context “is unusual”).

163. Cheng discloses utilizing user history to determine if a data access request or current user context is unusual; Cheng does not limit how this is determined, including by machine learning. Ex-1005, [0065]. A POSITA would have understood and at least found it obvious that this includes evaluating a file

access request by utilizing artificial intelligence, i.e. machine learning, to analyze/determine a risk score because that was well-known before the '623 patent.¹⁶

164. Cheng discloses or renders obvious the limitation of claim [2].

6. Claim 3:

3[pre]: “The method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users:”

165. To the extent the preamble of claim 3 is found to be limiting, Cheng discloses or renders obvious the method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users. *See* claim [1].

¹⁶ As discussed in Section II above, NIST publicly circulated a Risk-Adaptive Access Control working draft in connection with its 2009 Privilege Management Workshop. The working draft already detail that “RAdAC [Risk-Adaptive Access Control] also takes a **probabilistic, heuristic approach** to determine whether the access should be granted under the circumstances. The heuristics include a historical record of access control decisions and **machine learning**. This means that a RAdAC system will **use previous decisions as one input when determining whether access will be granted to a resource in the future.**” (Emphasis added). Ex-1018.

166. Cheng further discloses information regarding historical user behavior (e.g., obtaining and storing “access history” information in “**access history 312**”).

See claim [1]; *see also* Ex-1005, Fig. 3.

167. Cheng discloses or renders obvious the limitation of claim 3

```
[pre]
```

.

3[a]: “historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;”

168. Cheng discloses or renders obvious historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time (e.g., “history of data access” “based on volume”), types of the files accessed (e.g., “history of the user’s access to data of known sensitivity”), and applications used by the user over the predetermined period of time (“applications installed on the [user’s] device”). Ex-1005, [0065], [0066]. *See also* claims [1], 3

```
[pre]
```

.

169. Cheng further discloses that “the level of confidence may be determined *based on the history of data access (e.g., based on volume, topic, average sensitivity scores, etc.)* or the current context of the device (e.g., current location, nearby devices, etc.). For instance, the history may be used to determine if the data accessed or current context of the mobile device is unusual.” Ex-1005, [0092] (emphasis added); *see also id.*, [0065], [0094]. Cheng further discloses

“history of previous compromises of the mobile device” and “history of the user’s access to data of known sensitivity, the aggregated sensitivity score of all data items accessed by the user, the history of the user in experiencing the loss or theft of devices, and the history of the individual in accessing the device.” *Id.*, [0066].

170. Cheng discloses or renders obvious the limitation of claim 3[a].

3[b]: “historical data regarding observed locations of the user; and”

171. Cheng discloses or renders obvious historical data regarding observed locations of the user (e.g., “history of previous locations of the mobile device”). *Id.*, [0066]. *See also* claims [1], 3[pre].

172. Cheng further discloses that “the level of confidence may be based on a current context,” which includes “history of previous locations” in its analysis. Ex-1005, [0066], [0093].

173. Cheng discloses or renders obvious the limitation of claim 3[b].

3[c]: “historical data regarding observed times at which the user accesses files.”

174. Cheng discloses or renders obvious historical data regarding observed times at which the user accesses files (e.g., “time of last successful authentication”). *Id.*, [0065]. *See also* claims [1], 3[pre].

175. Cheng further discloses “time of [the] last successful authentication of the user through the mobile device 202.” Ex-1005, [0065]. Cheng discloses that historical data includes “the deviation of the most recent access patterns from the

access history 312 from a longer-term access patterns in the access history 312.”

Id., [0067]. To analyze history, Cheng discloses the “data protection system may collect all pertinent information relating to the data item (e.g., metadata, access history for the mobile device, authentication and context history, security information, etc.).” *Id.*, [0091]. For each of the “time of last successful authentication” and comparing short-term to long-term access patterns, Cheng discloses limitation 3[c].

176. Cheng discloses or renders obvious the limitation of claim 3[c].

7. Claim 4:

“The method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the first access request.”

177. Cheng discloses or renders obvious the method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request (e.g., “the user’s geographic location”). *Id.*, [0041]. *See also* claim [1].

178. Cheng discloses “determining a user’s context, such as the user’s geographic location.” Ex-1005, [0041]. Cheng contemplates different levels of access based on a location. *See id.*, [0046], [0066] (emphasis added) (“The context of the mobile device 202 may include one or more of the following: ***the current location of the mobile device 202,***”). A POSITA would have understood and at

least found it obvious that determining a geographic location would be based on the user's IP address because that was a well-known method of determining a location of a mobile device.

179. Cheng discloses or renders obvious the limitation of claim [4].

8. Claim 5:

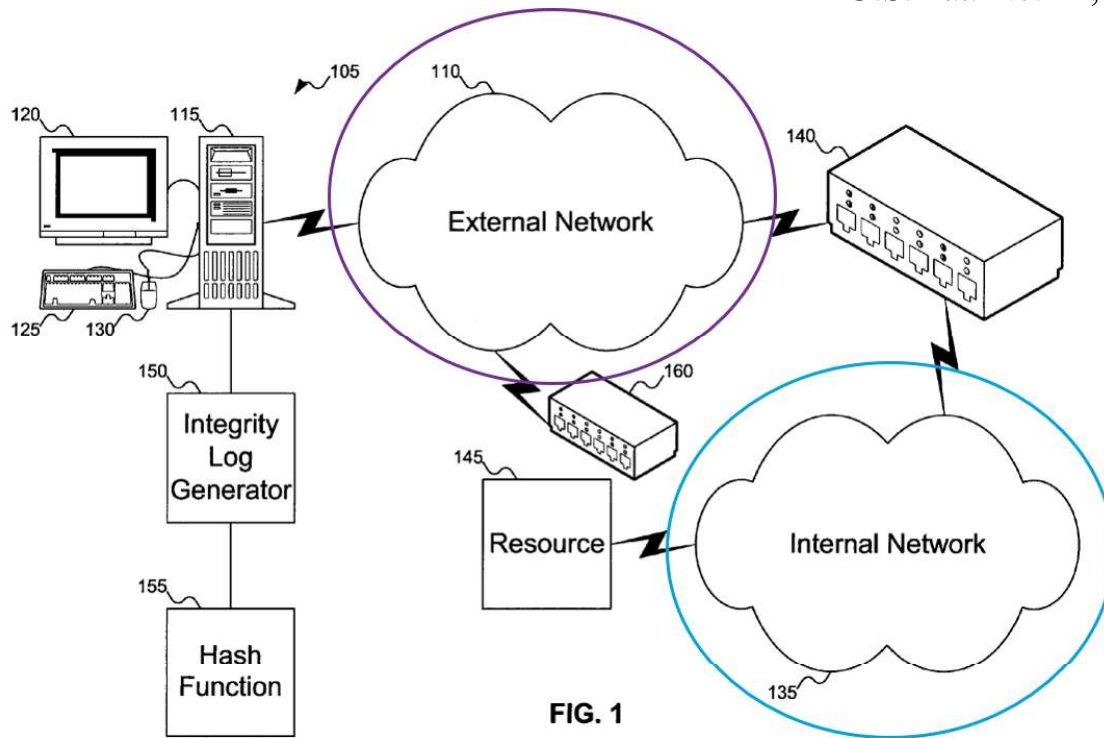
“The method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.”

180. Cheng discloses or renders obvious the method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted (e.g., “the security status of the networks which the device is connected to”). *Id.*, [0066]. *See also* claim [1].

181. Cheng describes determining “the security status of the networks which the device is connected to,” e.g., the level of trust in the network, including enterprise network connection. Ex-1005, [0066]. Cheng contemplates an enterprise environment in which access requests may come from users connected to the enterprise network or to public networks. *See id.*, [0006]; *see also id.*, [0074]. Cheng describes the level of confidence taking into account a user's current context, which includes “security status of the networks which the device is connected to.” *Id.*, [0093]. A POSITA would have understood that analyzing a

user's current context, including network connection, concerns whether a connection is trusted or untrusted.

182. To the extent Cheng does not disclose or suggest this limitation, it would have been obvious in light of Bleckmann. Bleckmann teaches an “[internal network 135](#)” which is a “network that is internal to the organization,” differentiating this from an “[External network 110](#),” “a network external to the organization.” Ex-1006, [0019]. It draws a distinction between systems inside the control of an organization and outside its control. “In one embodiment, integrity validator 140 is used only to validate computer systems that are not directly connected to [internal network 135](#). In this embodiment, there is an implicit assumption that computer systems connected to [internal network 135](#) are known to be safe and validated. This is not necessarily an unreasonable assumption, as computer systems internal to an organization are typically controlled by the organization. Thus, the likelihood of infection by a virus or similar agent is reduced relative to computer systems outside the control of the organization. By making this assumption, computer systems internal to the organization are granted faster access to requested resources, as there is no need to validate such computer systems.” *Id.*, [0028]. *See also id.*, Fig. 1 (colored outlining added):



183. A POSITA would have been motivated to combine Cheng and Bleckmann for the same reasons described above. *See supra* [III.B.3].

184. Cheng, alone or in combination with Bleckmann, discloses or renders obvious the limitation of claim [5].

9. Claim 6:

“The method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.”

185. Cheng discloses or renders obvious the method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection. *See* claims [1], [5].

186. Cheng discloses the level of confidence is affected, at least in part, by “the security status of the networks which the device is connected to.” Ex-1005, [0066], [0093]. Cheng further discloses that “the accumulated authentication score of the user is compared to a minimally required authentication score,” and when “trust is sufficient ... the decryption key is sent to the mobile device.” *Id.*, [0095]. A POSITA would have understood and at least found it obvious that the trustability of the network is considered in this disclosure. Cheng contemplates its invention within the context of enterprise networks then describes that a network’s security status affects the level of confidence. *Id.*, [0006], [0093]. A POSITA would have recognized an enterprise network would provide greater security, and thus would be trusted, whereas a public network would provide less, and would not be trusted.

187. To the extent Cheng does not disclose or suggest this limitation, it would have been obvious in light of Bleckmann.

188. As discussed in claim 5, Bleckmann discloses that there is an “implicit assumption that computer systems connected to [internal network 135](#) are known to be safe and validated.” Ex-1006, [0028]. *See* Fig. 1. A POSITA would have understood an enterprise network to be an “internal network” as described by Bleckmann and that Bleckmann treats the internal network as trusted.

189. A POSITA would have been motivated to combine Cheng and Bleckmann for the same reasons described above. *See supra* [III.B.3].

190. Cheng, alone or in combination with Bleckmann, discloses or renders obvious the limitation of claim [6].

10. Claim 7:

“The method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.”

191. Cheng discloses or renders obvious the method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection. *See* claims [1], [5], [6].

192. Cheng discloses preventing release of a decryption key when the level of confidence is too low. *See* claim [1]. Further, it discloses taking into account the security status of the network. *See* claim [5]. A POSITA would have understood and at least found it obvious that the “untrusted” network of claim 7 is the logical inverse of claim 6’s trusted network. Cheng describes that, for device lock methods, “15 minutes may be too long” for a user at a public bar. Ex-1005, [0007]. It describes “a public location” as one with “a high risk of unauthorized access.” *Id.*, [0074]. A POSITA would have recognized that, compared to the security of an enterprise network, other connections including public connections would be untrusted. Just as a POSITA would understand Cheng discloses the trusted network of claim 6, it discloses the untrusted network of claim 7.

193. To the extent Cheng does not disclose or suggest this limitation, it would have been obvious in light of Bleckmann.

194. As discussed in claims 5 and 6, Bleckmann discloses that there is an “implicit assumption that computer systems connected to [internal network 135](#) are known to be safe and validated.” Ex-1006, [0028]. It draws a clear distinction between this and access outside an internal system, such as [external network 110](#): “Thus, the likelihood of infection by a virus or similar agent is reduced relative to computer systems outside the control of the organization. By making this assumption, computer systems internal to the organization are granted faster access to requested resources, as there is no need to validate such computer systems.” *Id.* A POSITA would understand Bleckmann treats computer systems outside the control of the organization as untrusted.

195. A POSITA would have been motivated to combine Cheng and Bleckmann for the same reasons described above. *See supra* [III.B.3].

196. Cheng, alone or in combination with Bleckmann, discloses or renders obvious the limitation of claim [7].

11. Claim 8:

“The method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.”

197. Cheng discloses or renders obvious the method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper (e.g., “encrypted data item store 226”). Ex-1005, [0061].

198. As specified in the ’623 Patent, a “cryptographic wrapper” is a security layer in a file access control system that encrypts a file with a cryptographic algorithm. Ex-1001, 5:54-64. The cryptographic wrapper is then utilized by the file access control system taught in the ’623 Patent to controls file access, which involves restricting direct access to the unencrypted file unless an authorization process determines that the requesting user is permitted to access it. *Id.* The ’623 Patent specifies that “files of an enterprise network are encapsulated in a cryptographic wrapper, which protects the files by preventing direct access by users who do not have associated cryptographic keys.” *Id.* The wrapper therefore discloses that files “encapsulated in a cryptographic wrapper” refer to encrypted files that are encrypted using “associated cryptographic keys.”

199. Cheng further discloses the “encrypted data item store 226” securely transfers the encrypted data item to the mobile device, e.g., provides the file encapsulated in a cryptographic wrapper. Ex-1005, [0061].

200. Cheng’s data protection system protects data items by encrypting them before storage and transfer. Cheng discloses that “[i]f it is determined that the data item does need protection, protection techniques may be applied to the data

item. In a preferred embodiment, protection techniques may include encryption.”

Id., [0044]. The mechanism by which that encryption is applied is a dedicated key generated specifically for the data item: “[i]n block 108, an encryption key for the data item is determined” and “[i]n block 110, an encrypted version of the data item is created using the encryption key.” *Id.*, [0045].

201. The result of applying that unique encryption key to the data item is an encrypted data item stored in the encrypted data item store 226—a file that has been wrapped in a layer of cryptographic protection and cannot be accessed without the corresponding decryption key. Cheng confirms that the encrypted data item store 226 holds these protected files and releases them to the mobile device when access is initiated, while the decryption key store 224 holds the corresponding keys separately: “the unique identifier may also be used to retrieve the appropriate decryption key from decryption key store 224.” *Id.*, [0059].

202. A POSITA would have understood and at least found it obvious that Cheng’s encrypted data items constitute files encapsulated in a cryptographic wrapper within the meaning of claim 8.

203. Cheng discloses or renders obvious the limitation of claim [8].

12. Claims 9-15:

204. Nearly all limitations of claims 9-15 are substantively identical to limitations of claims [1]-[8], though there are differences in 9[pre] and 14[a].

