

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE, INC.,
Patent Owner.

Case IPR2023-00821
Patent 10,699,008

DECLARATION OF SETH JAMES NIELSON, PH.D.

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BASES FOR OPINIONS	1
III.	MATERIALS REVIEWED.....	2
IV.	EDUCATION AND EXPERIENCE.....	2
A.	Overview	3
V.	LEGAL STANDARDS.....	11
A.	Burden of Proof	11
B.	Anticipation and Obviousness.....	12
1.	Anticipation.....	12
2.	Obviousness.....	13
C.	Independent Claims and Dependent Claims	16
D.	Claim Construction.....	17
VI.	LEVEL OF ORDINARY SKILL IN THE ART	18
VII.	BACKGROUND	20
A.	Priority Date of the ‘008 Patent.....	20
B.	Overview of the ‘008 Patent.....	20
C.	File History of the ‘008 Patent	25
VIII.	SUMMARY OF REFERENCES	28
A.	U.S. Patent No. 9,602,529 (“Jones”) (EX-1004)	28
B.	U.S. Patent No. 10,503,907 (“Zheng”) (EX-1005)	30
C.	U.S. Patent No. 11,200,228 (“Keenan”) (EX-1006)	30

D.	U.S. Patent No. 9,948,652 (“Yu”) (EX-1007)	31
E.	U.S. Patent No. 10,216,938 (“Reith”) (EX-1008).....	31
IX.	CLAIM CONSTRUCTION.....	32
A.	“Redefine the First Threat Model by Including In It a Second Threat Model Associated with the Component Group”	32
B.	“Threat Model Components”	36
C.	Applicability of Ex Parte Schulhauser	37
X.	SUMMARY OF OPINIONS.....	38
XI.	OPINIONS CONCERNING THE CHALLENGED CLAIMS	39
A.	Ground 1: Jones Does Not Anticipate Claims 1 and 3.....	39
1.	Jones Does Not Disclose Adding a Component Group to a First Threat Model.....	39
2.	Jones Does Not Disclose “Display[ing] a Relational Diagram ... Using ... Visual Representations of One or More of the Compensating Controls” as Required by Element 1[e]	44
3.	Jones Does Not Teach or Suggest Claim 3	46
B.	Ground 2: Alleged Obviousness of Claims 1-20 Over Jones, Zheng, and Keenan.....	48
1.	Dependent Claim 2.....	48
2.	Independent Claim 4	52
3.	Dependent Claims 6 and 7	53
4.	Dependent Claim 8.....	55
5.	Dependent Claim 9.....	56
6.	Dependent Claim 10.....	56

7.	Dependent Claim 11.....	58
8.	Independent Claim 12	58
9.	Dependent Claim 13.....	59
10.	Dependent Claim 14.....	59
11.	Dependent Claim 15.....	59
12.	Dependent Claim 16.....	60
13.	Dependent Claim 17.....	60
14.	Dependent Claim 19.....	60
C.	Ground 3: Alleged Obviousness of Claims 1-20 Based on Jones, Zheng, Keenan, and Yu.....	62
D.	Ground 4: Alleged Obviousness of Claims 1-20 Based on Jones, Zheng, Keenan, Yu, and Reith	63
E.	Ground 5: Alleged Obviousness of Claims 5-8 and 13-15 Based on the References of Ground 4 and the Knowledge of a POSITA	66
XII.	CONCLUSION	67
XIII.	AVAILABILITY FOR CROSS-EXAMINATION	67
XIV.	RIGHT TO SUPPLEMENT.....	67
XV.	DECLARATION	68

Case IPR2023-00821

Patent 10,699,008

Declaration of Seth James Nielson, Ph.D.

EXHIBITS

Exhibit No.	Description
EX-2001	Patent Owner's December 4, 2023 Power of Attorney
EX-2002	Transcript of Robert Hurlbut Deposition taken February 5, 2024
EX-2003	Declaration of Seth James Nielson, Ph.D.

I. INTRODUCTION

1. I am Seth James Nielson, Ph.D. I am over 18 years of age. I hereby declare as follows:

2. I have personal knowledge of all of the matters about which I testify in this declaration.¹

3. Rimon P.C. retained me on behalf of ThreatModeler Software, Inc. (“ThreatModeler”) to provide my technical opinions and testimony about the petition for *inter partes* review (“Petition”) filed by IriusRisk, Inc. (“IriusRisk”) against claims 1-20 of U.S. Patent No. 10,699,008 (“the ‘008 Patent”). I refer to those claims as the “challenged claims.” The full text of the challenged claims appears in **Appendix A** to my declaration.

4. For my work in this matter, I am being compensated at my usual consulting rate of \$700/hour, and I am receiving reimbursement for expenses incurred in the course of my work. My compensation is not contingent in any way on either the opinions I have reached or the outcome of this proceeding.

II. BASES FOR OPINIONS

5. I have reviewed and considered the documents and other materials listed below in **Section III** in light of my specialized knowledge provided by my

¹ All emphases in quotations in this declaration are added unless otherwise specified.

education, training, research, and experience, as summarized in **Section IV** and described in detail in my CV, which is provided as Appendix C. My analysis of those materials, combined with the specialized knowledge that I have obtained over the course of my education and career, form the bases for my opinions in this declaration.

III. MATERIALS REVIEWED

6. I have reviewed and analyzed the parties' papers and exhibits in this proceeding, including the '008 Patent (EX-1001) and its prosecution history (EX-1002), IriusRisk's petition (Paper 1) and its associated exhibits, including U.S. Patent No. 9,602,529 ("Jones") (EX-1004), U.S. Patent No. 10,503,907 ("Zheng") (EX-1005), U.S. Patent No. 11,200,228 ("Keenan") (EX-1006), U.S. Patent No. 9,948,652 ("Yu") (EX-1007), U.S. Patent No. 10,216,938 ("Reith") (EX-1008); ThreatModeler's preliminary response (Paper 6); the Board's institution decision (Paper 7); and the transcript of Mr. Robert Hurlbut's February 5, 2024 deposition (EX-2002), including the associated exhibits. I have also reviewed and analyzed the exhibits and documents cited in this declaration. Attached as **Appendix B** is a complete list of the documents I have reviewed in preparing this report.

IV. EDUCATION AND EXPERIENCE

7. Below is a summary of my education and experience. My CV,

attached as **Appendix C**, records my education, experience, and publications in greater detail.

A. Overview

8. I am the Founder and Chief Scientist of Crimson Vista, a computer security research and engineering company. Furthermore, I hold appointments at the University of Texas at Austin as an Adjunct Associate Professor in the department of Computer Science and as a Cybersecurity Fellow in the Robert Strauss Center for International Security and Law. The following paragraphs summarize my professional experience.