205. The following chart shows parallel limitations of claims 9-15 with respect to claims 1-8 (emphasis added):

Claims 1-7	Claims 9-13	Claims 14-15
1[a] A method comprising: obtaining and storing, by one or more servers associated with an enterprise network , information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;	9[pre] A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processors of one or more servers associated with an enterprise network , causes the one or more processors to perform a method comprising:	14[a] A system, the system comprising: one or more processors; and a non-transitory computer-readable storage medium coupled to the one or more processors and embodying a set of instructions, which when executed by the one or more processors of one or more servers associated with an enterprise network , causes the one or more processors to perform a method comprising:
1[a] A method comprising: obtaining and storing , by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;	9[a] obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users , wherein <i>the information regarding historical user behavior includes for each user of the plurality of users:</i>	14[b] obtaining and storing information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users; 15[a] The system of claim 14, wherein <i>the information regarding historical user behavior includes for each user of</i>
3[pre] The method of		

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

claim 1, wherein <i>the information regarding historical user behavior includes for each user of the plurality of users:</i>		<i>the plurality of users:</i> ...
3[a] historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;	9[b] historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;	15[a] The system of claim 14, wherein <i>the information regarding historical user behavior includes for each user of the plurality of users:</i> historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;
3[b] historical data regarding observed locations of the user; and	9[c] historical data regarding observed locations of the user; and	15[b] historical data regarding observed locations of the user; and
3[c] historical data regarding observed times at which the user accesses files.	9[d] historical data regarding observed times at which the user accesses files;	15[c] historical data regarding observed times at which the user accesses files.
1[b] receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the	9[e] receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in	14[c] receiving a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

enterprise network in encrypted form;	encrypted form;	encrypted form;
1[c] responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and	9[f] responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and	14[d] responsive to receipt of the file access request, determining a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and
1[d] based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key 1[e] <i>wherein said permitting or denying comprises: ...</i>	9[g] based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key; <i>wherein said permitting or denying comprises:</i>	14[e] based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key, <i>wherein said permitting or denying comprises:</i>
1[e] wherein said permitting or denying comprises: when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;	9[h] when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;	14[f] when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;
1[f] when the risk score is greater than a second threshold, withholding the decryption key; and	9[i] when the risk score is greater than a second threshold, withholding the decryption key; and	14[g] when the risk score is greater than a second threshold, withholding the

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

		decryption key; and
1[g] when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.	9[j] when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.	14[h] when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.
[2] The method of claim 1, wherein said determining , by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.	[10] The non-transitory computer-readable storage medium of claim 9, wherein said determining the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning.	
[4] The method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.	[11] The non-transitory computer-readable storage medium claim 10, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request.	
[5] The method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.	[12] The non-transitory computer-readable storage medium claim 10, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access	

	request is trusted or untrusted.	
[8] The method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.	[13] The non-transitory computer-readable storage medium claim 10, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.	

9[pre] “A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:”/14[a] “A system, the system comprising: one or more processors;” and “a non-transitory computer-readable storage medium coupled to the one or more processors and embodying a set of instructions, which when executed by the one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:”

206. Cheng discloses or renders obvious a non-transitory computer-readable storage medium embodying a set of instructions that, when executed by one or more processors of one or more servers associated with an enterprise network, causes those processors to perform a method.

207. Cheng discloses that “aspects of the present invention may be embodied as a system, method or computer program product” and that those aspects “may take the form of a computer program product embodied in one or more computer readable medium(s) having computer readable program code embodied thereon.” Ex-1005, [0030]. Cheng further discloses that “[a]ny

combination of one or more computer readable medium(s) may be utilized” and that “[a] computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device,” providing a non-exhaustive list of specific examples including “a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory),” and “a magnetic storage device.” *Id.*, [0031]. Cheng confirms that “a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device,” satisfying the non-transitory requirement of the claim. *Id.*; *see also id.*, [0032]-[0033].

208. Cheng further discloses that “[t]hese computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.” *Id.*, [0034]. Those functions are the access control method steps performed by the data protection system when processing a user’s file access request. *See id.*, Figs. 4, 6. This claim limitation is satisfied.

209. As charted above, claim limitations 9[a] and 14[b] cover the same elements as 1[a] and 3[pre]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious elements 1[a] and 3[pre]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[a] and 14[b] for the same reasons.

210. As charted above, claim limitations 9[b] and 15[a] cover the same elements as 3[a]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious element 3[a]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[b] and 15[a] for the same reasons.

211. As charted above, claim limitations 9[c] and 15[b] cover the same elements as 3[b]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious element 3[b]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[c] and 15[b] for the same reasons.

212. As charted above, claim limitations 9[d] and 15[c] cover the same elements as 3[c]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious element 3[c]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[d] and 15[c] for the same reasons.

213. As charted above, claim limitations 9[e] and 14[c] cover the same elements as 1[b]. For the reasons discussed above, Cheng and Bleckmann disclose

and/or render obvious element 1[b]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[e] and 14[c] for the same reasons.

214. As charted above, claim limitations 9[f] and 14[d] cover the same elements as 1[c]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious element 1[c]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[f] and 14[d] for the same reasons.

215. As charted above, claim limitations 9[g] and 14[e] cover the same elements as 1[d]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious element 1[d]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[g] and 14[e] for the same reasons.

216. As charted above, claim limitations 9[h] and 14[f] cover the same elements as 1[e]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious element 1[e]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[h] and 14[f] for the same reasons.

217. As charted above, claim limitations 9[i] and 14[g] cover the same elements as 1[f]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious element 1[f]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[i] and 14[g] for the same reasons.

218. As charted above, claim limitations 9[j] and 14[h] cover the same elements as 1[g]. For the reasons discussed above, Cheng and Bleckmann disclose

and/or render obvious element 1[g]. Consequently, Cheng and Bleckmann disclose and/or render obvious limitations 9[j] and 14[h] for the same reasons.

219. As charted above, claim limitation [10] covers the same elements as [2]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious [2]. Consequently, Cheng and Bleckmann disclose and/or render obvious [10] for the same reasons.

220. As charted above, claim limitation [11] covers the same elements as [4]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious [4]. Consequently, Cheng and Bleckmann disclose and/or render obvious [11] for the same reasons.

221. As charted above, claim limitation [12] covers the same elements as [5]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious [5]. Consequently, Cheng and Bleckmann disclose and/or render obvious [12] for the same reasons.

222. As charted above, claim limitation [13] covers the same elements as [8]. For the reasons discussed above, Cheng and Bleckmann disclose and/or render obvious [8]. Consequently, Cheng and Bleckmann disclose and/or render obvious [13] for the same reasons.

**C. GROUND 2: COMBINATION OF CHENG, BLECKMANN
AND KIRTI RENDERS CLAIMS 2, 4, AND 10-13 OBVIOUS.**

223. Kirti discloses a “cloud security monitoring and control system [that] analyzes information about user activity in one or more clouds using machine learning and other algorithms to perform threat detection and to provide recommendations concerning appropriate responses to different categories of threat.” Ex-1008, 3:54-58.

224. Activity data associated with user accounts includes information relating to the use of and actions taken with a user account at a cloud application, including login and logout statistics, IP addresses used to access the application, devices used to access the application, and cloud resources accessed, including files and folders. *Id.*, 10:30-39. Such event activities are logged with event details including a user name, the resource on which the user performed some action, event time, and network IP address. *Id.*, 18:19-22. Activity data is organized using profiles that cover different time periods through fixed moving windows, and in several embodiments those windows are non-overlapping, such that an eight-week profile does not include events in a four-week profile or one-week profile, and similarly the four-week profile does not include events within the one-week profile. *Id.*, 18:33-67.

225. A risk score is calculated for the user based on the baseline user profile, a ranking of a plurality of users in one or more cloud applications is generated based upon those risk scores, and the risk scores are used to prioritize threat remediation actions within the one or more cloud applications, which helps organizations to remediate the most severe issues first. *Id.*, 1:57-65; 4:15-22.

1. Motivation to Combine

226. A POSITA would have been motivated to combine Cheng and Bleckmann with Kirti with a reasonable expectation of success for several reasons.

227. Cheng, Bleckmann and Kirti are analogous art, which includes server-based access control systems that evaluate the trustworthiness and current context of a requesting user to make dynamic access decisions regarding protected data items in a network environment, and are reasonably pertinent to the same alleged problems, including the need to determine whether a requesting user's access patterns deviate from established normal behavior as part of computing a risk score that controls whether access to an encrypted file is granted or denied.

228. Each reference addresses the problem of deciding whether and to what extent a requesting party should be permitted access to sensitive resources. Ex-1005, [0072]-[0074]; Ex-1008, 1:44-59; Ex-1006, [0008].

229. For example, both Cheng and Kirti teach systems that collect user activity data over time, build profiles reflecting normal user behavior, and evaluate

current access activity against those profiles to identify potential threats to protected resources. *See, e.g.*, Ex-1005, [0024], [0028], [0064], [0089]; Ex-1008, 12:58-64; 14:5-13, Figs. 5B, 5C. Similarly, Bleckmann discloses determining the conditions under which a computer system can be permitted to access a resource. Ex-1006, [0042]. Thus, all three references teach systems for detecting suspicious activity or threats in the context of computer networks.

230. Additionally, both Cheng and Kirti are pertinent to the same alleged problems, including overcoming the limitations of static, rules-based access control approaches that fail to dynamically account for variations in user behavior and context when protecting sensitive data on mobile and enterprise networks. *See, e.g.*, Ex-1005, [0006]-[0008], [0024]; Ex-1008, 4:60-5:24, 14:3-13.

231. A POSITA would have been motivated to apply Kirti's machine learning techniques to Cheng and Bleckmann's score-based data protection system to advantageously provide a more accurate and adaptive model of user behavior for determining whether a user is eligible to receive a decryption key for a requested data item, rather than a fixed accumulated authentication score that does not account for evolving patterns.

232. Cheng acknowledges that its data protection system should evaluate "the level of confidence in the user's identity," in which Bleckmann provides explicit threshold scores, and adjust access decisions based on contextual factors,

but does not expressly teach using machine learning to build the underlying model of user behavior against which access requests are evaluated. Kirti fills this gap, disclosing that “activity data collected from various parameters over period of time can be used with machine learning algorithms to generate patterns referred to as user behavior profiles,” and that algorithms including neural networks, boosted trees, decision trees, and naive Bayes analysis can be trained and deployed to generate a threat score for each user account. Ex-1008, 12:58-13:40, Fig. 5C.

233. Kirti further discloses that IP addresses collected from user access events are resolved to geographic coordinates using a dedicated algorithm, that a baseline profile of valid IP addresses and associated geolocations is maintained for each user, and that a threat is recognized when activity occurs from a geolocation not on that list, directly mapping to the requirement that observed data include a current location of the user as determined from the source IP address. *Id.*, 13:35-42.

234. In applying these teachings to Cheng and Bleckmann, Cheng’s policy decision module 222, as modified with Kirti’s machine learning techniques, would employ a model of user behavior developed by machine learning and trained on historical access data including IP address geolocation patterns to generate the accumulated authentication score or confidence level used to determine whether to deliver a decryption key to the requesting device.

235. Because Cheng already teaches a policy decision module that evaluates user eligibility based on an accumulated authentication score that incorporates the access history and current context of the client device and user (Ex-1005, [0028], [0064], [0089], [0095]), implementing Kirti's machine learning techniques in Cheng's data protection system to develop the underlying model of user behavior would have been a straightforward modification and additive to Cheng, rather than taking anything away from Cheng. Similar to Cheng's policy decision module, which already compares a computed score to a minimum required authentication score to determine whether to provide a decryption key, Kirti teaches applying named machine learning algorithms trained on historical activity data to generate a numerical risk score reflecting deviation from normal user behavior, and resolving source IP addresses from access events to geographic coordinates to identify anomalous access locations.

236. A POSITA would have understood that the combination of Cheng and Bleckmann could be implemented with a machine learning derived behavioral model as taught by Kirti, such that the accumulated authentication score would reflect not only explicit authentication inputs but also the degree to which the current access request conforms to established behavioral and geolocation patterns for that user. In the meantime, a POSITA would have been motivated to keep

Cheng's policy decision module 222 modified with Bleckmann's two-threshold framework as discussed in *supra* §III.B.3.

237. Thus, a POSITA would have found it straightforward and advantageous to apply Kirti's machine learning and IP geolocation teachings to Cheng and Bleckmann's data protection system, and would have known such a combination would predictably work and provide the expected functionality.

2. Claim 2:

238. Kirti discloses or renders obvious "evaluating the file access request with reference to a model of user behavior developed by machine-learning" (e.g., "machine learning algorithms" to "analyze user activity"). Ex-1008, 3:53-61; 5:44-54.

239. Kirti describes "calculating a risk score for the user based on the baseline user profile and generating a ranking of a plurality of users in one or more the cloud applications based upon the risk scores." *Id.*, 2:14-17. "In several embodiments, the cloud security monitoring and control systems analyzes information about user activity in one or more clouds using machine learning and other algorithms." *Id.*, 3:53-56. Kirti further discloses the use of machine learning to "build user behavior profiles" (12:60-64), "establish baselines of user behavior" (4:60-66), and generate "risk scores" (24:39-50).

240. Kirti discloses “evaluating the file access request with reference to a model of user behavior developed by machine-learning” as required by this claim. Cheng and Bleckmann, combined with Kirti, renders claim 2 obvious.

3. Claim 4:

241. Kirti discloses or renders obvious “observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request,” (e.g., “IP addresses and associated valid geolocations”). *Id.*, 2:3-4.

242. Kirti discloses that a baseline profile created by a user includes “a list of IP addresses and associated valid geolocations” and that a geolocation can be determined a threat, i.e. abnormal, based on the IP address. *See id.*, 2:3-7. Kirti describes that IP addresses are the type of activity data a system would analyze for a file access request. “More specific types of activity data can include, but are not limited to, login and logout statistics (including attempts and successes), IP addresses used to access the application, devices used to access the application, and cloud resources that were accessed (including, but not limited to, files and folders in a file management cloud application [such as Box] ...).” *Id.*, 10:34-40.

243. Kirti further discloses “Event correlation analytics can include information such as a list or count of unique IP addresses per day per user (for example a normal condition being five or less) and/or IP addresses resolved to

geolocations within a certain distance from each other (for example, a normal condition being one within 1,000 miles).” *Id.*, 17:13-19.

244. Kirti discloses “observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the file access request” as required by this claim. Cheng and Bleckmann, combined with Kirti, renders claim 4 obvious.

4. Claim 10-13

245. As discussed above, claims 10-13 do not add additional limitations separate from claims 1-8. *See supra* §III.B.12. Claim 10 includes the same “machine learning” limitation from claim 2, as does its dependent claims. Additionally, claim 11 adds only the same limitation as does claim 4.

246. The combination of Cheng, Bleckmann, and Kirti discloses all limitations of claims 10-13 for the same reason as described above.

D. GROUND 3: COMBINATION OF CHENG, BLECKMANN, AND VAN DIJK RENDERS CLAIMS 3, 9-13, AND 15 OBVIOUS

247. Van Dijk discloses an adaptive authentication system that generates a risk score for an incoming access request by comparing it against a baseline profile of the user’s historical request behavior, that baseline built from request records across a series of time windows.

248. Van Dijk's system stores, for each user, a set of database entries in which each entry includes a user identifier, a time period, and behavioral data drawn from observed requests during that period, including a timestamp indicating the time of each request. The system generates the baseline profile from those time-windowed records and computes a User Risk score by comparing the current request against the behavioral patterns observed in that historical data, using the formula "Overall Risk = User Risk x Transaction Risk." *Id.*, 6:38-7:4; 5:17-35.

249. Van Dijk further discloses that adaptive authentication techniques compare information associated with a login attempt, including the time of the login and the location from which it originated, with the historical record of typical expected behavior for that user. *Id.*, 1:17-24.

250. Based on the resulting overall risk score, Van Dijk's access manager determines whether to grant or deny access, and where access is granted, directs a key manager to release the appropriate data protection keys to the requesting user. *Id.*, 8:36-48. The system ties risk-scored behavioral evaluation directly to cryptographic key release. Van Dijk's time-windowed historical database captures times at which the user has previously requested access to files, organized into a time window that serves as the basis for the risk score determination.

251. The disclosure of non-overlapping time windows applied to time-stamped access records, used to build a behavioral baseline against which current

requests are scored, and the release of data protection keys upon a favorable risk determination, address the limitations of claim 3 of the '623 patent.

1. Motivation to Combine

252. A POSITA would have been motivated to combine Cheng and Bleckmann with Van Dijk with a reasonable expectation of success for several reasons.

253. Cheng, Bleckmann, and Van Dijk are analogous art because both are in the same field of risk-scored access control for encrypted sensitive data, and both are pertinent to the same core problem: evaluating whether an access request is authorized based on the trustworthiness of the request, including behavioral signals collected from prior interactions. *See, e.g.*, Ex-1005, [0001], [0003], [0063], [0065]; Ex-1007, 1:6-25, 3:40-65; Ex-1006, [0042].

254. Each reference addresses the problem of deciding whether and to what extent a requesting party should be permitted access to sensitive resources. Ex-1005, [0072]-[0074]; Ex-1007, 2:45-52; Ex-1006, [0008].

255. A POSITA would have been motivated to apply Van Dijk's time-window-indexed behavioral baseline teachings to Cheng's **access history module 312**, coupled with Bleckmann, to advantageously improve the precision of anomaly detection. Cheng already teaches that the level of confidence may be determined based on the history of data access, and that the **access history 312** may

be used to determine if the data accessed or the current context of the mobile device is unusual. *See* Ex-1005, [0065].

256. However, to the extent that the combination of Cheng and Bleckmann, does not specify that this access history includes observing the times at which a user accesses files, a POSITA would have recognized Van Dijk as increasing the effectiveness of deviation detection.

257. Van Dijk discloses that adaptive authentication techniques compare information associated with a login attempt, such as the time of the login, with a historical record of a typical user who exhibits some expected login behavior; that the historical baseline comprises a database where each entry includes a user identifier, a time period, and user data organized into distinct, non-overlapping time intervals. *See* Ex-1007, 1:20-25, 4:33-40.

258. A POSITA would have understood that applying Van Dijk's time-period-indexed structure to Cheng and Bleckmann would make deviation detection more precise by comparing a current access attempt against the user's historical behavior during the same time window in prior periods, rather than an undifferentiated all-time average. This combination would yield the expected and predictable result of a more granular anomaly detection system. In the meantime, a POSITA would have been motivated to keep Cheng's policy decision module 222

modified with Bleckmann's two-threshold framework, as discussed in *supra* §III.B.3.

2. Claim 3:

259. Van Dijk discloses or renders obvious this limitation (e.g. a “timestamp from request 11”) as recited in Claim 3[c]. Ex-1007, 5:19-20.

260. Van Dijk discloses utilizing historical data, including observed time of file access, e.g. timestamps from request 11, in determining file access. “Adaptive authentication techniques typically compare information associated with a login attempt received by the service provider, such as the time of the login and a location from where the login originated, with a historical record of a typical user who exhibits some expected login behavior.” *Id.*, 1:17-25. Authenticator requestor 18 sends request 11 to a user device upon request. *Id.*, 5:17-18. “Processor 22 stores data such as username, fact values and timestamp from request 11.” *Id.*, 5:19-20. *See also id.*, 4:29-47. Van Dijk discloses the limitation of claim 3[c].

261. Cheng and Bleckmann, combined with Van Dijk, renders claim 3 obvious.

3. Claims 9-13, 15:

262. As discussed above, claims 9-15 do not add additional limitations separate from claims 1-8. *See supra* §III.B.12. Claim 9 includes the same limitations from claim 3, as does its dependent claims. Additionally, claim 15 adds

the same limitations to its independent claim as does claim 3. The combination of Cheng and Van Dijk discloses all limitations of claims 9-13, 15 for the same reason as described above.

263. Van Dijk, in view of Cheng and Bleckmann, discloses the limitations of claims 9-13 and 15.

**E. GROUND 4: COMBINATION OF FORD AND VAN DIJK
RENDERS CLAIMS 1-15 OBVIOUS**

264. Ford is directed to “methods and systems contributing to managing digital rights management (DRM) protected content sharing” in an “enterprise network.” Ex-1009, [0005].

265. Ford discloses that the exchange enables “electronic transmission and reception of confidential documents over a global communication network such as the Internet for distributing electronic documents containing sensitive information or data to selected entities, for notifying intended recipients of the availability of such documents, for tracking access, downloading and uploading of such documents, and the like.” *Id.*, [0055]. Ford’s exchange host server “may be distributed over a plurality of server computers,” with the server computers working “together to provide essentially seamless access to a large number of users on various platforms with varying communications speeds.” *Id.*, [0061].

266. Ford discloses secure cross-entity content sharing with DRM/encryption-based protection. *Id.*, [00344], [00354]. Files are stored in encrypted form, users initiate access requests, the server evaluates those requests against a dynamic risk rating derived from a plurality of contextual and behavioral factors, and the server permits or denies access by returning or withholding a decryption key. *Id.*, [00344]-[00345].

267. Ford additionally discloses a matrix of dynamic risk rating states tied to DRM protection controls. *Id.* This includes a graduated access control framework including provision of only a portion of a file based on the user's risk level. *Id.*, [00350]. When a user is granted access to the file, this includes release of a decryption key to decrypt the document. *Id.*, [00354]-[00357]. As demonstrated below, Ford, alone or in combination with Van Dijk, expressly discloses, or at minimum renders obvious to a POSITA, each limitation of Claims 1-15 of the '623 patent. Though Ford describes each aspect of its invention as "an embodiment," it uses this language to describe components and individual functions of one integrated secure-exchange platform as a whole, not distinct embodiments. Further, a POSITA would recognize that combining like-embodiments is straightforward for a POSITA and would not have demanded any ingenuity. *See id.*, [00573] ("While the invention has been disclosed in connection with the preferred

embodiments shown and described in detail, various modifications and improvements thereon will become readily apparent to those skilled in the art.”).

1. Motivation to Combine

268. A POSITA would have been motivated to combine Ford and Van Dijk with a reasonable expectation of success for several reasons.

269. Ford and Van Dijk are analogous art because both are in the same field, which includes server-based access control systems that evaluate the risk of a user’s access request using behavioral signals drawn from prior interactions, and both are pertinent to the problem of determining whether a requesting user’s current access behavior is consistent with established temporal patterns of normal access activity. Ford teaches a secure exchange server that performs risk-based detection based on a user or device history, including pattern of use. Van Dijk similarly teaches adaptive authentication techniques that compare information associated with a login attempt, including the time of the login, with a historical record of a typical user’s expected login behavior.

270. A POSITA would have been motivated to apply Van Dijk’s time-window-indexed behavioral baseline architecture to Ford’s risk detection framework in order to provide a more structured and precise model of normal user access behavior. Ford discloses its dynamic risk rating which may be based on user or device history including timestamps associated with access events. To the extent

Ford does not specify further historical data inputs, a POSITA would have turned to Van Dijk. Van Dijk discloses a historical baseline comprising a database where each entry includes a user identifier, a time period, and user data organized into distinct, non-overlapping time intervals, such that a current access attempt is compared against the user's behavior during the same time window in prior periods. *See* Ex-1007, 4:33-40, 5:10-35.

271. Because Ford already teaches collecting timestamps associated with user access events as part of its risk evaluation framework, incorporating Van Dijk's time-period-indexed structure into Ford's access history records would have been a straightforward modification yielding the expected and predictable result of a more granular anomaly detection system.

2. Claim 1:

1[a]: “A method comprising: obtaining and storing, by one or more servers associated with an enterprise network, information regarding historical user behavior of a plurality of users of the enterprise network by observing file access requests initiated by the plurality of users;”

272. Ford discloses or renders obvious a method (e.g., “methods...contributing to managing digital rights management (DRM) protected content sharing”) comprising: obtaining and storing, by one or more servers associated with an enterprise network (e.g., obtaining and storing, in “data stores” by an “exchange host server...distributed over a plurality of server computers”),

information regarding historical user behavior of a plurality of users of the enterprise network (e.g., information for “risk-based questioning and detection based on a user or device history, such as location, device type, pattern of use, and the like” for “a large number of users”) by observing file access requests initiated by the plurality of users (e.g., by “tracking access, downloading and uploading of such documents” by users).

273. Ford discloses a “method” in a DRM system using an “exchange host server” that comprises “a plurality of server computers” and performs a “method” for managing “DRM” content sharing. Ex-1009, [0053], [0061]. The server uses “data stores” to store information used for “authentication” and “risk-based questioning” to provide file access for a “large number of users.” *Id.*, [0061], [0071], [00221]. Information about the historical behavior of users of the system is collected including by “tracking access, downloading and uploading of such documents” by users using, e.g., an “audit and access history” for protected files in the system. *Id.*, [0055], [0087].

274. Further, Ford discloses a “Contextual Sharing Facility” that “manages the sharing of data based on the contextual environment 4404 of a user.” “The contextual sharing facility may be utilized in file sharing or workstream collaboration, applied to individuals of the same or different enterprises, utilized for managing the sharing.” *Id.*, [00287] “For instance, two users, attempting to

share information between them, may both be operating under sharing constraints placed upon them by different contextual environments.” *Id.*, [00287]-[00289]. A POSITA would have recognized that two users attempting to share files constitutes a file access request.

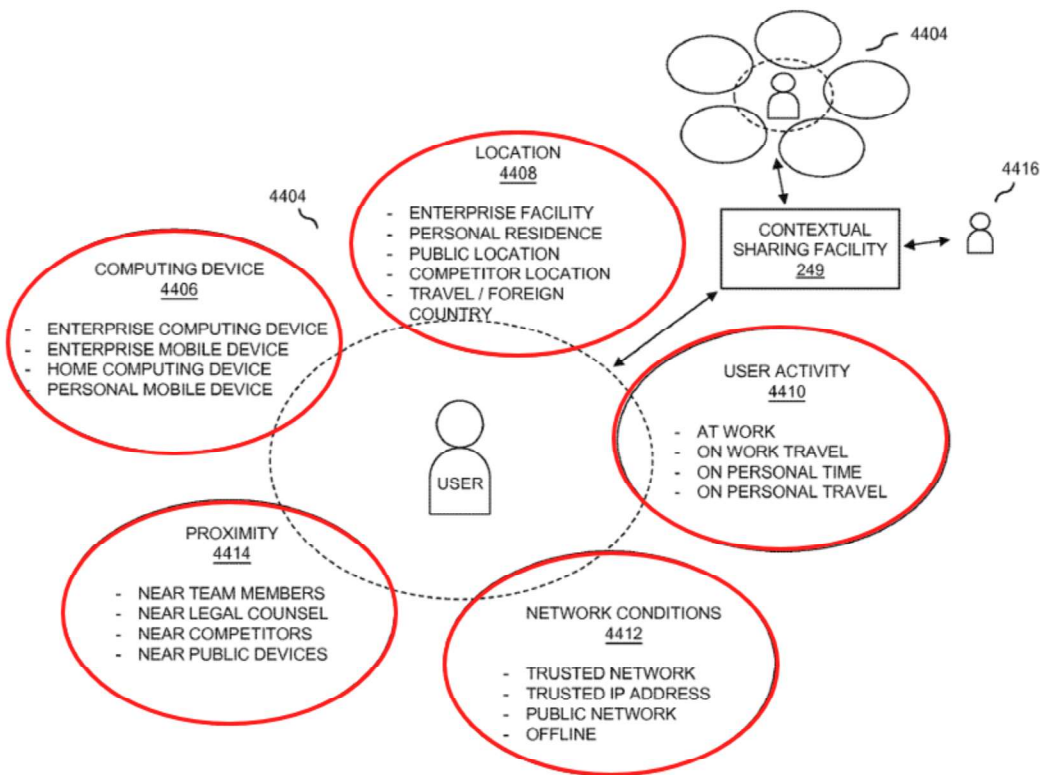


Fig. 44

Id., Fig. 44 (colored outlining added).

275. Ford describes a method of “networked secure collaborative computer data exchange,” including methods and systems contributing to managing digital rights management (DRM).” *Id.*, [0005]. Over exchange servers, documents and files are exchanged over a plurality of servers. *Id.*, [0055]. “In another

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

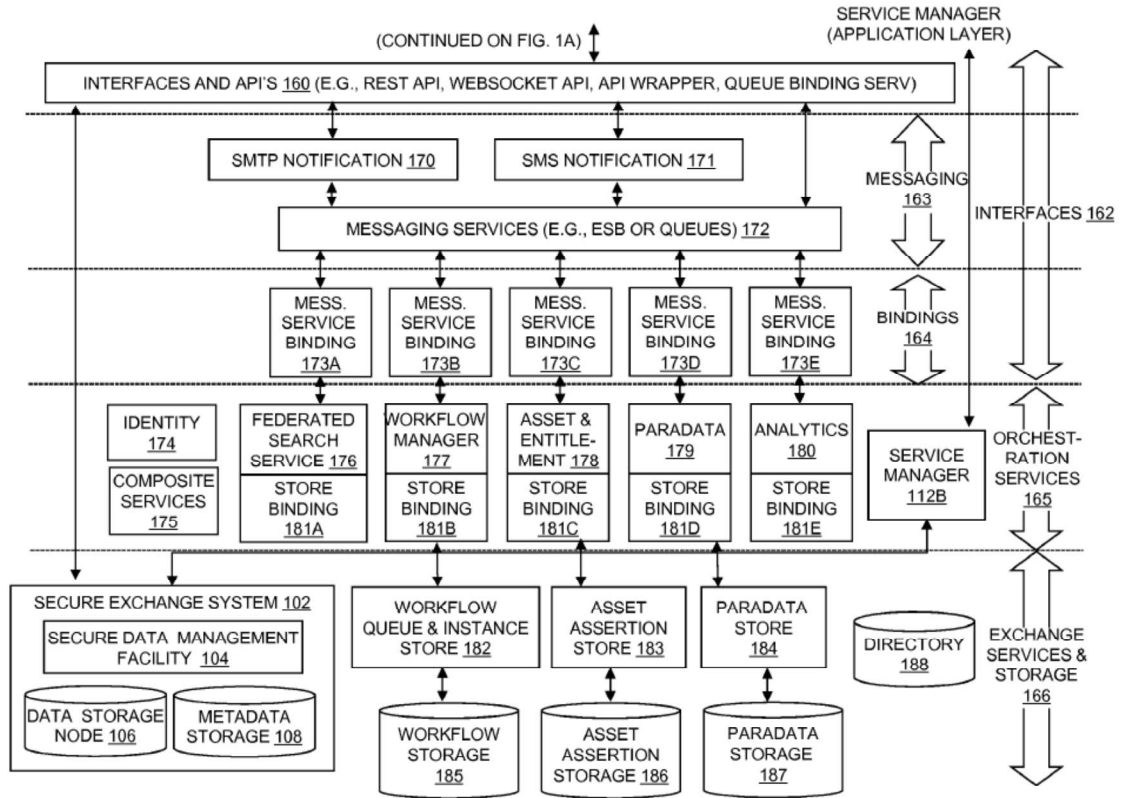


FIG. 1B

Id., Figs. 1A, 1B.