9. I hold a Ph.D. in Computer Science from Rice University, awarded in 2009. I also received B.S. and M.S. degrees in Computer Science from Brigham Young University in 2000 and 2004 respectively. In addition to my academic degrees, I hold a CISSP certification.

10. In terms of industry practice, I worked professionally in various engineering positions from 2000 to 2011. Employers and clients include Microsoft, Google, Metrowerks, and various smaller entities. The engineering projects included testing systems, software development kits, engineering applications, networking components, security systems, file systems, cryptography components, web components, package management, and virtual-machine-based

infrastructure. I also worked with software development infrastructure such as testing systems, source code repositories, code reviews, network security components, remote access systems, virtual private networks, routing, firewalls, webmail components, web servers, embedded devices, embedded deployment, and cross-architecture toolchains. Throughout my engineering years I wrote hundreds of thousands of lines of computer code in C++, C, Python, Perl, Java, and other languages.

11. I have provided consulting services in a wide range of computer science areas from 2009 to the present. The clients of these services have included companies of all sizes including Fortune 50 entities, Tier-1 banks, security companies, medical companies, heavy industry, insurance companies, software companies, and start-ups. I was also invited to provide some analysis for United States Department of Justice in an antitrust investigation.

12. Forensic source code review is a common services I have provided as a consultant. I have analyzed an extensive collection of commercial software, including software related to secure email, cloud-based multimedia delivery, document signing, anti-virus and anti-intrusion, high-performance routing, networking protocol stacks in mobile devices, PBX telecommunications software, VoIP, high-frequency trading, e-commerce, antivirus, cloud systems, digital radios,

mobile devices, video games, industrial controls, deep learning systems, medical software, and peer-to-peer communications.

13. I have also guided companies on matters related to security and privacy, including adequately protecting personal data during data acquisition, data storage, and data usage based on threat assessments and risk analysis. In other engagements, I have evaluated devices, including medical devices, for security vulnerabilities, flaws, and the associated threats. I also analyzed security considerations for potential technology acquisitions. In addition to these kinds of evaluations, I have provided VCISO services to companies that need help getting their security programs off the ground and in accordance with NIST recommendations for risk analysis and threat assessment. In another engagement, I provided guidance to a start-up on matters related to Blockchain, smart contracts, and distributed ledgers.

14. Additional forensic services I have provided include analyses to help companies figure out what has gone wrong with a data breach or other security incident. This includes forensic analysis of how the intrusion happened, the impact, and any necessary remediation. Forensic investigations include analysis of networking components, identification of intrusion vectors (e.g., via email, server breach, unauthorized VPN access, etc.), and review of data from monitoring

systems such as logging systems, SIEMs, and IDS/IPS components.

15. In yet another example of forensic expertise, I am often retained for my expertise in software forensics and have been instrumental in multiple cases to discovering and identifying stolen source code or misappropriated trade secrets. I have also provided testimony on forensics related to electronic document modification.

16. I also have presented training sessions at multiple conferences on topics related to data security, data privacy, protecting intellectual property, Blockchain basics, and improving a company's security posture based on risk analysis and threat modelling.

17. In addition to work for clients, I also contribute to industry research. I was the primary investigator on a DOD-funded research project for protecting systems from Ransomware threats. I also am a named contributor on another research grant held by another company on developing insider-resistant systems and secure enclaves for government networks that are designed to counter insider threats for high-risk environments.

18. I am also the co-founder and current director of the Crypto Done Right project. This project was originally hosted by Johns Hopkins University and funded by a grant from Cisco. However, I have transitioned the project into a

completely independent non-profit entity and I am one of the founding directors.

Crypto Done Right is designed to bridge the gap between cryptography SME's and the IT professionals that use it.

19. Beyond my professional work and professional research, I also have contributed professionally in academia to both teaching and research.

20. During the 2014-2019 time period I taught the Network Security and Advanced Network Security courses at the Johns Hopkins University. I developed my own curriculum focused on threat identification and modelling, risk analysis, mobile code, cryptography, autonomous agents, intrusion analysis, and education psychology. I published a paper related to my curriculum in the Journal of Computer Science Education entitled, "PLAYGROUND: Preparing Students for the Cyber Battleground."

21. From 2016-2019, I was the Director of Advanced Research Projects at the Johns Hopkins University Information Security Institute (JHUI SI). During this time, I published "Potential Forensic Analysis of IoT Data: An Overview of the State-of-the-Art and Future Possibilities" in the 2017 IEEE International Conference on Internet of Things (iThings). I also published a paper related to threats against industrial systems entitled, "Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices" in

2018 IEEE International Symposium on Technologies for Homeland Security (HST).

22. In addition to published research, I mentored capstone projects related to IDS/IPS threat detection, intrusion detection, cryptography threats, drone threats, iOS threats, BitCoin, SSL vulnerabilities and associated threats, and Twitter “botnets.” Many of these projects involved industry collaboration. For example, we coordinated with the company OnBoard Security to develop better security for anti-collision protocols for air traffic after identifying practical threats against them.

23. I also gave a talk on “Detecting Malicious Sandboxes” at the Workshop on Defensive Deception and Trust in Autonomy, in association with the 2018 Naval Applications of Machine Learning Workshop.

24. From 2020 to the present, I have held the position of adjunct professor at the University of Texas at Austin. I have taught the undergraduate Network Security and Privacy class in the Computer Science department. I also teach the Introduction to Cybersecurity Technology class in the Law School. I have also mentored independent study courses for Computer Science students on topics of computer security and artificial intelligence.

25. I am also the author of two books. The first is entitled “Cryptography

in Python: Learning Correct Cryptography by Example” and covers the practical implementation of a wide range of cryptography algorithms. The second book, entitled, “Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner” provides a technical overview of cybersecurity basics, including threat modeling and risk management, for readers with no background in engineering or computer science.

26. My qualifications also include education and professional experience with threat modeling and cybersecurity risk management. The importance of threat models and basic examples of threat modeling are typical topics for courses in cybersecurity. For example, my first graduate class in computer security in 2004 used as the textbook “Security Engineering” by Ross Anderson (1st edition). This edition of the book is freely available online from Ross Anderson’s website (<https://www.cl.cam.ac.uk/~rja14/book.html>). Anderson explains that threat models are fundamental to cybersecurity: “Where a top-down approach to security engineering is possible, it will typically take the form of threat model—security policy—security mechanisms.” (Security Engineering, 1st Edition, p. 138). He goes on to say, “In a top-down approach to security engineering, one should first determine the threat model, then write the policy, and finally test the policy by observing whether it works in real life.” (*Id.* p. 171). Throughout the text, the

importance of the threat model to cybersecurity is repeated and analyzed.

27. Chapter 22 of the first edition also includes an example of concrete threat modeling techniques. For example, one such technique known as “threat trees” at pages 500-501. I have reproduced an illustration from this chapter hereinbelow:

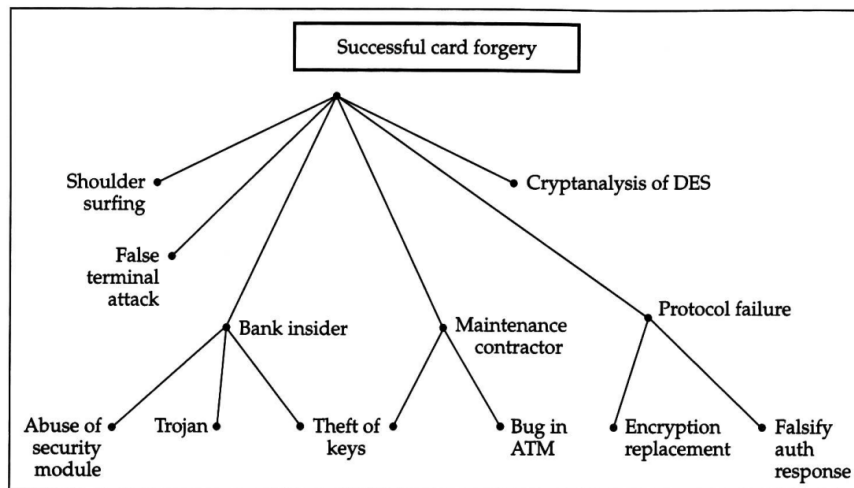


Figure 22.4 A threat tree.

28. I subsequently taught courses in Network Security at the undergraduate and graduate levels at the Johns Hopkins University from 2014-2019. I used later editions of Ross Anderson’s book as my text and specifically instructed my students on threat models and techniques such as threat trees.

29. Moreover, in my work as a professional cybersecurity engineer, I worked with my clients to develop threat models. I also used the threat tree analysis as one of the approaches in creating the model. This included threat

models for a medical device manufacturer. I have also used frameworks such as NIST SP800-154 (“Guide to Data-Centric System Threat Modeling”, <https://csrc.nist.gov/pubs/sp/800/154/ipd>) in my work with clients.

30. Similarly, I have also taught and also consulted on the topic of cybersecurity risk management. On these topics, I also use various guidelines and recommendations including those from NIST. A list of relevant NIST publications related to risk management can be found here: <https://csrc.nist.gov/projects/risk-management/publications>. These are publications I have used in consulting with clients about cybersecurity risk.

V. LEGAL STANDARDS

31. My understanding of the legal standards is stated below. I am not an attorney and have no formal training in the law concerning patents, but I have used my understanding of the legal principles, as set forth below, in reaching my opinions.

A. Burden of Proof

32. I understand that in this proceeding, IriusRisk has the burden of proving that the challenged claims are unpatentable by a “preponderance of the evidence.” I understand “preponderance of the evidence” to mean evidence sufficient to show that a fact is more likely true than not true.

B. Anticipation and Obviousness

33. I understand that for a patent claim to be patentable and valid it must be, among other things, new and not obvious in light of knowledge that was publicly available before the invention. I understand that knowledge that was publicly available before the claimed invention is generally referred to as “prior art.”

34. I understand that whether a patent claim is new and not obvious is judged from the perspective of a “person of ordinary skill in the art.” I understand that a person of ordinary skill in the art is presumed to know all prior art and is a hypothetical person of ordinary creativity who can use common sense to solve problems. I describe a person of ordinary skill in the art in greater detail in **Section VI** below.

1. Anticipation

35. I understand that a prior art reference that demonstrates a patent claim is not new is said to “anticipate” that claim. I understand that to anticipate a claim of a patent, a single prior art reference must disclose, either expressly or inherently, each “limitation” (or “element”) of that claim combined in the same way as recited in the claim. I understand further that even if a prior art reference does not expressly spell out all of the limitations arranged or combined as in the claim, it

can still anticipate if a person of ordinary skill in the art, reading the reference, would at once envisage the claimed arrangement or combination.

36. I understand that a limitation is disclosed inherently in a reference only if it is necessarily present in the process or product described in the prior art reference. That is, I understand that probabilities or possibilities are insufficient to show that a prior art reference inherently discloses something beyond what it discloses explicitly. However, I understand further that it is not required that a person of ordinary skill in the art recognize or appreciate the inherent feature at the time the prior art was first known or used.

37. I understand that for a reference to anticipate a claim, the reference must be complete enough to enable a person of ordinary skill in the art to carry out the claimed invention.

2. Obviousness

38. I understand that a claim is invalid for “obviousness” if the differences between the claim and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person of ordinary skill in the art to which the subject matter pertains at the time of the invention. I understand that obviousness is a question of law based on underlying factual issues. Those factual issues are: (1) the scope and content of the prior art;

(2) differences between the prior art and the inventions of the claims at issue; (3) the level of ordinary skill in the art at the time the invention was made; and (4) whether objective factors indicating obviousness or non-obviousness are present.

39. I understand that such objective factors, sometimes referred to as “objective indicia,” may include: (a) commercial success of products covered by the patent claims; (b) a long-felt, but unmet, need for the invention; (c) skepticism by others in the field; (d) failed attempts by others to make the invention or solve the problem solved by the invention; (e) copying of the invention by others working in the field; (f) unexpected results achieved by the invention; and (g) the fact that the patentee proceeded contrary to the accepted wisdom of the prior art. For the objective factors to be relevant, I understand that the evidence relating to these factors must have a connection or causal “nexus” to the subject matter as claimed.

40. I understand that a claim is not invalid for obviousness unless every limitation of the claim would have been obvious to a person of ordinary skill in the art (or anticipated) at the time of the invention.

41. I understand that a claim is not obvious merely because each claim element was known in the prior art. I also understand that, in assessing obviousness, I should consider whether a reason existed that would have prompted

a person of ordinary skill in the art to combine the prior art elements in the way they are combined in the patent claim. I understand an expansive and flexible approach should be applied to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.

42. I understand that an obviousness case based on modifying or combining one or more prior art references also requires the petitioner to show that a person of ordinary skill in the art would have had a reasonable expectation of successfully achieving the claimed invention.