276. Ford discloses servers associated with an enterprise network. “In embodiments, certain modules of the secure exchange system may be at least in part located on enterprise premises 110 to provide on premises and user device applications and services 161, such as client-side customer managed keys, ... content access management ... container digital rights management, contextual sharing facility ... dynamic entitlement management, key management in a secure content environment ... and the like.” *Id.*, [0067]. For example, “the user may be

provided permissions ... to all DRM documents the user has DRM access to that are stored within an enterprise network[.]” *Id.*, [00346].

277. Ford discloses “risk-based questioning and detection based on a user or device history, such as location, device type, pattern of use, and the like.” *Id.*, [00221].

278. To the extent Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk.

279. Van Dijk teaches baseline profiles that are stored within a database which are equivalent to the servers associated with information regarding historical user behavior of a plurality of users.

280. The access manager 340 observes file access requests initiated by the user(s) and will make a determination based on the user’s associated data. Van Dijk stored per-user historical records in database storage keyed by user identifier across the plurality of enterprise network users, maintaining a continuously updated behavioral record for each user of the system. Ex-1007, 4:44-47 (“Storage device 15 is constructed and arranged to store database 16 which contains current and baseline profiles for a user. Database 16 includes a set of entries, each entry of which includes a user identifier, a time period and user data.”); 5:17-25.

281. Van Dijk describes a distributed server-side architecture in which the access manager, key manager, adaptive authentication device, and database storage

may be implemented as server-side components operating within the enterprise network infrastructure. *Id.*, 6:45-48 (“The access manager 340 may be embodied, for example, as an adaptive authentication server, as modified herein to provide the features and functions of the present invention.”). The obtaining and storing of historical user behavioral data, specifically the construction and maintenance of the per-user baseline profile database, is performed by Van Dijk’s server-side adaptive authentication device and database storage components, not by the requesting client. *Id.*, 6:38-63.

282. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 1[a].

1[b]: “receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users, wherein the file access request relates to a file stored within the enterprise network in encrypted form;”

283. Ford discloses or renders obvious receiving, by the one or more servers, a file access request initiated by a first user of the plurality of users (e.g., “a download of the document is requested” from the servers by a “user”), wherein the file access request relates to a file stored within the enterprise network in encrypted form (e.g., request relates to “a document” that is “uploaded” to the system; “the document may be encrypted...through a randomly generated encryption key”). Ex-1009, [00170].

284. Ford discloses a user “request[ing]” a “download of the document” from a server. *Id.* Documents stored at a server that are requested by a user are “encrypted” for storage when the “document is uploaded.” *Id.*

285. Ford discloses documents may be stored within an enterprise network: “the user may be provided permissions ... to all DRM documents the user has DRM access to that are stored within an enterprise network.” *Id.*, [00346].

286. Ford disclosed storing files in encrypted form awaiting an access request. *Id.* “A secure managed key facility may be provided for managing the use of encryption keys, such as for managed content sharing between users in a secure sharing and un-sharing facility, managing access to content through digital rights management, content sharing amongst users in a customizable secure exchange platform ...” where “receiver client 5306” receives the file and decryption key. *Id.*, [00354]-[00357].

287. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 1[b].

1[c]: “responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first user based on a plurality of factors, including information regarding historical user behavior, the file access request and observed data determined based on the file access request; and”

288. Ford discloses or renders obvious responsive to receipt of the file access request, determining, by the one or more servers, a risk score for the first

user (e.g., responsive to an access request, the servers in “the system assign[] a dynamic risk rating (DRR) to a user”), based on a plurality of factors including information regarding historical user behavior (e.g., DRR “may change as conditions associated with the user change” and based on “user or device history”), the file access request (e.g., based on the “action the user wishes to take”) and observed data determined based on the file access request (e.g., “the context of their current location”). *Id.*, [00345].

289. Ford further discloses that in responses to receiving an access request, the server determines whether the “user should not be able to access the document.” *Id.*, [00345]. To make this determination, the system assigns a “dynamic risk rating (DRR)” to a user. *Id.* The rating is based on, e.g., historical information about “user or device history”; what “action the user wishes to take” as specified in the file access request itself; and data determined based on the file access request such as the “context of [the user’s] current location.” *Id.*, [0087], [00221], [00345], [00349].

290. Ford discloses dynamic entitlement, where enterprise policy analyzes a user profile and overrides personal access permissions for DRM. *Id.*, [00345]. “The level of control applied to a document (even if the person is the owner of the document), may be based on their current risk profile as determined by the assigned DRR.” *Id.*

291. Ford discloses “The DRR may be based on IP address, geography, data node factors (e.g., who controls the nodes that data has to travel across), type of data, metadata, action the user wishes to take, and the like.” *Id.* Ford further discloses processing the “complete set of customer data can be reconstituted in its entirety including historical information with date and time information” and “validate the user’s workspace identity, and provide a historical access to the workspace identity.” *Id.*, [00414], [00249].

292. Further, Ford discloses a contextual sharing facility, describing it “may also apply to other access related facilities as described herein, such as for managing the synchronization of documents to a computing device, to determine access control to files, to determine viewing privileges of a document, to control e-signature privileges, secure viewing on a mobile device, and the like.” *Id.*, [00287]. “In embodiments, the contextual sharing facility 249 may reside on a secure server, where the users’ computing devices provide the parameters that comprise the current contextual environment. The server-based contextual sharing facility may then continuously gather contextual parameters from the users’ computing devices, and manage the sharing permissions for devices.” *Id.*, [00291].

293. Ford’s contextual sharing facility analyzes the “contextual environment 4404 of a user,” including the “computing device 4406,” “the location 4408 of the computing device,” “the user’s current activity state 4410,” “network

conditions 4412” and access time. *Id.*, [00287]. A POSITA would have recognized that Ford’s contextual sharing facility disclosures were a part of Ford’s user or device history and resulting DRR score, or at least would have been obvious to include.

294. A POSITA would have also understood and found at least obvious that Ford’s teachings of using “user or device history” as part of a risk calculation discloses and at least renders obvious calculating the DRR using historical user behavior.

295. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 1[c].

1[d]: “based on the risk score, permitting or denying, by the one or more servers, access to the file by returning a decryption key for the file or withholding the decryption key”

296. Ford discloses or renders obvious based on the risk score, permitting or denying, by the one or more servers, access to the file (e.g., based on the “risk score,” servers determine whether “the user should not be able to access the document”) by returning a decryption key for the file or withholding the decryption key (e.g., by “provid[ing] the receiver user with a decryption key if access is permitted”). *Id.*, [00345].

297. Ford further discloses that the system’s servers determine that a “user should not be able to access the document” depending on the user’s “DRR”/“risk

score.” *Id.* As discussed further for 1[e]-1[f], the servers “provide the receiver user with a decryption key” only if “access is permitted.” *Id.*, [00356]-[00357].

298. Discussing both document access and system access, Ford discloses “if a user’s risk score is not higher than X” then access will not be allowed. *Id.*, [00345]. Additionally, it discloses different classifications to understand a risk score: “The DRR may have a classification such as highly sensitive, low sensitivity, and the like.” *Id.*

299. Ford directly ties this risk score, DRR, to file access: “Extending a user’s DRM-based entitlement permissions may relate to DRM documents that the user has permission to access or to DRM documents that they do not have explicit permission to access.” *Id.*, [00346]. Ford describes files access as generating decryption keys when access is enabled and sending these keys to users. *Id.*, (“The secure managed key facility may then use the content key reference to retrieve the content key from the key store, and provide the receiver user with a decryption key if access is permitted.”).

300. Ford requires the secure management key facility to first “determine[] that the receiver user has permission to access the content file” before it “may send the receiver user the decryption key to decrypt the content file.” *Id.*, [00361]. A POSITA would have recognized or at least found obvious that this requires withholding the decryption key if conditions are not met.

301. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 1[d].

1[e]: “wherein said permitting or denying comprises when the risk score is less than a first threshold, returning the decryption key and providing full access to the file;”

302. Ford discloses or renders obvious wherein said permitting or denying comprises: when the risk score is less than a first threshold (e.g., in “a matrix of DRR states,” when the “risk score” is “higher than X”), returning the decryption key and providing full access to the file (e.g., grant “access” and “provide the receiver user with a decryption key if access is permitted”). Ex-1009, [00345], [00357].

303. As explained for 1[d], Ford discloses granting a user access to a file based on the user’s DRR. Ford further discloses that granting “access” is based on “a matrix of DRR states.” *Id.*, [00345]. If the user’s “risk score” is “higher than X” then the user can access “highly sensitive” information and is granted “access” to the file, and the system also “provide[s] the receiver user with a decryption key.” *Id.*, [00345], [00356]-[00357].

304. Ford’s teachings of a “matrix” with a “risk score” that is, e.g., “higher than X” discloses or renders obvious a risk score that is less than a first threshold. Ford states that “higher than” is exemplary; implementing this teaching by having a risk score be higher than a threshold (i.e., trust is higher) vs. lower than an

equivalent threshold (i.e., risk is higher) disclose the same functionality. At most, the difference between this limitation and Ford's teachings would have been nothing more than an obvious design choice to a POSITA that is nothing more than the selection between two known and substantially similar alternatives. *See id.*, [00345].

305. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 1[e].

1[f]: “when the risk score is greater than a second threshold, withholding the decryption key; and”

306. Ford discloses or renders obvious when the risk score is greater than a second threshold, (e.g., in the “matrix of DRR states,” “user’s risk score is not higher than X” and should not see even a “portion of the file”) withholding the decryption key (e.g., determine the “user should not be able to access the document.”). *Id.*

307. Ford further discloses determining, based on the user’s “risk score” not satisfying a threshold of “X,” the user’s access is limited to “low sensitivity” information and the user “should not be able to access the document.” *Id.* The secure managed key facility withholds the decryption key if it is determined access should be denied. *Id.*, [00357].

308. As further explained below for 1[g], a POSITA would have understood or at least found it obvious that multiple thresholds are in the “matrix of DRR states” such that, between first and second thresholds, access is granted to a “portion of a file”—disclosing that there are “DRR” states present between the two thresholds. *Id.*, [00350].

309. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 1[f].

1[g]: “when the risk score is between the first threshold and the second threshold, returning the decryption key and providing limited access to the file.”

310. Ford discloses or renders obvious when the risk score is between the first threshold and the second threshold (e.g., in the “matrix of DRR states,” a “second user” may access “only a portion of a file...based on the second user’s risk level”), returning a decryption key and providing limited access to the file (e.g., “restrict access by providing a second user only a portion of a file, rather than the whole file, based on the second user’s risk level”). Ex-1009, [00345], [00350]

311. Ford further discloses that, in addition to granting or denying access to a file, users also may be granted access to “only a portion of a file” or one-time as opposed to “offline” file access. *Id.*, [00350], [00227]-[00229], [00241]-[00242]; *see also id.*, [00345]. A POSITA would have understood or at least found it

obvious that this discloses at least two separate thresholds for (1) denying and (2) granting partial access to a file instead of granting full access. *See id.*

312. Ford teaches using such intermediate levels for documents in an “uncertain security state,” e.g., when an employee is “working from home,” or an employee needs to share a document with a “third party” without access to a “secure storage facility.” *Id.*, [00430]; *see also id.*, [00345]-[00346] (discussing using DRR to control user access based on factors including “geographic location” and “location context”). Access may be determined “per [an] access policy,” resulting in the secure managed key facility providing the decryption key to the user. *Id.*, [00356].

313. Ford’s context sharing facility further discloses that “utilized to restrict or to enhance sharing opportunities.” *Id.*, [00287]. “For instance, the contextual sharing facility 249 may be applied to sharing in a workstream, where sharing may be restricted based on the conditions under which users are working.” *Id.* “The contextual sharing facility may allow, restrict, deny, and the like, the sharing of information with a second user based upon the parameters 4406, 4408, 4410, 4412, 4414 or other contextual environment parameters under which users finds themselves. The second user may have contextual sharing constraints placed upon them as based upon their contextual environment 4404.” *Id.*, [00288].

314. The '623 patent itself does not describe how releasing a single decryption key provides forms of intermediate access, except to suggest transfer via VPN as an embodiment. To the extent this limitation is only met when a single decryption key is utilized, using a single encryption key is expressly contemplated by Ford. Ford teaches that “a single encryption key may provide for multiple accesses, such as determined by the offline file access facility at the time the encryption keys 1208 were downloaded to the mobile computing device.” *Id.*, [00288], [00356].

315. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 1[g].

3. Claim 2:

“The method of claim 1, wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine learning,”

316. Ford discloses or renders obvious the method of claim 1, wherein said determining, by the one or more servers, the risk score for the first user comprises evaluating the file access request with reference to a model of user behavior developed by machine-learning (e.g., “devices having artificial intelligence”). Ex.1009, [00569].

317. Ford discloses that authentication may utilize patterns of use. *Id.*, [00221]. Ford further discusses the applicability of its disclosures for “devices having artificial intelligence,” e.g., the use of machine learning, such that a POSITA would have been informed to apply this to create a model of user behavior. *Id.*, [00569]. A POSITA would have understood or at least found it obvious that this includes evaluating a file access request by utilizing artificial intelligence, i.e. machine learning, to analyze/determine a risk score.

318. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 2.

4. Claim 3:

3[pre]: “The method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users:”

319. To the extent the preamble of claim 3 is found to be limiting, Ford discloses or renders obvious the method of claim 1, wherein the information regarding historical user behavior includes for each user of the plurality of users. *See* claim [1].

320. Ford further discloses information regarding historical user behavior (e.g., “tracking access, downloading and uploading of such documents” by users using, e.g., an “audit and access history” for protected files in the system.) Ex-1009, [0055], [0087]. *See* claim [1].

321. To the extent Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk.

322. Van Dijk teaches baseline profiles that are stored within a database which are equivalent to the servers associated with information regarding historical user behavior of a plurality of users. (e.g., Van Dijk stored per-user historical records in database storage keyed by user identifier across the plurality of enterprise network users, maintaining a continuously updated behavioral record for each user of the system, “Storage device 15 is constructed and arranged to store database 16 which contains current and baseline profiles for a user. Database 16 includes a set of entries, each entry of which includes a user identifier, a time period and user data.”). Ex-1007, 4:44-47.