43. I understand that example reasons to combine or modify prior art references that may support a conclusion of obviousness include combining prior art elements according to known methods to yield predictable results; simple substitution of one known element for another to obtain predictable results; use of a known technique to improve similar techniques; combining elements in a way that would be ‘obvious to try’ where there exists a finite number of identified, predictable solutions and a reasonable expectation of success; design incentives or market forces that would prompt variations of known work if those variations were predictable to a person of ordinary skill in the art; a teaching, suggestion, or motivation in the prior art to combine or modify prior art references to arrive at the

claimed subject matter; and optimization of a variable which achieves a recognized result by a person of ordinary skill in the art if that optimization would be routine.

44. I understand that there are also reasons that would prevent a person of ordinary skill in the art from modifying or combining prior art references. Examples of prior art references that a person of ordinary skill in the art would not combine or modify to achieve the claimed invention include prior art references that “teach away” (discourage or lead away) from one another or from the claimed invention; prior art references whose combinations or modification would change the principle of operation of either prior art reference; prior art references whose combination or modification would render them inoperable or unsuitable for their intended purpose; and prior art references whose combination or modification would destroy a key objective of that prior art reference.

45. I understand that in determining whether a person of ordinary skill in the art would combine or modify prior art references, the entire contents of each prior art reference must be considered, including parts of those references that would suggest against the proposed combination or modification.

C. Independent Claims and Dependent Claims

46. I understand that patents have two types of claims: “independent claims,” which do not refer to other claims in a patent, and “dependent claims,”

which refer to at least one other claim in a patent. I understand that a dependent claim incorporates every limitation of the claim or claims to which it refers, or “depends.” Thus, if a claim is not anticipated, then any claim that depends from that claim is not anticipated either. And if a claim is not obvious, then any claim that depends from that claim is not obvious either.

D. Claim Construction

47. I understand that the language of claims is interpreted, or “construed,” in accordance with the plain and ordinary meaning of such claims as understood by one of ordinary skill in the art in light of the patent’s specification and prosecution history of the patent. I understand that when a patent explicitly defines language used in the claims, that definition applies to the claims even if it varies from the plain and ordinary meaning of the language.

48. I understand that “intrinsic evidence” is the primary means by which claim terms are interpreted. Intrinsic evidence includes the claims themselves; the specification of the patent in which the claims appear; and the prosecution history of the patent.

49. I understand that, during the prosecution history of the patent, an applicant for a patent may state that the claims do not cover a particular feature or embodiment, and that such statement, a “prosecution history disclaimer,” by an

applicant may limit the scope of the claim language. However, I also understand that proving a disclaimer requires a showing of clear intent by the applicant to redefine the claim language in order to overcome prior art, on the basis of a specific claim element. Further, it is my understanding that a general description of the invention is not sufficient to limit the claim language.

50. I understand that a claim term should not be given a meaning that renders portions of the claim language meaningless or superfluous.

51. I understand that “extrinsic evidence,” such as expert and inventor testimony, dictionaries, and learned treatises, can also inform the meaning of a claim term. However, extrinsic evidence is less significant than the intrinsic evidence in determining the meaning of a claim term. Further, I understand that extrinsic evidence cannot be used to vary, contradict, expand, or limit the claim language from how it is defined, even by implication, in the specification or file history.

VI. LEVEL OF ORDINARY SKILL IN THE ART

52. I understand that it is necessary to analyze both a patent’s claims and the prior art from the perspective of a hypothetical “person of ordinary skill in the art” at the time of the patent’s invention.

53. I understand that several factors are considered in determining the level of ordinary skill in the art, including the educational level of active workers in the field, the types of problems encountered in the art, the nature of prior art solutions to those problems, prior art patents and publications, the activities of others, the sophistication of the technology involved, and the rapidity of innovations in the field.

54. I understand that, solely for purposes of this IPR, Patent Owner does not contest Petitioner's proposed definition of a person of ordinary skill in the art. Consequently, I have applied Petitioner's proposed level of ordinary skill in the art in rendering my opinions in this Declaration. Based on that level of ordinary skill in the art, I had sufficient education and experience to qualify as a person of ordinary skill in the art as of May 17, 2017 and am also familiar with the knowledge of a person of ordinary skill in the art as of that time based upon my interactions with others in the field. Accordingly, my analysis in this case is based on the perspective of a person of ordinary skill in the art as of May 17, 2017.

55. Throughout the remainder of this Declaration, I will refer to a person of ordinary skill in the art as a "POSITA."

VII. BACKGROUND

A. Priority Date of the ‘008 Patent

56. U.S. Patent Application No. 16/228,738 (“the ‘738 Application”) was filed on December 20, 2018. The ‘738 Application issued as the ‘008 patent on June 30, 2020. The ‘738 Application claims priority to four U.S. Provisional Applications, the earliest of which was filed on May 17, 2017.

57. I understand that IriusRisk’s petition for *inter partes* review and Mr. Hurlbut’s expert opinions are based on the May 17, 2017 priority date. (Petition, 8; EX-1003 ¶ 47). Accordingly, my opinions contained within this declaration are also based on the perspective of a POSITA as of May 17, 2017.

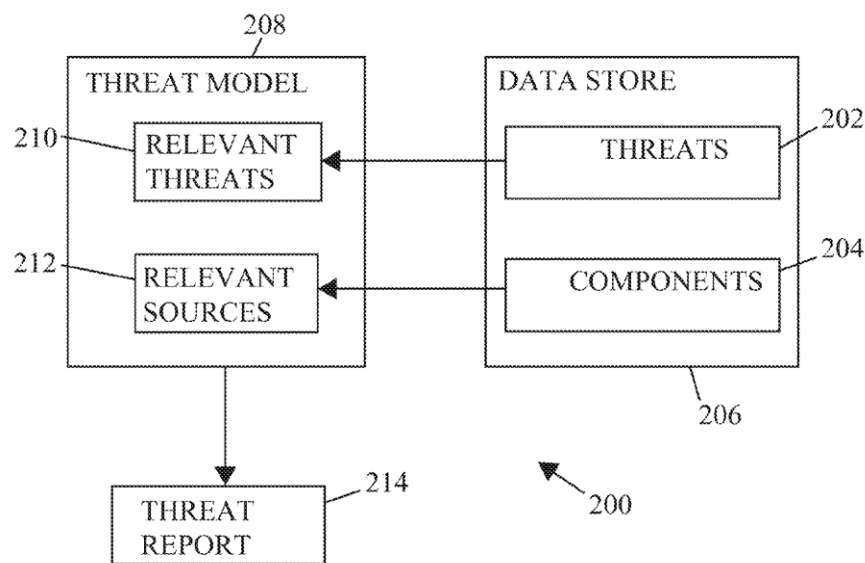
B. Overview of the ‘008 Patent

58. The ‘008 Patent is entitled “Threat Model Chaining and Attack Simulation Systems and Related Methods” and relates to threat modeling systems and processes. EX-1001, cover page. The ‘008 Patent explains that “[t]hreat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized.” EX-1001, 1:48-49.