323. Ford, along or in combination with Van Dijk, discloses or renders obvious the limitation of claim 3[pre].

3[a]: “historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time;”

324. Ford discloses or renders obvious historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by

the user over the predetermined period of time (e.g., “user or device history, such as...pattern of use”).

325. As explained for 1[a], Ford discloses that the system uses “historical” information about the user when determining whether to grant access to a file. This information includes, e.g., “pattern of use” information—which a POSITA would have understood and found obvious includes one or more of a number of files accessed by the user over a predetermined period of time, types of the files accessed, and applications used by the user over the predetermined period of time. *See* Ex-1009, [00221] (“Multi-factor authentication may set authentication requirements beyond username and password, to not only challenge questions, but to risk-based questioning and detection based on a user or device history, such as location, device type, pattern of use, and the like.”). For example, it was well understood that a user’s “pattern of use” comprises the frequency, number, and type of files and applications used.

326. A POSITA would have understood that Ford’s disclosure of multi-factor authentication applies to the Dynamic Entitlement Management disclosures, and that this limitation is taught by Ford.

327. Ford’s contextual sharing facility describes “contextual environment 4404 of a user” which includes “what computing device 4406 the user is utilizing when attempting to share information (e.g., enterprise computing device, enterprise

mobile device, home computing device, personal mobile device), the location 4408 of the computing device (e.g., enterprise facility, personal residence, public location, competitor location, on travel, in a foreign country), the user's current activity state 4410 (e.g., at work, on work travel, on personal time, on personal travel), network conditions 4412 (e.g., connected to a trusted network, using a trusted IP address, connected to a public network, operating offline of a network), proximity 4414 (e.g., near team members, near legal counsel, near competitors, near public devices), time (e.g., during regular work hours, on weekends, during normal sleep time), based on a restrictive list (e.g., a white list, a black list, a combined listing of individuals by sharing privilege), and the like.” *Id.*, [00287].

328. Ford discloses the contextual environment “may then continuously gather contextual parameters from the users’ computing devices, and manage the sharing permissions for devices.” *Id.*, [00291]. A POSITA would have understood the disclosure of “continuously gather[ing]” contextual information, alongside analyzing a “pattern of use” as disclosing historical data.

329. To the extent that Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk.

330. Van Dijk discloses historical data regarding general file access, including one or more of a number of files accessed by the user over a predetermined period of time (e.g., previous browsing and other network access

history), types of the files accessed, and applications used by the user over the predetermined period of time (e.g., “software running thereon” compared to baseline profiles). Ex-1007, 6:38-7:4.

331. Van Dijk’s access manager measures “various aspects of the client device including software running thereon, previous browsing and other network access history, various nearby devices including their locations, as well as other factors,” and compares “[t]he measured factors of the client device” with “prior results obtained from the same user as well as other users who might access the system.” *Id.*; *see also id.* 1:13-25; 4:42-47. That historical record of prior network access activity and software usage encompasses the number and type of prior access events and the applications used to initiate them.

332. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 3[a].

3[b]: “historical data regarding observed locations of the user; and”

333. Ford discloses or renders obvious historical data regarding observed locations of the user (e.g., “determin[ing] the geographical location of a person using the device”/location-based security). Ex-1009, [00220].

334. As explained for 1[a], Ford discloses that the system uses “historical” information about the user when determining whether to grant access to a file. Ford discloses a “a location-based security facility 290” which provides server-based

file access “where permissions of the file determine access based on location, such as the location of the device requesting the file or resource. Enterprises often want to limit access to sensitive data based on whether someone is physically present at a facility or location.” *Id.* The user’s location informs the risk profile. *Id.*, [00286] (“Synchronization may also take the current risk profile of a computing device into account (e.g., a user is on travel in China versus they are in the corporate home office).”).

335. This information includes, e.g., “pattern of use” information—which a POSITA would have understood and found obvious includes data regarding observed locations of the user. For example, it was well understood that a user’s “pattern of use” comprises location from which the user accesses a network or the physical location of the user’s hardware during use.

336. Ford’s contextual sharing facility discloses a “contextual environment 4404” that includes access locations: “the location 4408 of the computing device (e.g., enterprise facility, personal residence, public location, competitor location, on travel, in a foreign country)” and “proximity 4414 (e.g., near team members, near legal counsel, near competitors, near public devices)” *Id.*, [00287]. *See also id.*, [00288]-[00292].

337. To the extent that Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk.

338. Van Dijk discloses that adaptive authentication techniques “compare information associated with a login attempt received by the service provider, such as the time of the login and a location from where the login originated, with a historical record of a typical user who exhibits some expected login behavior.” Ex-1007, 1:13-25. The comparison of a current access location against a historical record of typical user locations teaches the user of historical data regarding observed locations of the user.

339. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 3[b].

3[c]: “historical data regarding observed times at which the user accesses files.”

340. Ford discloses or renders obvious historical data regarding observed times at which the user accesses files (may provide the ability to know where the data resided at any time, as well as who accessed it, for all content that is stored for any purpose associated with the enterprise, regardless of the type of store (cloud, data center, individual device), the location of the same, or the type of content that is accessed.).

341. As explained for 1[a], 3[a], Ford discloses that the system uses “historical” information about the user when determining whether to grant access to a file.

342. Ford discloses historical data regarding file access. In discussing sharing (and “un-sharing”) of file access, Ford discusses time-based factors. “Un-sharing may be triggered based on a policy, based on time-based factors (e.g., access is provided for a limited time), based on a requirement that the destination user re-establish credentials to use the viewer, and the like.” Ex-1009, [00187]. Additionally, Ford discloses a user’s historical views of a file through “changes to documents through indicators of modification, or ‘modification stamps’, on the documents that have been marked as favorites by a user.” *Id.*, [00161].

343. Ford’s contextual sharing facility discloses a “contextual environment 4404” that includes access times: “e.g., during regular work hours, on weekends, during normal sleep time.” *Id.*, [00287]. “One of the contextual environment’s parameters may also be time, such as a user being able to share under certain parameter conditions during regular working hours.” *Id.*, [00289]. *See also id.*, [00287]-[00292].

344. A POSITA would have understood and found obvious, given’s Ford disclosure of the use of historical information, to include times at which a user accesses files in the historical user behavior.

345. To the extent that Ford does not disclose or suggest this limitation, it would have been obvious in light of Van Dijk.

346. Van Dijk discloses utilizing historical data, including observed time of file access, e.g. timestamps from request 11, in determining file access. “Adaptive authentication techniques typically compare information associated with a login attempt received by the service provider, such as the time of the login and a location from where the login originated, with a historical record of a typical user who exhibits some expected login behavior.” Ex-1007, 1:17-25. Authenticator requestor 18 sends request 11 to a user device upon request. *Id.*, 5:17-18. “Processor 22 stores data such as username, fact values and timestamp from request 11.” *Id.*, 5:19-20. *See also id.*, 4:29-47.

347. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 3[c].

5. Claim 4:

“The method of claim 1, wherein the observed data includes a current location of the first user as determined based on a source Internet Protocol (IP) address contained in the first access request.”

348. Ford discloses or renders obvious the observed data includes a current location of the first user (e.g., user’s “DRR” is based on “current location” of the user) as determined based on a source Internet Protocol (IP) address contained in the file access request (e.g., using a “trusted IP address”).

349. Ford further discloses determining a user’s DRR using the “current location” of the user. Ex-1009, [00345]. Information about the user’s location

includes, e.g., a “network conditions 4412 (e.g., connected to ***a trusted network, using a trusted IP address***, connected to a public network, operating offline of a network)” for the user. *Id.*, [00287] (emphasis added). For example, Ford teaches that trusted IP addresses are “specified” to “establish an access restriction rule.” *Id.*, [00371]. A POSITA would have understood that “trusted” IP addresses would be associated with known locations; for example, IP addresses “may restrict a user from accessing the secure exchange facility from their work computer.” *Id.*

350. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 4.

6. Claim 5:

“The method of claim 1, wherein the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted.”

351. Ford discloses or renders obvious the observed data includes a status indicative of whether the connection through which the first user initiated the file access request is trusted or untrusted (e.g., “the security level provided by a network connection”).

352. Ford teaches “DRM protection for customer managed keys may provide access control that is controlled ... contextually (e.g., the user’s location, ***the security level provided by a network connection***).” *Id.*, [00367] (emphasis added). “A user’s authorization for viewing may be determined at least in part on

the network connectivity of the mobile device, such as with the enterprise network, a trusted network, a WiFi network, and the like. For instance, a user may not be authorized to download a secure document through a cellular network, such as when they are not connected to a WiFi or wired network connection.” *Id.*, [00157]. The system thus monitors “network connectivity” of a device when determining if a user may access content. *Id.* For example, a user connecting through a “trusted network” may be granted “authorization for viewing” content, but “may not be authorized” on a “cellular network.” *Id.* Additionally, Ford discloses determining a user’s permissions based on geographic location, which a POSITA would have recognized as determined by IP address. *Id.*, [00350].

353. Ford’s contextual sharing facility further discloses observing connection status, explicitly describing trusted versus untrusted networks. The contextual environment analyzed includes “network conditions 4412 (e.g., connected to a trusted network, using a trusted IP address, connected to a public network, operating offline of a network).” *Id.*, [00287]. “For instance, all users may be considered to be unconstrained (or relatively unconstrained) under a certain set of conditions, such as being at their own desk in their enterprise facility connected to the trusted enterprise network.” *Id.*, [00289].

354. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 5.

7. **Claim 6:**

“The method of claim 5, wherein the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection.”

355. Ford discloses or renders obvious the connection is trusted when the first user is on the enterprise network or accessing the enterprise network remotely via a secure connection (e.g., when on the “enterprise network” or a “trusted network”).

356. As explained for claim [5], Ford teaches that access control is controlled by the “security level provided by a network connection.” Ex-1009, [00367]. Ford further exemplifies connectivity through “enterprise,” “trusted,” “WiFi network, and the like” as trusted network connections, contrasting “cellular” connections, one a POSITA would have understood as untrusted. *Id.*, [00157].

357. Ford’s contextual sharing facility further discloses observing connection status, explicitly describing trusted versus untrusted networks. The contextual environment analyzed includes “network conditions 4412 (e.g., connected to a trusted network, using a trusted IP address, connected to a public network, operating offline of a network).” *Id.*, [00287]. “For instance, all users may be considered to be unconstrained (or relatively unconstrained) under a certain set of conditions, such as being at their own desk in their enterprise facility connected to the trusted enterprise network.” *Id.*, [00289].

358. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 6.

8. Claim 7:

“The method of claim 5, wherein the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection.”

359. Ford discloses or renders obvious the connection is untrusted when the first user is not on the enterprise network or accessing the enterprise network remotely via an insecure connection (e.g., connection not through a “trusted” or “like” connection; use “may not be authorized” “outside their home” or “outside a small geographic area around an office around an enterprise...and the like”).

360. As explained for claims [5]-[6], Ford teaches that access control is controlled by “the security level provided by a network connection.” *Id.*, [00367]. Access may be denied when not connected through the “enterprise,” “trusted,” or “like” connections. *Id.*, [00157]. For example, such network connectivity limits access outside a “small geographic area around an office of an enterprise, around the user’s home, on a known transportation route...and the like,” or is connecting remotely via an insecure “cellular” connection. *Id.*

361. Ford’s contextual sharing facility further discloses observing connection status, explicitly describing trusted versus untrusted networks. The contextual environment analyzed includes “network conditions 4412 (e.g.,

connected to a trusted network, using a trusted IP address, connected to a public network, operating offline of a network).” *Id.*, [00287]. “For instance, all users may be considered to be unconstrained (or relatively unconstrained) under a certain set of conditions, such as being at their own desk in their enterprise facility connected to the trusted enterprise network.” *Id.*, [00289].

362. Ford contrasts trusted enterprise networks with public networks, treating them as untrusted and restricting access: “For instance, a user may be constrained from sharing information with a second user because the first user is at home, but whose sharing privileges become unconstrained when they get to work.” *Id.*, [00287].

363. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 7.

9. Claim 8:

“The method of claim 1, wherein the encrypted form involves the file being encapsulated in a cryptographic wrapper.”

364. Ford discloses or renders obvious the encrypted form involves the file being encapsulated in a cryptographic wrapper (e.g., content uses “end-to-end encryption” and is “encrypted and remain[s] encrypted/protected for the rest of its lifecycle”; data encrypted using a “customer key” and “system master key”).

365. Ford further teaches that encrypting stored content includes implementing “end-to-end encryption” for the content such that the “data content” is “encrypted and remain[s] encrypted/protected for the rest of its lifecycle.” Ford, [00375]. Ford teaches that customer managed keys “provide the ability for customers to control their own data encryption keys” and that “both the system-provided keys and the customer keys are needed in order to access the data, such that neither can do it alone.” *Id.*, [00362].

366. Ford describes additional cryptographical protection, including “generating random data key and key ID per file, encrypting file with the data key, encrypting the data key with a customer key, and encrypting the data key with a system master key.” *Id.* Ford teaches using both a “customer key” and “system master key” to encrypt data such that both keys are required to decrypt the data. *Id.*

367. Because this form of end-to-end encryption means a cryptographic key is required to decrypt and access the content, a POSITA would have understood Ford to disclose using cryptographic wrappers to protect content—and at least render obvious the same. *See id.*

368. Ford, alone or in combination with Van Dijk, discloses or renders obvious the limitation of claim 8.

10. Claims 9-15

369. As discussed above, there is only one limitation not present in claims 9-15 represented in claims 1-8. *See supra* §III.B.12. With exception to that limitation, discussed below, claims 9-15 are disclosed or rendered obvious by Ford in combination with Van Dijk for the same reasons as discussed in claims 1-8.

9[pre] A non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:”; 14[a] “A system, the system comprising: one or more processors;” and “a non-transitory computer-readable storage medium coupled to the one or more processors and embodying a set of instructions, which when executed by the one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method comprising:”

370. Ford discloses or renders obvious a non-transitory computer-readable storage medium embodying a set of instructions, which when executed by one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method. (e.g., “methods and systems...may be deployed...through a machine that executes computer software on a server”; server “may include...computer readable media, storage media” associated with an “enterprise intranet”). Ex-1009, [00560].

371. Ford further discloses a system (e.g., “system”), the system comprising: one or more processors; and a non-transitory computer-readable

storage medium coupled to the one or more processors and embodying a set of instructions, which when executed by the one or more processors of one or more servers associated with an enterprise network, causes the one or more processors to perform a method (e.g., “server” in “enterprise internet” has “one or more...processors,” “computer readable media, storage media,” and the processors “execute[...]instructions” to “deploy[]” the “method”). *Id.*, [00560]-[0562].

372. Ford further discloses that the disclosed teachings are implemented in an enterprise environment using multiple “servers” with multiple “processors” implementing disclosed methods using “instructions” stored in “computer readable media” and “storage media.” *Id.*, [00560].

373. As charted above, claim limitations 9[a] and 14[b] cover the same elements as 1[a]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious element 1[a]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[a] and 14[b] for the same reasons.

374. As charted above, claim limitations 9[b] and 15[a] cover the same elements as 3[a]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious element 3[a]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[b] and 15[a] for the same reasons.

375. As charted above, claim limitations 9[c] and 15[b] cover the same elements as 3[b]. For the reasons discussed above, Ford and Van Dijk disclose

and/or render obvious element 3[b]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[c] and 15[b] for the same reasons.

376. As charted above, claim limitations 9[d] and 15[c] cover the same elements as 3[c]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious element 3[c]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[d] and 15[c] for the same reasons.

377. As charted above, claim limitations 9[e] and 14[c] cover the same elements as 1[b]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious element 1[b]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[e] and 14[c] for the same reasons.

378. As charted above, claim limitations 9[f] and 14[d] cover the same elements as 1[c]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious element 1[c]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[f] and 14[d] for the same reasons.

379. As charted above, claim limitations 9[g] and 14[e] cover the same elements as 1[d]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious element 1[d]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[g] and 14[e] for the same reasons.

380. As charted above, claim limitations 9[h] and 14[f] cover the same elements as 1[e]. For the reasons discussed above, Ford and Van Dijk disclose

and/or render obvious element 1[e]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[h] and 14[f] for the same reasons.

381. As charted above, claim limitations 9[i] and 14[g] cover the same elements as 1[f]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious element 1[f]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[i] and 14[g] for the same reasons.

382. As charted above, claim limitations 9[j] and 14[h] cover the same elements as 1[g]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious element 1[g]. Consequently, Ford and Van Dijk disclose and/or render obvious limitations 9[j] and 14[h] for the same reasons.

383. As charted above, claim limitation [10] covers the same elements as claim [2]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious [2]. Consequently, Ford and Van Dijk disclose and/or render obvious [10] for the same reasons.

384. As charted above, claim limitation [11] covers the same elements as claim [4]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious [4]. Consequently, Ford and Van Dijk disclose and/or render obvious [11] for the same reasons.

385. As charted above, claim limitation [12] covers the same elements as claim [5]. For the reasons discussed above, Ford and Van Dijk disclose and/or

render obvious [5]. Consequently, Ford and Van Dijk disclose and/or render obvious [12] for the same reasons.

386. As charted above, claim limitation [13] covers the same elements as claim [8]. For the reasons discussed above, Ford and Van Dijk disclose and/or render obvious [8]. Consequently, Ford and Van Dijk disclose and/or render obvious [13] for the same reasons.

F. GROUND 5: COMBINATION OF FORD, VAN DIJK, AND KIRTI RENDERS CLAIMS 2 AND 10-13 OBVIOUS

1. Motivation to Combine

387. A POSITA would have been motivated to combine Ford and Van Dijk with Kirti with a reasonable expectation of success for several reasons.

388. Ford, Van Dijk, and Kirti are analogous art because they are in the same field, which includes server-based access control systems that evaluate the risk of a user's access request using behavioral signals drawn from prior interactions to determine whether protected data should be made available, and are reasonably pertinent to the same alleged problems, including the need for a dynamic, automated, and continuously improving mechanism for assessing whether a requesting user's current behavior is consistent with established normal behavior patterns.

389. Ford teaches a secure exchange server that implements multi-factor authentication going beyond username and password to include risk-based questioning and detection based on a user or device history, such as location, device type, and pattern of use. Ex-1009, [00221]. Van Dijk similarly teaches “access control systems that mediate access to derivatives of sensitive data,” including an adaptive authentication server. Ex-1007, 1:52-53; 6:45-49. Kirti likewise teaches that activity data collected from various parameters over a period of time can be used with machine learning algorithms to generate patterns referred to as user behavior profiles. Ex-1008, 13:2-42.

390. A POSITA would have been motivated to apply Kirti’s machine-learning techniques to Ford’s risk-based access control framework in combination with Van Dijk to advantageously provide a more accurate, adaptive, and automated model of user behavior for determining whether a user’s access request should be granted, one that continuously improves based on observed behavioral data rather than relying solely on manually configured risk rules or static scoring criteria. Ford teaches a dynamic risk rating that can change as conditions associated with the user change and may be based on signals such as IP address, geography, data node factors, type of data, metadata, and the action the user wishes to take. Ex-1009, [00345].

391. Kirti expands this idea, disclosing that the aggregation of user activity information in the analytics repository enables the system to establish baselines of user behavior and that machine learning techniques can then be applied to detect threats, including deviations from baseline expectations and behavior analytics to derive suspicious behavior, with algorithms and profiles trained to intelligently predict whether an unusual behavior is a security risk. Ex-1008, 12:28-57; 13:2-42.

392. Kirti further discloses that named machine learning algorithms, including neural networks, boosted trees, decision trees, and clustering, are applied to user activity data to generate a threat score, directly mapping to Claim 2's requirement that the risk score be determined by evaluating the file access request with reference to a model of user behavior developed by machine learning. *Id.*, 12:58-13:27.

393. Because Ford and Van Dijk already teach collecting and using behavioral and contextual history, including user or device history such as location, device type, and pattern of use, to drive risk-based access decisions, implementing Kirti's machine learning techniques within Ford's risk scoring framework to develop the underlying model of user behavior would have been a straightforward modification. Ex-1009, [00221]; Ex-1007, 4:33-43. Similar to Ford's dynamic risk rating mechanism or Van Dijk's "Overall Risk" calculation, which already evaluate a combination of contextual signals to produce a risk-based access

determination, Kirti teaches applying machine learning algorithms trained on historical activity data to generate a numerical risk score reflecting deviation from normal user behavior.

394. A POSITA would have understood that Ford's dynamic risk rating engine with Van Dijk's contributions could be implemented with a machine-learning-derived behavioral model as taught by Kirti, such that the risk score would reflect the degree to which the current access request conforms to behavioral patterns established from historical user activity data.

395. Thus, a POSITA would have found it straightforward and advantageous to apply Kirti's machine learning teachings to Ford's risk-based access control system, and would have known such a combination, yielding the limitation of Claim 2 of the '623 patent requiring a model of user behavior developed by machine learning, would predictably work and provide the expected functionality. In the meantime, a POSITA would have also been motivated to apply Van Dijk's time-window-indexed behavioral baseline architecture to Ford's risk detection framework, as discussed *supra* §III.E.1.

2. Claims 2, 10-13:

396. As discussed above, Kirti discloses or renders obvious machine learning as required by claims 2, 10-13. *See supra* §III.C.2.

**G. GROUND 6: COMBINATION OF FORD, VAN DIJK, AND
BLECKMANN RENDERS CLAIMS 1-15 OBVIOUS**

1. Motivation to Combine

397. A POSITA would have been motivated to combine Ford and Van Dijk with Bleckmann with a reasonable expectation of success for several reasons.

398. Ford, Van Dijk, and Bleckmann are analogous art, which includes server-based access control systems that evaluate the risk or trustworthiness of a requesting party to determine the appropriate level of access to a protected resource, and both are pertinent to the problem of defining structured, threshold-based access control policies that produce differentiated outcomes depending on the degree of trust or risk associated with the request.

399. Ford teaches a secure exchange server that implements risk-based detection and multi-factor authentication based on a user or device history, including location, device type, and pattern of use, and assigns a dynamic risk rating that may change as conditions associated with the user change. Ex-1009, [00221]. Van Dijk similarly teaches “access control systems that mediate access to derivatives of sensitive data,” including an adaptive authentication server. Ex-1007, 1:52-53; 6:45-49. Bleckmann similarly teaches a trust score-based access control system in which a policy controls access to a resource based on the trust score generated for the requesting computer. Ex-1006, [0042].

400. A POSITA would have been motivated to apply Bleckmann's two-threshold policy framework to a Ford and Van Dijk combination, allowing the risk-based access control system to advantageously include a structured, tiered access architecture that produces differentiated outcomes depending on the level of confidence in the requesting user, rather than relying solely on a binary grant or deny determination.

401. Ford teaches that its dynamic risk rating may be used to drive risk-based access decisions, but does not teach a two-threshold policy producing three discrete access outcomes keyed to separate risk levels. Bleckmann fills this gap directly, disclosing that a policy including two threshold scores controls access to a resource such that if the trust score meets or exceeds the first threshold, the computer system is granted full access to the resource; if the trust score falls below the first threshold but meets or exceeds the second threshold, the computer system is granted partial access; and if the trust score falls below the second threshold, the computer system is denied access entirely. *Id.*, [0043].

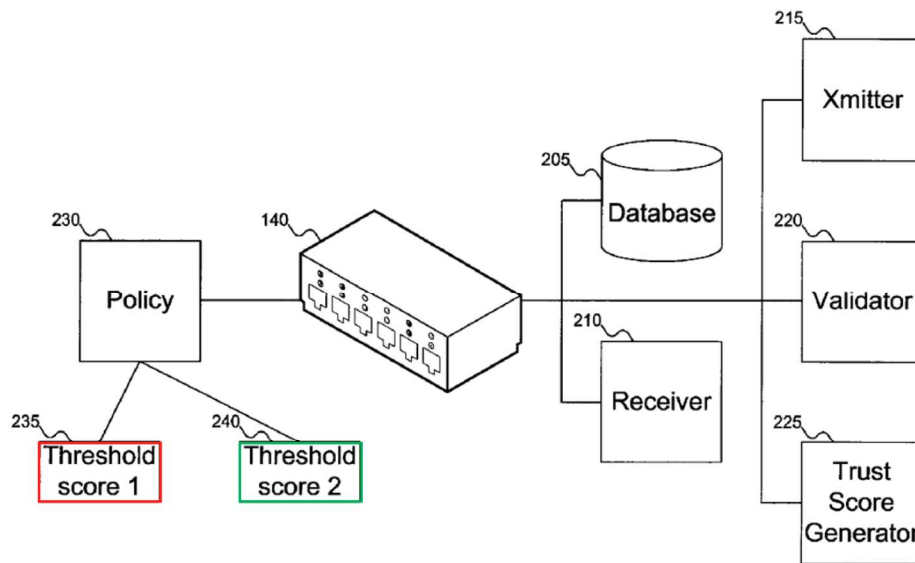
402. Because both Ford and Van Dijk already teach computing a dynamic risk rating or Overall Risk based on behavioral and contextual signals associated with the access request and using that rating to drive an access control determination, implementing Bleckmann's two-threshold policy framework within Ford and Van Dijk would have been a straightforward modification.

403. A POSITA would have understood that Ford's dynamic risk rating could be evaluated against two defined threshold values, as Bleckmann teaches, such that the access control determination produces three discrete outcomes: full access when the rating satisfies the higher threshold, partial access when the rating falls between the two thresholds, and denial when the rating falls below the lower threshold. Thus, a POSITA would have found it straightforward and advantageous to apply Bleckmann's two-threshold access control policy to Ford's risk-based access control system, and would have known such a combination would predictably work and provide the expected functionality. In the meantime, a POSITA would have also been motivated to apply Van Dijk's time-window-indexed behavioral baseline architecture to Ford's risk detection framework, as discussed *supra* §§III.E.1, III.F.1.

2. Claim 1

404. Bleckmann discloses a first and second threshold as required by claim 1. *See supra* §III.B.2. Bleckmann discloses **Threshold score 1**, i.e. a first threshold and **Threshold score 2**, i.e. a second threshold. "In one embodiment, policy 230 includes **threshold score 235**. To be granted access to the resource, the computer system should have a trust score at least as high as threshold score 235." Ex-1006, [0042].

405. “In another embodiment, policy 230 can include multiple threshold scores. For example, in FIG. 2, policy 230 is shown as including two threshold scores 235 and 240. If the trust score for the computer system is at least as high as threshold score 235, then the computer system can be granted full access to the resource. If the trust score for the computer is less than threshold score 235 but at least as high as threshold score 240, then the computer system can be granted partial access to the resource. And if the trust score for the computer system is smaller than threshold score 240, the computer system can be denied access to the resource (although the computer system can be redirected to a help resource to determine why the computer system has such a low trust score).” *Id.*, [0043].



Id., Fig. 2 (colored outlining added).

406. Additionally, Bleckmann discloses providing limited access to the file, as required by claim 1. *See id.*; *see also supra* §III.B.4.

407. In the combination of Ford, Van Dijk, and Bleckmann, a POSITA would find it obvious to implement Bleckmann's Threshold score 1 and Threshold score 2 with Ford and Van Dijk. Ford discloses three tiers of access: grant, deny, or limited access. Ex-1006, [0043]; Ex-1009, [00350]. For example, Ford describes granting access based on "a matrix of DRR states," such that if the user's "risk score" is "higher than X" then the user can access "highly sensitive" information. Ex-1009, [00345]. Bleckmann's Threshold score 1 and Threshold score 2 provides a POSITA with explicit values to replace "X" such that Ford's DRR falls clearly into one of the three outcomes.

H. GROUND 7: COMBINATION OF FORD, VAN DIJK, BLECKMANN AND KIRTI RENDERS CLAIMS 2 AND 10-13 OBVIOUS

408. The elements of these claims are met for the same reasons as in Ground 5. *See supra* §III.F.

409. Because Ford and Van Dijk already teach collecting and using behavioral and contextual history, including user or device history such as location, device type, and pattern of use, to drive risk-based access decisions, implementing Kirti's machine learning techniques within Ford's risk scoring framework to develop the underlying model of user behavior would have been a straightforward

modification. Ex-1009, [00221]; Ex-1007, 4:33-43. The addition of Bleckmann supplying discrete values as thresholds for claim 1 does not change this analysis. Similar to Ford's dynamic risk rating mechanism or Van Dijk's "Overall Risk" calculation, which already evaluate a combination of contextual signals to produce a risk-based access determination, Kirti teaches applying machine learning algorithms trained on historical activity data to generate a numerical risk score reflecting deviation from normal user behavior. A POSITA would have been motivated to combine Ford, Van Dijk, Bleckmann, and Kirti for the same reasons as above. *See supra* §§III.F.1, III.G.1.

Declaration of Paul Martin
In Support of Petition for *Inter Partes* Review of
U.S. Pat. No. 11,449,623

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001; and further that such willful false statements may jeopardize the validity of the application or any patent issued thereon. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on 2026-09-14 in Potomac, MD.



Paul D. Martin, Ph.D.

APPENDIX A

Paul D. Martin, Ph.D.
 Chief Scientist at Harbor Experts
 Lecturer at Johns Hopkins University

P: 443.449.9006
 E: paul@harborexper.com

Profile

Dr. Martin has testified more than **19 times** in complex software- and hardware-related litigation, including **13 depositions**, **4 trials**, and **2 evidentiary hearings**. He has led and managed more than 100 large-scale source code reviews involving sophisticated software and hardware systems. Dr. Martin is the Chief Scientist at Harbor Experts and a Lecturer in the Department of Computer Science at Johns Hopkins University, where he teaches courses on software development, computer and network security, and cryptography. His research interests include embedded system security, operating system security, vulnerability analysis, reverse engineering, network protocol analysis, applied cryptography, and privacy-preserving protocols.