59. Threat modeling can be applied to a broad range of environments or activities. EX-1001, 1:54-58. “With regards to modeling computing networks, traditional threat modeling systems and methods exist for assessing risk from potential cyber threats at an individual application level without fully accounting

for application-application interactions, thereby miscalculating organizational risk.” EX-1001, 1:62-66.

60. Figure 2 of the ‘008 Patent is one example of a threat modeling process of the invention that is applicable to any application, process, or system under consideration. EX-1001, 8:38-41.



61. The ‘008 Patent explains that threat models are created from defined threats and threat model components, which are stored within a database. *Id.*, 8:50-56 (“As illustrated in FIG. 2, process 200 may include storing a plurality of threats 202 and threat model components (components) 204 in a data store 206. This may include, by non-limiting example, storing titles, definitions or descriptions, and/or associated images in the database 108 for each component and/or threat. The threats and components are used to create threat model 208.”). The “database

allows for the correlation of any threat to any number of components and likewise, the correlation of any component to any number of threats.” ’008 Pat., 9:48-52.

“[E]ach asset could have any number of threats that could threaten to compromise it. ... Some assets may be threatened by only a single threat, some may be threatened by two or three threats, or more, and so forth.” ’008 Pat., 24:4-10.

62. Referring to Figure 2, a user selects from among the available components those components which are relevant to any given system, process or application being examined. This process is represented by the arrow between the components 204 and the relevant sources 212. The relevant sources are the sources determined by the system that are involved in the specific application, system or process and defining relationships between and among the relevant components. The system also retrieves from the database where the threats and components are stored, the threats that were previously correlated with the components to thereby form the threat model 208. The threat model includes the relevant threats and the relevant sources of those threats related in a manner that corresponds to the architecture of the system being modeled. The threat model can be used to generate a threat report 214.

63. The ‘008 Patent describes each “threat model component” as “a potential relevant source for one or more threats.” EX-1001, 9:28-30. One

example provided in the specification is that one threat may be “Bluejacking,” in which a potential attacker may seek to gain improper access to a system via its Bluetooth interface. In this example, the threat model component is the “Bluetooth port,” *i.e.*, the potential source of the threat. EX-1001, 9:28-32. As another example, an “online banking interface” may be stored as a threat model “component,” and “a threat may be a virus being introduced to the bank’s environment through a breach in the banking interface.” ’008 Pat., 24:42-52.

64. Similar to the described embodiments above, the challenged claims of the ’008 Patent recite a “database,” and in claim 1, the database comprises, in relevant part, “a plurality of threat model components stored therein; a plurality of threats stored therein, each threat associated with at least one of the threat model components through the one or more databases; and a plurality of compensating controls stored therein, each compensating control associated with at least one of the threats through the one or more databases.” Independent claims 4 and 12 include substantially similar features. As claimed, the “database” does not simply store a numeric value as a property or characteristic of a component. Rather, as claimed, the one or more databases expressly stores “a plurality of threats,” and associates each of the threats with “at least one of the threat model components through the one or more databases.”

65. The independent claims of the ‘008 Patent recite at least two inventive features. Independent claim 1 of the ‘008 patent recites that the diagram interface is configured to “add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.” ‘008 Patent, 35:56-63. Independent claims 4 and 12 of the ‘008 Patent recite that, in response to a user selection of one of the diagramed threat model components, the diagram interface is configured to “visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.” ‘008 Patent, 36:36-42, 37:44-38:3.

66. The ‘008 Patent explains that a group of threat model components can be diagrammed separately as an independent threat model and then saved as a component so that it can be imported into another threat model. EX-1001, 20:23-26. That newly created “component” can be saved, for example, in a toolbox menu as a single item. EX-1001, 20:37-39. For example, a user could define a “Windows 7” component group. EX-1001, 20:39-41. That group may include, for example, a file system, PDF client, Skype, Outlook 2010, McAfee HIPS, McAfee AV VSE, Internet Explorer 11, Office 2010 and other components. EX-1001,

19:52-56. Once created and stored, a user could add the Windows 7 component to another threat model thereby importing into the threat model the threats associated with the Windows 7 threat model. EX-1001, 20:41-45. When a user adds a component group to an existing threat model, the threat model of the component group is added to (or “nested” within) the existing threat model. EX-1001, 20:26-30. In this way, a user can modify a threat model by incorporating previously defined threat models for the component groups. EX-1001, 20:30-32. The ‘008 Patent also refers to this as “threat model chaining.” EX-1001, 20:32-33.

67. The second inventive aspect of the independent claims relates to displaying attack paths. The ‘008 Patent explains that a user can select a particular one of the threat model components (*e.g.*, an asset) and the system will display all attack paths (or what the ‘008 Patent also refers to as “attack vectors”) associated with the threats which may compromise the asset. EX-1001, 23:13-16. Displaying all attack paths allows a user to determine what compensating controls may be included to protect the asset. EX-1001, 23:16-18. The user can add or remove compensating controls (or toggle compensating controls on or off) to see the effectiveness of the compensating controls. EX-1001, 23:18-26.

C. File History of the ‘008 Patent

68. I understand that the ‘008 Patent was filed as U.S. Patent Application

No. 16/228,738 (“the ‘738 application”) on December 20, 2018. EX-1002, p.358.

69. Based on the file history, I understand that the Examiner issued an office action on August 8, 2019 rejecting all pending claims based on judicially created double patenting and as being directed to nonpatentable subject matter. EX-1002, pp.392-401. On October 25, 2019, the applicant filed a response to the August 8, 2019 office action arguing against the non-patentable subject matter rejection and indicating that a terminal disclaimer would be filed to overcome the double patenting rejection. EX-1002, pp.427-454. Applicant filed the terminal disclaimer on the same day. EX-1002, pp.456-457. On November 20, 2019, the Examiner issued a second office action in which the Examiner withdrew the non-patentable subject matter rejection but maintained the double patenting rejection. EX-1002, pp.461-470. Counsel for applicant called the Examiner to advise that the applicant had already filed the required terminal disclaimer. The Examiner called back to say that a notice of allowance would be issued. EX-1002, p.492. The Examiner issued the Notice of Allowance on February 24, 2020. EX-1002, p.523.

70. I further understand that the ‘008 Patent issued on June 30, 2020 after, in relation to claims 1 and 4, the Examiner found that the cited prior art did not disclose or teach “*configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual*

representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model, and configuring the diagram interface to, in response to receiving one or more inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.” EX-1002, p.528. The Examiner found that claim 12 was substantially similar to claims 1 and 4 as it relates to the reason for allowance and therefore allowed claim 4 and all dependent claims on that basis. *Id.*

71. According to the file history, on March 2, 2020, the applicant commented on the Examiner’s reasons for allowance by stating that the applicant believed that each claim was patentable in its own right, for other reasons raised during prosecution, or as explained in the patent’s specification. EX-1002, p.557. The ‘008 Patent issued on June 30, 2020. On July 6, 2020, the applicant’s counsel filed a certificate of correction request. EX-1002, pp.584-585. The Patent Office issued two certificates of correction – one issued on October 5, 2020 correcting the specification (EX-1002, p.623) and the second issued on December 8, 2020 correcting the drawings (EX1002, pp.629-632).

VIII. SUMMARY OF REFERENCES

72. I understand that Petitioner requests review of the ‘008 Patent on the following grounds:

Ground	Claims	Statutory Basis	Alleged Prior Art
1	1, 3	§102	Jones
2	1-20	§103	Jones, Zheng, and Keenan
3	1-20	§103	The references of Ground 2 and Yu
4	1-20	§103	The references of Ground 3 and Reith
5	5-8 and 13-15	§103	The references of Ground 4 and the knowledge of a POSITA

Petition, 11; EX-1003, ¶20.

A. U.S. Patent No. 9,602,529 (“Jones”) (EX-1004)

73. Jones discloses a system for modeling threats in “information systems.” EX-1004, Abstract. In relevant part, Jones’ information systems may include components such as hosts, processes, data stores and/or external entities, and data flows between those components. EX-1004, 5:4-6. The information system may be described as having a “hierarchical breakdown” or “hierarchy” of its components at different levels. EX-1004, 5:10-14. The information system may have multiple “nested” components, one or more of which may further have

its own additional “nested” components at lower levels of the hierarchy. EX-1004, 5:14-19. In other words, the components of Jones’ information system may have components that have subcomponents, and some of the subcomponents may have their own subcomponents, etc. By moving from one layer of the hierarchy to another allows a user to examine threats at different “levels” of the information system. EX-1004, 5:4-19.

74. Jones explains that if it is desired to look at the components of the information system in greater detail so as to examine their specific security threats, the decomposer 110 is used to “decompose” the components of the information system modeled by the data flow diagram (“DFD”) into their “nested” subcomponents and the data flows between those subcomponents. EX-1004, 6:12-18. The “nested” subcomponents were already present in the information system and the threat model created by Jones’ system for analyzing the information system. *See* EX-2002, 71:9-72:3, *see also* 51:25-52:22, 53:4-10, 70:6-23, 116:15-117:7. But the nested subcomponents were not visible at level “n” of the hierarchy, for example. Those subcomponents may become visible when the threat model components are “decomposed” into their level “n+1” subcomponents. *See* EX-2002, 71:9-72:3, *see also* 51:25-52:22, 53:4-10, 70:6-23, 116:15-117:7. The threats associated with the subcomponents and their threat modeling are included

in the threat model for the component itself. *See* EX-2002, 54:4-14.

B. U.S. Patent No. 10,503,907 (“Zheng”) (EX-1005)

75. Zheng is directed to a system for visualizing and analyzing security threats in a suite of software applications. EX-1005, Abstract. Zheng’s system includes multiple layers for visualizing different information available from the system. The system includes a base layer includes components representative of the software applications and relationships among the software applications. EX-1005, 1:46-52. The system includes a threat modeling module configured to identify security threats I the suite of software applications. EX-1005, 1:53-59. The system also includes a security controls module for implementing security controls to mitigate threats, and a threat update module for assessing the current state of security on a visually displayed map. EX-1005, 1:59-67. Zheng’s system also includes a data flow module to facilitate display of simulated data flow through the components of the map. EX-1005, 2:19-25. Zheng defines a “security threat” as a threat actor, a threat target, and a displayable vector connecting the threat actor to the threat target. EX-01005, 2:36-39.

C. U.S. Patent No. 11,200,228 (“Keenan”) (EX-1006)

76. Keenan relates to risk management – not threat modeling. Keenan was filed by and assigned to an insurance company: American International

Group, Inc. Keenan assigns a risk value to certain aspects of a system, but the threats underlying that risk value are neither determined by Keenan nor important to Keenan. The purpose of Keenan is to provide a view that allows a user to see (via a “view”) an overall risk level associated with an infrastructure for business and insurance purposes, not to detail or prioritize vulnerabilities or threats.

Keenan, 1:33-38. Keenan teaches that different “views” can display colors according to different properties, including the risk level, associated with various objects.

D. U.S. Patent No. 9,948,652 (“Yu”) (EX-1007)

77. Yu is directed to systems and methods for identifying threat vectors and implanting controls for security resources within a network. Yu determines threat vectors associated with the resources, and determines controls associated with the threat vectors. EX-1007, Abstract.

E. U.S. Patent No. 10,216,938 (“Reith”) (EX-1008)

78. Rieth discloses a system in which a “threat matrix” may include multiple “threat landscapes.” Each threat landscape may include one or more “recombinant” threat models. EX-1008, 4:30-32. Each threat model may stand on its own within the threat landscape or it may be connected to other threat models. EX-1008, 4:32-35. A threat matrix represents all of the threats faced by an

enterprise, government, or an organization in general. EX-1008, 4:41-44.

79. The threat matrix may be comprised of recombinant threat models which would allow for the cross-correlation of information from different threat models. EX-1008, 7:65-8:1. The threat matrix and threat models may be shown in a diagram or graph. EX-1008, 8:9-12. Each node in the graph represents an entity within the threat matrix. EX-1008, 8:16-18. Nodes have relationships to other nodes. EX-1008, 8:20-21. A node from one threat model may be connected to a node from a different threat model. EX-1008, 8:27-29.

IX. CLAIM CONSTRUCTION

80. In the Institution Decision, the Board invited the parties to address the proper construction of the following claim term: “redefine the first threat model by including in it a second threat model associated with the component group.”

Decision Granting Institution of *Inter Partes* Review, 15-16. Additionally, the Board invited the parties to address the potential applicability of *Ex Parte Schulhauser*, No. 2013-007847, 2016 WL 6277792 (PTAB Apr. 28, 2016) (precedential).

A. “Redefine the First Threat Model by Including In It a Second Threat Model Associated with the Component Group”

81. The claim phrase “redefine the first threat model by including in it a second threat model associated with the component group” appears in independent

claim 1 and dependent claims 11 and 20. This phrase should be construed to mean “change the first threat model by adding a predefined interrelated component group and its associated second threat model to the first threat model where the added component group was not a part of the first threat model before being added.”