Education

2011-2016	<i>Ph.D. Computer Science, Johns Hopkins University, Baltimore, MD</i>
2011-2013	<i>M.S.E. Computer Science, Johns Hopkins University, Baltimore, MD</i>
2007-2011	<i>B.S. Computer Science, Johns Hopkins University, Baltimore, MD</i>

Industry Experience

2024-Present	<i>Harbor Experts</i>	Chief Scientist
2023-Present	<i>Johns Hopkins University</i>	Lecturer
2023-2024	<i>Harbor Labs</i>	Vice President of Applied Research and Technology
2018-2024	<i>Harbor Labs</i>	Director of Firmware Security, Senior Research Scientist
2013-2018	<i>Harbor Labs</i>	Research Scientist
2011-2016	<i>Johns Hopkins University</i>	PhD Candidate, Research Assistant
2013	<i>Applied Communication Sciences</i>	Graduate Intern
2011	<i>University of Michigan</i>	Penetration Tester
	<i>Inter-university Consortium for Political and Social Research (ICPSR)</i>	
2009-2011	<i>Independent Security Evaluators</i>	Security Intern
2008-2010	<i>Johns Hopkins University</i>	Student Software Developer
	<i>Digital Research and Curation Center (DRCC)</i>	
2008	<i>Brandeis University</i>	Freelance Software Developer

Teaching Experience

2025	<i>Intermediate Programming</i>	Lecturer
2024	<i>Security and Privacy in Computing</i>	Lecturer
2023	<i>Security and Privacy in Computing</i>	Lecturer
2015	<i>Introduction to Hardware Hacking</i>	Instructor
2012-2014	<i>Security and Privacy</i>	Teaching Assistant
2011	<i>Practical Cryptographic Systems</i>	Course Assistant

Publications

P. Martin, D. Russel, M. Ben Salem, S. Checkoway, A. Rubin, Sentinel: Secure Mode Profiling and Enforcement for Embedded Systems, Proc. ACM/IEEE International Conference on Internet-of-Things Design and Implementation, (IoTDI '18).

P. Martin, M. Rushanan, T. Tantillo, C. Lehmann and A. Rubin, Applications of Secure Location Sensing in Healthcare. In the proceedings of ACM Conference of Bioinformatics, Computational Biology, and Health Informatics (BCB '16).

J. Carrigan, P. Martin, M. Rushanan, KBID: Kerberos Bracelet Identification. In the Proceedings of Financial Cryptography and Data Security (FC '16).

P. Martin, M. Rushanan, S. Checkoway, M. Green, A. Rubin. Classifying Network Protocol Implementation Versions: An OpenSSL Case Study. Technical Report 13-01, Johns Hopkins University (December 2013).

P. Martin, A. Rubin, and R. Bhatti, *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control*. In ACM Conference on Bioinformatics, Computational Biology, and Biomedical Informatics Health Informatics Symposium (BCB-HIS), (September 2013)

Professional Committees & Standards Bodies

IEEE 7024 Working Group — “Standard for the Procurement, Verification and Validation, and Life Cycle Management of Forensic Technologies” (Current Member)

IEEE Symposium on Security and Privacy (Winter 2024)

IEEE Symposium on Security and Privacy (Summer 2024)

Patents

System and Method for automatically extracting information from binary files for use in Database Queries	US 10,762,214 B1
System and method for network traffic profiling and visualization	US 10,230,599 B2
System and method for network traffic profiling and visualization	US 9,667,521 B2
Healthcare privacy breach prevention through integrated audit and access control	US 8,984,583 B2
Healthcare privacy breach prevention through integrated audit and access control	US 9,438,632 B2

Current Research

Quantifying vulnerability divergence and patch lead time between rolling and enterprise Linux distributions, including whether enterprise distributions should share soft-forked package versions.

Performance analysis and optimization of local large language model inference, including forecasting of architecture and parameter-scaling trends.

Use of multimodal large language models for diagnosis of disease progression.

Use of large language models for certain types of technical research and analysis.

Expert Witness Engagements

Evox Productions, LLC v. Cars.com, LLC

Case:

Case # 5:25-cv-02357-KK-SP

Description:

Analysis related to web architecture.

Services:

Source code review, expert report drafting, comparative analysis.

Expert Testimony at Deposition:

Potomac, MD (August 26, 2026)

Malikie Innovations Ltd, Key Patent Innovations Ltd v. Foundry, Inc.

Case: Case # 7:25-CV-00567-DC-DTG
 Description: Analysis related to cryptography, elliptic curve cryptography, hardware accelerated cryptography.
 Services: Source code review, claim construction, expert report drafting, validity analysis, infringement analysis.
 Expert Testimony at Deposition: Potomac, MD (July 31, 2026)

The Nielsen Company v. TVision

Case: Case #. 25-575-CJB
 Description: Analysis related to audience measurement and identification systems and audio fingerprinting systems.
 Services: Source code review, expert report drafting, source code and algorithm analysis and simulations.
 Expert Testimony at Trial: Wilmington, DE (June 8-9, 2026)

CERTAIN FLASH-SPUN NONWOVEN MATERIALS AND PRODUCTS CONTAINING SAME

Case: ITC Investigation No. 337-TA-1424
 Description: ITC Investigation related to nation-state threat actors, unfair competition and trade secret misappropriation.
 Services: Malware analysis and reverse engineering, cyber-attribution, computer forensics, reasonableness of security measures.
 Expert Testimony at Deposition: Washington, DC (September 6, 2025)
 Expert Testimony at Trial: Washington, DC (January 29, 2026)

Malikie Innovations Ltd, Key Patent Innovations Ltd v. MARA Holdings, Inc.

Case: Case # 7:25-cv-00222-DC-DTG
 Description: Analysis related to cryptography, elliptic curve cryptography, random number generation and cryptocurrencies.
 Services: Source code review, expert report drafting, validity analysis.
 Expert Testimony at Deposition: Potomac, MD (January 22, 2026)

Bayerische Motoren Werke Aktiengesellschaft v. Onesta IP, LLC

Case: Case # 6:2025-cv-00581
 Description: Analysis related to power and latency-sensitive process scheduling.
 Services: Expert declaration drafting, patent analysis.

Toyota Motor Corp v. AutoConnect Holdings LLC

Case: PGR2025-00041
 Description: Analysis related to cloud-based vehicle management and security systems.
 Services: Expert report drafting, validity analysis.

Twitch Interactive, Inc. v. Razdog Holdings LLC,

Case: IPR2025-03017
 Description: Analysis related to cloud-based content aggregation and streaming.
 Services: Invalidity analysis. IPR drafting.
 Expert Testimony at Deposition: Washington, DC (October 10, 2025)

The Nielsen Company v. Hyphametrics, Inc.

Case: Case # 23-136-GBW-CJB
 Description: Analysis related to audience measurement and identification systems and machine learning systems.
 Services: Source code review, expert report drafting, infringement

	analysis.
Expert Testimony at Deposition:	Potomac, MD (February 5, 2025)
Expert Testimony at Trial:	Wilmington, DE (July 24-25, 2025)
Jonathan Day and Michelle Dobek v. Advanced Micro Devices, Inc.	
Case:	Case # 3:22-cv-04305
Description:	Litigation related to computer fTPM and TEE design characteristics.
Services:	Technical analysis and expert reports on security and performance characteristics of trusted execution environments and the design of NVRAM interfaces through SPI. Drafting of expert reports.
Expert Testimony at Deposition:	Washington, DC (February 7, 2025)
State of New Jersey v. Paul Caneiro	
Case:	Indictment # 19-02-283; PG # 18-4915
Description:	Analysis related to reliability of specific types of computerized DNA analysis in criminal proceedings.
Services:	Source code review, expert report drafting.
Expert Testimony at Hearing:	Freehold, NJ (December 6, 2024)
Amazon.com, Inc. v. B.S.D. Crown, Ltd.,	
Case:	IPR2025-00057
Description:	Analysis related to emulation and virtualization technology.
Services:	Invalidity analysis. IPR drafting.
MediaTek Inc. v. Daedalus Prime LLC	
Case:	IPR2025-00100
Description:	Analysis related to security processors embedded in microprocessors.
Services:	Invalidity analysis. IPR drafting.
McKinney v. Corsair Gaming, Inc.	
Case:	Case # 4:22-cv-00312-JST
Description:	Litigation related to computer memory performance.
Services:	Technical analysis and expert reports on characteristics of computer memory and forensic analysis of computer systems.
LoganTree v. Fossil	
Case:	Case # 21-cv-0385-JDW
Description:	Litigation related to fitness tracking wearables.
Services:	Technical analysis and expert reports on validity and infringement.
Expert Testimony at Deposition:	Monrovia, MD (August 11, 2023)
Nielsen v. TVSquared	
Case:	Case # 6:22-cv-00244-ADA
Description:	Litigation related to network-based audience measurement.
Services:	Technical analysis and expert reports on patentable subject matter.
ISI v. Intuitive Surgical, Inc.	
Case:	Case # 3:21-cv-03496-VC
Description:	Litigation related to cryptographic security protections.
Services:	Technical analysis and expert reports on security and technical aspects of surgical devices.
Expert Testimony at Deposition:	Monrovia, MD (March 16, 2023)

Healthcare Advanced Risk Technologies, Inc. and Inspirien Holdings Corp. v. Terrence Mills, Al.io Corp., Jane Nemcova and VEUU, Inc.

Case: Case # 2:22-cv-04192-JS-AYS
 Description: Litigation related to timeline of software development and misappropriation of trade secrets.
 Services: Source code and documentation review, source code copying analysis, expert report drafting.

Communication Technologies, Inc. v. Samsung Electronics America, Inc., and Samsung Electronics Co. Ltd.

Case: Case # 2:21-cv-444-JRG
 Description: Litigation related to patents on secure erase processes.
 Services: Source code review of algorithms related to secure erase processes, declaration on aspects of source code review process and representativeness of source code

Planck, LLC D/B/A Patch Media v. Particle Media, Inc. D/B/A News Break, Et. Al.

Case: Case # 20-cv-10959 (LGS)
 Description: Litigation related to copyright.
 Services: Review of web scraping facts, contracts and agreements and syndicated web feed technology, declaration on web scraping and syndicated web feed technology

WSOU Investments, LLC D/B/A Brazos Licensing and Development v. Cisco, Inc.

Case: Case # 6:21-cv-00128-ADA
 Description: Litigation related to patents on wireless network handoff, network management and authentication technologies.
 Services: Source code review of accused products, declaration on aspects of source code review process.

United States v. Laffon Ellis

Case: Case # 2:19-cr-00369-DWA
 Description: Analysis related to reliability of specific types of computerized DNA analysis in criminal proceedings.
 Services: Source code review, expert report drafting.
 Expert Testimony at Hearing: Monrovia, MD (December 20, 2021)

Sysmex Corporation and Sysmex America, Inc. v. Beckman Coulter, Inc.

Case: CA # 19-1642-RGA-CJB
 Description: Litigation related to hematology analysis machine patents.
 Services: Source code review. Expert report drafting.
 Expert Testimony at Deposition: Monrovia, MD (November 22, 2021)

CERTAIN ROUTERS, ACCESS POINTS, CONTROLLERS, NETWORK MANAGEMENT DEVICES, OTHER NETWORKING PRODUCTS, AND HARDWARE AND SOFTWARE COMPONENTS THEREOF

Case: ITC Investigation No. 337-TA-1227
 Description: ITC Investigation related to patents on wireless network handoff, network management and QoS technologies.
 Services: Source code review, validity and prior art analysis, expert report drafting.
 Expert Testimony at Deposition: Monrovia, MD (June 9-10, 2021)
 Expert Testimony at Trial: Washington, DC (July 28, 2021)

Micro Focus, Inc. v. Insurance Services Organization

Case: DE Civil Action # 15-252-RGA
 Description: Litigation related to unlicensed use of runtime environments, libraries and software compilers.

Services: Source code review. Binary reverse engineering and analysis, affidavit drafting, expert report drafting.
Expert Testimony at Deposition: Wilmington, DE (Feb 2, 2021)

loanDepot.com, LLC v. Sigma Infosolutions, Inc.

Case: AAA Case # 01-18-0001-5821
Description: Litigation related to software development practices.
Services: Source code analysis, experimentation, report drafting.
Expert Testimony at Deposition: Baltimore, MD (December 17, 2019)

Cypress Lake Software, Inc. v. Samsung Electronics America and Dell, Inc.

Case: Case # 6:18-cv-00030-RWS
Description: Litigation related to infringement of UX patents.
Services: Source code analysis, report drafting.
Expert Testimony at Deposition: Baltimore, MD (July 9, 2019)

Apple, Inc. Device Performance Litigation

Case: CA Civil Action # 18-md-02827-EJD
Description: Litigation related to business practices.
Services: Technical analysis and expert reports on security and technical aspects of mobile phone forensics.

Italian Antitrust Authority v. Apple, Inc.

Case: PS/11309
Description: Litigation related to business practices.
Services: Technical analysis and expert reports on security and technical aspects of software update processes.

Carl Zeiss AG and ASML Netherlands B.V. v. Nikon

Case: Case # 2:17-cv-07083-RGK (MRWx)
Description: Litigation related to patents on image detection algorithms.
Services: Source code review of algorithms related to image processing and detection algorithms, declaration on aspects of source code review process.

Decision Resources, LLC v. Brigham Hyde, Precision Health Intelligence, LLC and Orr Inbar

Case: MA Civil Action # 17-2834J
Description: Litigation related to timeline of software development and misappropriation of trade secrets.
Services: Source code and documentation review, development timeline analysis, affidavit drafting.

Litigation Support

Video Solutions v. Cisco, Inc

Case: Case # 2:23-cv-222-JRG
Description: Litigation related to videoconferencing and network performance optimization.
Services: Infringement analysis. Source code review.

OmniTracs, LLC v. Motive Technologies, Inc.

Case: Case # 3:23-cv-05261-RFL
Description: Litigation related to driver fleet management.
Services: infringement analysis. Source code review.

Robocast v. Netflix, Inc

Case: Case # 1:22-cv-00305-JLH-CJB
Description: Litigation related to hypermedia and multimedia node

structures.
Services: Invalidity and noninfringement analysis and report drafting.
Source code review.

Proxense, LLC. v. Google, LLC

Case: Case # 6:23-cv-00320-ADA
Description: Litigation related to patents on biometrics and payment processing.
Services: Claim construction analysis and report drafting.

Epic Games, Inc. & Anor vs. Apple Inc & Anor

Case: Case # NSD 1236 of 2020
Description: Litigation related to security and competition.
Services: Document review, interviews, report drafting.

Softex LLC v. Absolute Software Corporation, Dell Technologies Inc, and HP Inc.

Case: Case # 1:22-cv-01309-DAE
Description: Litigation related to computer anti-theft technology.
Services: Claim construction analysis, source code review, report review, binary reverse engineering and product testing.

Mediapointe, Inc v. Microsoft Corporation

Case: Case # 2:22-cv-01009-MCS-MRW
Description: Litigation related to content delivery networks.
Services: Claim construction analysis, source code review, validity analysis, infringement analysis, report drafting.

Mediapointe, Inc v. Akamai Corporation

Case: Case # 2:22-cv-06233-MCS-AFM
Description: Litigation related to content delivery networks.
Services: Claim construction analysis, source code review, validity analysis, infringement analysis, report drafting.