This proposed construction is supported by the plain language of the claims and the specification.

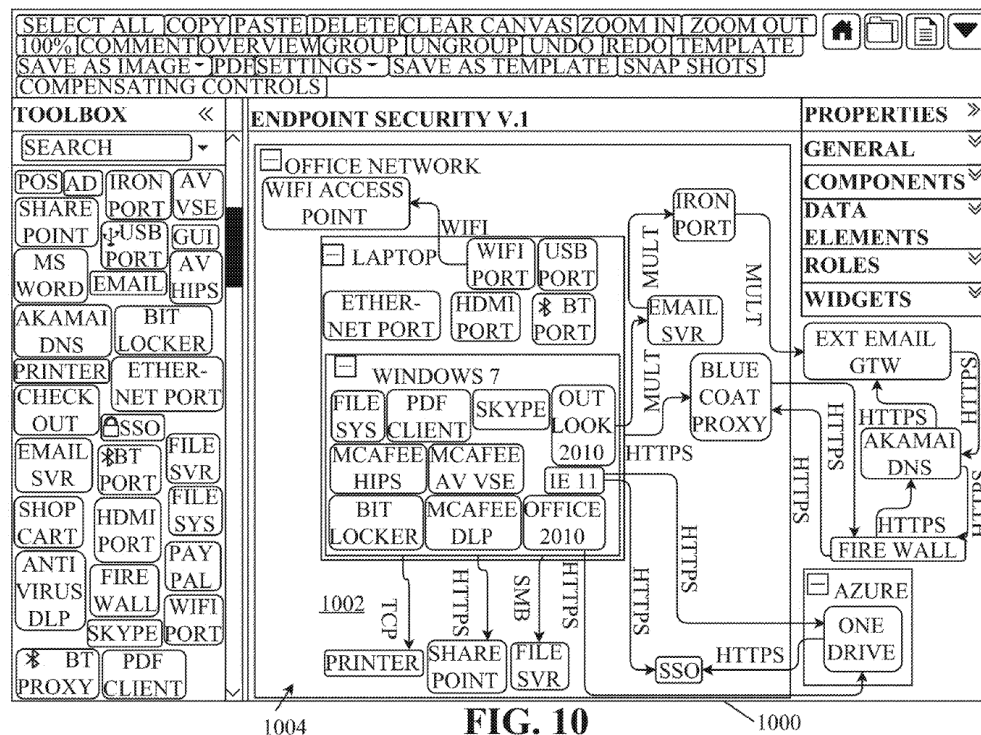
82. As an initial matter, a person of ordinary skill in the art would understand the word “redefine” to require the threat model to change, not simply to be expanded with more detail. This is supported by the claims and the specification as well. For example, claim 1 requires that the “component group” that is **added** to the first threat model must comprise “a predefined interrelated group of two or more of the threat model components.” Thus, the “component group” must be defined before it is added to the first threat model. The claim language also requires that the “component group” is “add[ed]” to the first threat model. This means that the component group could not have been part of the first threat model prior to being added. The claim language also explains that the addition of the component group to the first threat model “thereby redefine[s]” the first threat model “by including in it a second threat model associated with the component group.” Thus, the component group must have had its own “second”

threat model before it was added to the first threat model and the addition of the component group also requires that the threat model of the component group is added to the first threat model.

83. The specification explains this further. The '008 Patent explains that a group of threat model components can be diagrammed separately as an independent threat model and then saved as a component so that it can be imported into another threat model. EX-1001, 20:23-26. That newly created “component” (*i.e.*, a “component group” in the language of the claims) can be saved, for example, in a toolbox menu as a single item. EX-1001, 20:37-39. For example, according to the specification, a user could define a “Windows 7” component group. EX-1001, 20:39-41. That group may include, for example, a file system, PDF client, Skype, Outlook 2010, McAfee HIPS, McAfee AV VSE, Internet Explorer 11, Office 2010 and other components. EX-1001, 19:52-56. Once created and stored, a user could add the Windows 7 component to another threat model thereby importing into the threat model the threats and threat model associated with the Windows 7 component group. EX-1001, 20:41-45. When a user adds a component group to an existing threat model, the threat model of the component group is added to (or “nested” within) the existing threat model. EX-1001, 20:26-30. In this way, a user can modify a threat model by incorporating

The ‘008 Patent also refers to this as “threat model chaining.” EX-1001, 20:32-33; 24:10-30; 32:11-39. Notably, however, the “nesting” is not simply an expansion of detail on the existing model. The “Windows 7” component is not an expansion on an existing computer component but is an addition that “redefines” the threat model and introduces new threat model components into the existing threat model.

84. Figure 10 from the ‘008 Patent shows this “nested” arrangement graphically after the Windows 7 component group has been added to a first threat model.



85. In the center of Figure 10, the Windows 7 component group (shown in

a box within the “laptop” box) has been added to the “Laptop” group.

B. “Threat Model Components”

86. The ‘008 Patent describes each “threat model component” as “a potential relevant source for one or more threats.” EX-1001, 9:28-30. One example provided in the specification is that one threat may be “Bluejacking,” in which a potential attacker may seek to gain improper access to a system via its Bluetooth interface. In this example, the threat model component is the “Bluetooth port,” *i.e.*, the potential source of the threat. EX-1001, 9:30-36. As another example, an “online banking interface” may be stored as a threat model “component,” and “a threat may be a virus being introduced to the bank’s environment through a breach in the banking interface.” EX-1001, 24:42-52.

87. Further, the ‘008 Patent explains that threat model components are not limited to physical components. Components can be steps, actions, or a physical component. EX-1001, 9:38-52. An example of a non-physical component/source is “merging onto freeway” when modeling the threats of commuting to work. “Merging onto freeway” is an action as opposed to a physical component that may be correlated to a threat such as a “freeway collision.” EX-1001, 9:39-45.

88. Figure 10 of the ‘008 Patent and its associated description in the specification provide other examples of threat model components/sources

including a USB port, SSO (single sign on), Bluetooth port, and Bluetooth proxy.

EX-1001, 17:12-17.

89. The term “threat model components” should be construed as “a potential relevant source for one or more threats.” Petitioner and its expert agree with this construction. Petition, 12; EX-1003, ¶51.

C. Applicability of Ex Parte Schulhauser

90. In the Institution Decision, the Board asked the parties to consider whether *Ex parte Schulhauser*, No. 2013-007847, 2016 WL 6277792 (PTAB Apr. 28, 2016) (precedential), applies to the limitations of the claims of the ‘008 Patent. Institution Decision, 16. The example limitation the Board asked the parties to consider was “configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model.”