Lauri Valjakka v. Netflix, Inc

Case: Case # 4:22-cv-01490-JST
Description: Litigation related to content delivery networks.
Services: Claim construction analysis, invalidity analysis, noninfringement analysis, report review.

Fanduel, Inc v. Winview, Inc

Case: IPR 2022-01306, IPR-01307
Description: Litigation related to patents on probability systems.
Services: Document review, invalidity analysis, report review.

Proxense, LLC. v. Samsung Electronics America, Inc., and Samsung Electronics

Case: Case # 6:21-cv-00210-ADA
Description: Litigation related to patents on biometrics and payment processing.
Services: Source code review, documentation review, product testing, validity analysis, infringement analysis, report drafting.

Global Eticket Exchange Ltd. vs. TicketMaster LLC

Case: Case # 6:21-cv-00399-ADA
Description: Litigation related to patents on electronic ticketing.
Services: Source code review, documentation review, product testing, invalidity analysis, non-infringement analysis, report drafting.

US Dominion, Inc. vs. Fox News Network

Case: Case # N21C-03-257-EMD
 Description: Litigation related to defamation and voting machine security.
 Services: Source code review, documentation review, product testing, report drafting.

Centripetal Networks, Inc. vs. Keysight Technologies, Inc.

Case: Case # 2:22-cv-0002-AWA-DEM
 Description: Litigation related to patents on network monitoring devices and security gateways.
 Services: Source code review, documentation review, product testing, noninfringement analysis, infringement analysis.

Milliman, Inc and Vigilytics LLC, vs. Gradient A.I. Corp.

Case: Case # 1:21-cv-10865-NMG
 Description: Litigation related to breach of contract and source code copying.
 Services: Source code review, documentation review.

WSOU Investments, LLC D/B/A Brazos Licensing and Development v. Microsoft Corporation

Case: Case # 6:20-cv-00464-ADA, 6:20-cv-00460-ADA, 6:20-cv-00457-ADA,
 Description: Litigation related to patents on telephony management systems and skill-based matchmaking.
 Services: Source code review, documentation review, validity analysis, infringement analysis, report drafting.

10Tales Inc. v. TikTok PTE. Ltd.

Case: Case # 1:18-cv-826-WCB
 Description: Litigation related to patents on user-adapted video streams.
 Services: Claim construction analysis.

Carriere v. Symantec Corporation

Case: Case # 500-06-000894-176
 Description: Class action litigation related to product security.
 Services: Source code review, documentation review, report drafting.

IOENGINE, LLC v. Ingenico, Inc.

Case: Case # 1:18-cv-826-WCB
 Description: Litigation related to patents on payment processing systems.
 Services: Source code review, documentation review, validity analysis, infringement analysis, report drafting.

IOENGINE, LLC v. PayPal Holdings, Inc.

Case: Case # 1:18-cv-452-WCB
 Description: Litigation related to patents on payment processing systems.
 Services: Source code review, documentation review, validity analysis, infringement analysis, report drafting.

AGIS Software Development LLC v. Uber Technologies

Case: Case # 2:21-cv-00026-JRG-RSP
 Description: Litigation related to patents on map overlays and messaging systems.
 Services: Source code review.

Finjan v. Palo Alto Networks

Case: Case # 4:14-CV-04908-PJH
 Description: Litigation related to patents on malware scanning gateways.
 Services: Invalidity analysis, Claim construction analysis, source code review.

Huawei Technologies Co. v. Verizon Communications Inc.

Case: Case # 6:20-CV-00090
 Description: Litigation related to patents on malware scanning gateways with cloud components.
 Services: Source code review, non-infringement analysis.

Epic Games, Inc. vs. Apple, Inc.

Case: Case # 4:20-cv-05640-YGR-TSH
 Description: Litigation related to security and competition.
 Services: Document review, interviews, report drafting.

Philips North America LLC ; Koninklijke Philips N.V. vs. Summit Imaging Inc.

Case: Case # 2:19-cv-01745-JLR
 Description: Litigation related to third-party repair services.
 Services: Source code review, document review, report drafting.

California Physicians Service, Inc D/B/A Blue Shield of California vs. Healthplan Services Inc,

Case: Case # 3:18-cv-3730
 Description: Litigation related to software development practices and breach of contract.
 Services: Document review, source code review, report drafting.

Finjan v. Qualys

Case: Case # 4:18-cv-07229-YGR
 Description: Litigation related to patents on vulnerability assessment products.
 Services: Invalidity analysis, Non-infringement analysis, source code review, report drafting.

Finjan v. Sonicwall

Case: Case # 5:17-cv-04467-BLF-HRL
 Description: Litigation related to patents on malware scanning gateways.
 Services: Invalidity analysis, Non-infringement analysis, source code review, report drafting.

TecSec Inc. v. Cisco and Oracle

Case: Case # 1:10-cv-115 LO-TCB
 Description: Litigation related to patents on hardware accelerated cryptographic processors.
 Services: Infringement analysis, validity analysis, source code review, report drafting.

Blackberry Limited v. Facebook, Inc.

Case: Case # 2:18-cv-01844-KSx
 Description: Litigation related to patents on agent-based network monitoring, configuration and security systems.
 Services: Infringement analysis, validity analysis, source code review, report drafting.

Uniloc, Inc. v. Big Fish Games, Inc.

Case: Case # 2:16-cv-00741-JRG
 Description: Litigation related to patents on hardware cryptographic chips.
 Services: Non-infringement analysis, report drafting, source code review.

SPEX Technologies, Inc. v. Toshiba America Electronic Components, Inc., et al.

Case: Case # 8:16-cv-01800-JVS
 Description: Litigation related to patents on hardware cryptographic chips.
 Services: Non-infringement analysis, report drafting.

Symantec Corporation v. Zscaler, Inc.

Case: Case # 3:17-cv-04414-JST,
Description: Litigation related to patents on security gateways, URL filtering and categorization
Services: Infringement analysis, assignor estoppel, document review.

Koninklijke Philips v. Microsoft Inc.

Case: Case # 4:18-cv-01885-HSG,
Description: Litigation related to patents on secure cryptographic protocols
Services: Non-infringement analysis, validity analysis, claim construction analysis, document review, source code review.

Netfuel, Inc. v. Cisco Systems, Inc.

Case: Case # 5:18-cv-2352-EJD
Description: Litigation related to patents on agent-based network monitoring, configuration and security systems.
Services: Infringement analysis, claim construction analysis, source code review, report drafting.

Byrd et al. v. Aaron's, Inc., et al.

Case: PA Civil Action # 1:11-cv-00101-SJM-SPB
Description: Class action litigation related to privacy.
Services: Attend depositions, source code review, report drafting.

Finjan v. Juniper Networks

Case: Case # 3:17-cv-05659-WHA
Description: Litigation related to patents on malware scanning gateways.
Services: Invalidity analysis, non-infringement analysis, source code review.

Grace et al. v. Apple Inc.

Case: Case # 5:17-cv-00551-LHK (NC)
Description: Litigation related to device performance and service outages.
Services: Mobile forensics and device analysis, report drafting, source code review, document review, technical analysis and argument construction.

Rimini Street, Inc. v. Oracle International Corporation, et al.

Case: Case # 2:14-cv-01699 LRH-CWH
Description: Litigation related to false claims on security.
Services: Large-scale testing of IPS techniques for including custom test infrastructure and implementation of techniques to block exploitation of vulnerabilities, technical analysis of vulnerabilities.

Finjan v. Symantec Corporation

Case: Case # 14-cv-02998-HSG
Description: Litigation related to patents on malware scanning gateways, endpoint protection and firewalls.
Services: Build and/or test software for Windows, invalidity argument strategy, non-infringement argument strategy, report preparation, source code reviews.

Strikeforce, Inc. v. Entrust et al.

Case: Case # 1:17-cv-00309
Description: Litigation related to patents on authentication technologies.
Services: Invalidity argument development, non-infringement argument development, report drafting.

Sony Corporation, Inc. v. Arris

Case: Inv. # 337-TA-1049
 Description: Litigation related to patents on television streaming devices and/or services.
 Services: Validity argument development, source code review of entire platform codebase including numerous embedded platforms, infringement argument development.

Kudelski SA, Nagra USA, Inc., NagraVision SA, and OpenTV, Inc. v. Comcast Corporation

Case: Case # 2:16-cv-1362-JRG, Inv. # 337-TA-1049
 Description: Litigation related to patents on television streaming devices and/or services.
 Services: Validity argument development, source code review of entire platform codebase including numerous embedded platforms, infringement argument development.

Amazon.com Inc., Hulu, LLC, and Netflix, Inc. v. Uniloc Luxembourg S.A.

Case: IPR 2017-00948
 Description: Litigation related to patents on DRM protection for content distribution
 Services: Prior art search, PGR Preparation, IPR preparation.

PhishMe v. Wombat Technologies, Inc.

Case: Case # 16-403-LPS-CJB
 Description: Litigation related to patents on anti-phishing training technologies.
 Services: Prior art search, PGR Preparation, IPR preparation.

Nader Asghari-Kamrani and Kamran Asghari-Kamrani v. United States Automobile Association

Case: Case # 2:15-cv-478
 Description: Litigation related to patents on authentication technologies.
 Services: Prior art search, invalidity argument strategy, non-infringement argument strategy, source code reviews

Vir2us v. Invoicea Inc. and Invoicea Labs, LLC

Case: Case # Case 2:15-cv-00162-HCM-LRL
 Description: Litigation related to patents on virtualization and automated corruption repair.
 Services: Prior art search, invalidity argument strategy, non-infringement argument strategy, source code reviews

Palo Alto Networks v. Finjan

Case: IPR 2016-00159, IPR 2016-00151, IPR 2015-01974, IPR 2015-02001, IPR 2015-01979
 Description: Litigation related to patents on malware scanning gateways and firewalls,
 Services: Prior art search, patent interpretation, IPR preparation support, claim chart review

TVIIM v. McAfee

Case: Case # 3:13-cv-04545-VC
 Description: Litigation related to patents on vulnerability scanning
 Services: Build and test software for SPARC/Linux/Windows, patch out license checks/crack software (with permission), obtain hard-to-find legacy software, prior art and non-infringement argument strategy support, source code reviews, prior art search

Al Cioffi et al. v. Google

Case:	Case # 2:13-cv-103-JRG-RSP
Description:	Litigation related to patents on browser sandboxing and process isolation.
Services:	Code review/software testing to collect evidence of infringement, Infringement argument preparation support, claim chart review

Rovi Solutions & Veracode v. Appthority

Case:	Case # 12-10487-DPW
Description:	Litigation related to patents on static debugging tools
Services:	Source code review refuting opposing expert testimony

Analysis, Design and Development Clients

Arai	ICU Medical
Baxter	Inexto
Bigfoot Medical	Intuitive Surgical
BT Group	Merlin
Cardiac Sciences	Orpheus
Dyadic	Security First Corporation
Fresenius	Texas Instruments
HLFIP Holdings	Thesys
Hospira	Vaxxin

Pre-Harbor Labs Security Design and Software Development Experience

2013 *At Applied Communication Sciences*

Role:	Graduate Intern
Technologies:	JavaScript, Python, Tcpdump, Wireshark

- Developed extensible real-time traffic visualization tool to chart and analyze high-volume tcpdump streams of lossy metropolitan-area mesh network traffic.

2011 *At University of Michigan ICPSR*

Role:	Penetration Tester
Technologies:	Numerous Security Tools, Amazon EC2, VMware VSphere

- Conducted wide-scale penetration testing on virtualized cloud-based systems meant to be secure environments for researchers to store confidential results
- Created formal threat model document detailing potential security vulnerabilities from all possible attack vectors
- Wrote two reports detailing results from penetration test

2009-2011 *At Independent Security Evaluators*

Role:	Security Intern
Technologies:	C++, C#, Dalvik Bytecode, Gcov, GDB, Javascript, Peach Fuzzer, Python, RegEx, XML, Wireshark

- Created log parsing framework to analyze 20+ log file formats
- Assisted with malware testing, research and analysis
- Reverse engineered DRM schemes in Android and IOS applications
- Researched and prototyped secure cryptographic mail delivery system
- Developed web crawler to collect file sets for use in fuzzing
- Wrote code-coverage analysis tool for constructing minimum file set for fuzz testing
- Wrote fuzzing plugins using Peach Fuzzer framework and reverse engineered binary file

specifications

- Wrote Internet Explorer and Chrome extensions for cryptographic proxy system
- Created and debugged network protocols for use in network protocol testing
- Wrote and debugged unit tests in C++ and Python for proprietary disk-encryption system

2008-2010 *At Johns Hopkins University DRCC*

Role: Student Software Developer
Technologies: DOM, Java EE, JSP Perl, SAX, XSLT

- Drafted a report detailing security recommendations for an NSF funded data conservancy project
- Set up and deployed a Fedora digital repository with the Islandora frontend
- Ported IRStats statistics package to the DSpace information repository XMLUI
- Wrote batch importer that is now used to import more than 20 digitized books a week into DSpace repository

2008 *At Brandeis University Information Technology Services Hardware Repair Shop*

Role: Freelance Software Developer
Technologies: Java, Visual C++, VBScript

- Sole programmer on project to interface Request Tracker ticketing system with Brother PT- 9500PC Label Printer

Technical Skills

Languages	BASH, C, C++, C#, HTML, Java, JavaScript, Objective-C, Python, Perl, PHP, Regular Expressions, SQL, XML
Architectures	6502, 8051, 8080, ARM Cortex-M, ARMv7, ARMv8, AVR, m68k, MIPS, MSP430, PIC, SPARC, PowerPC, x86, x86-64, Z80
Operating Systems	Android, ChromeOS, FreeBSD, iOS, OpenBSD, Linux, macOS, Windows
DevOps and Development Tools	Ansible, Ant, BitBucket, Confluence, Docker, gdb, git, GitHub, GitLab, Gradle, Hadoop, jad, jd-gui, Jira, Maven, make, MySQL, PostgreSQL, subversion, Trello, Vagrant, valgrind
Security Tools	Aircrack-ng, apktool, binwalk, bulk-extractor, Burp suite, Charles Proxy, curl, dex2jar, ftk, hashcat, IDA Pro, Metasploit, mitmproxy, Nessus, nmap, OpenSSL, ophcrack, p0f, Scalpel, skipfish, snort, sslstrip, sslyze, Volatility, Web Scarab, wget, Wireshark
Cloud and Virtualization	AWS, Azure, Bhyve, KVM, LXD, QEMU, virt-manager, VMware, Xhyve

Honors, Societies and Awards

- Member Upsilon Pi Epsilon International Computer Science Honor Society
- Member Institute for Electrical and Electronics Engineers (#97507890)
- Member Association for Computing Machinery (#9700346)

At Johns Hopkins University

- Computer Science Department Outstanding Teaching Assistant Award (2014)
- Treasurer, Upsilon Pi Epsilon International Computer Science Honor Society (JHU Chapter)
- Computer Science Department Faculty Liaison Czar
- Student Representative to the Computer Science Undergraduate Curriculum Planning Curriculum

Committee

Certifications

- Six Sigma Black Belt
- Six Sigma Green Belt