91. I understand that ultimately, whether *Schulhauser* applies to the claims of the ‘008 Patent or not is a legal conclusion. But from the perspective of a POSITA and generally an expert in the field of computer and network security, I do not read the example limitation identified above to include a conditional claim language.

92. The example limitation from the ‘008 Patent the Board identified is “configuring the diagram interface to, in response to receiving one or more user

inputs, add a component group to the first threat model.” In my opinion, there is no condition present in this claim language. Instead, to satisfy the claim, the claim requires that the system “receiv[e] one or more user inputs,” and in response to the one or more inputs, “configure[e] the diagram interface to ... add a component group to the first threat model.” To satisfy this step, both the user input(s) must be received and the diagram interface must be configured to add a component group. Because of the “in response to” language, this claim language requires that the user input is received before the diagram interface is configured.

93. Other claims recite similar language such as “receiving a [user] selection” (claims 2, 4, 12), “receiving one or more user inputs” (claims 3, 5, 8-12, 15-17, 19-20), “receiving a user toggle” (claims 6, 7), and “receiving a user input” (claims 13, 14). In each of these cases, my opinion is the same. The “receiving” of the input, selection, or toggle are required elements of the claims. These are not conditions determining whether a particular method step needs to be performed.

X. SUMMARY OF OPINIONS

94. Petitioner, IriusRisk, did not show that any challenged claim is anticipated by Jones, or would have been obvious over Jones in combination with any of the other references relied upon in Grounds 2-5. Petitioner failed to show that all limitations of the challenged claims were disclosed by or would have been

obvious to a person of ordinary skill in the art in May 2017 in light of the references relied upon in Grounds 1-5.

95. To summarize:

- It is my opinion that claims 1 and 3 are not anticipated by Jones (Ground 1).
- It is my opinion that claims 1-20 are not obvious based on Jones, Zheng, and Keenan (Ground 2).
- It is my opinion that claims 1-20 are not obvious based on the references of Ground 2 and Yu (Ground 3).
- It is my opinion that claims 1-20 are not obvious based on the references of Ground 3 and Reith (Ground 4).
- It is my opinion that claims 5-8 and 13-15 are not obvious based on the references of Ground 4 and the knowledge of a POSITA (Ground 5).

XI. OPINIONS CONCERNING THE CHALLENGED CLAIMS

A. Ground 1: Jones Does Not Anticipate Claims 1 and 3

1. Jones Does Not Disclose Adding a Component Group to a First Threat Model

96. Claim 1 reads, in part:

configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined

interrelated group of two or more of the threat model components.²

97. EX-1001, 35:56-63. This portion of claim 1 requires that the “component group” that is added to the first threat model must comprise “a predefined interrelated group of two or more of the threat model components.” Thus, the “component group” must be defined before it is added to the first threat model. The claim language also requires that the “component group” is “add[ed]” to the first threat model. This means that the component group could not have been part of the first threat model prior to being added. The claim language also explains that the addition of the component group to the first threat model “thereby redefine[s]” the first threat model “by including in it a second threat model associated with the component group.” Thus, the component group must have had its own “second” threat model before it was added to the first threat model. The addition of the component group also requires that the threat model of the component group is added to the first threat model.

98. Jones does not satisfy these claim requirements. Jones’ information systems may include components such as hosts, processes, data stores and/or external entities, and data flows between those components. EX-1004, 5:4-6. The

² This is labeled Element 1[f] in the petition.

information system may be described as having a “hierarchical breakdown” or “hierarchy” of its components at different levels. EX-1004, 5:10-14. The information system may have multiple “nested” components, one or more of which may further have its own additional “nested” components at lower levels of the hierarchy. EX-1004, 5:14-19. In other words, the components of Jones’ information system may have components that have subcomponents, and some of the subcomponents may have their own subcomponents, etc. By moving from one layer of the hierarchy to another allows a user to examine threats at different “levels” of the information system. EX-1004, 5:4-19.

99. Jones explains that if one wants to analyze the nested components of the information system in greater detail so as to examine their specific security threats, the decomposer 110 is used to “decompose” the components of the information system modeled by the data flow diagram (“DFD”) into their “nested” subcomponents and the data flows between those subcomponents. EX-1004, 6:12-18. The “nested” subcomponents were already present in the information system and the threat model created by Jones’ system for analyzing the information system. *See* EX-2002, 71:9-72:3, *see also* 51:25-52:22, 53:4-10, 70:6-23, 116:15-117:7. But the nested subcomponents were not visible at level “n” of the hierarchy, for example. Those subcomponents may become visible when the threat

model components are “decomposed” into their level “n+1” subcomponents. *See* EX-2002, 71:9-72:3, *see also* 51:25-52:22, 53:4-10, 70:6-23, 116:15-117:7. The threats associated with the subcomponents and their threat modeling are included in the threat model for the component itself. *See* EX-2002, 54:4-14. Notably, the DFD creator modifies the “threat-model DFD *for* the decomposed components.” *Id.*, 6:18-22. This illustrates that the threat model is updated to show more detail as existing components are further analyzed.

100. In Jones, the subcomponents at the n+1 level of the hierarchy are already included in the level n threat model. The decomposer 110 simply exposes some selection of those level n+1 subcomponents so that the threats associated with those subcomponents can be analyzed.

101. Element 1[f] requires that a predefined, interrelated “component group” of threat model components must be “add[ed]” to the first threat model. “Adding” the “component group” does not occur in Jones because all components and subcomponents of the information system being examined are already present in the information system. *See* EX-2002, 71:9-72:3, *see also* 51:25-52:22, 53:4-10, 70:6-23, 116:15-117:7. Jones’ decomposer 110 breaking the level n components into its level n+1 subcomponents. But those subcomponents were already present. No component or “component group” is added to a first threat model in Jones’

system.

102. Element 1[f] also requires that the “component group” that is added to the first threat model must be a “predefined” interrelated group of threat model components. Petitioner and its expert, Mr. Hurlbut, argue that Jones discloses a “predefined” group of threat model components because the underlying information system is predefined. EX-1003, ¶82 (p.45); EX-2002, 76:5-19. Just because the information system in Jones is “predefined” says nothing about whether there is a “component group” including a “predefined interrelated group” of threat model components. There is no teaching in Jones that a “component group” of threat model components is “predefined.” Petitioner’s and Mr. Hurlbut’s assertion to the contrary is conclusory and not based on any evidence. On the other hand, Jones describes the decomposer as doing analysis when decomposing existing components. As discussed above, Jones discloses decomposing components based on their existing hierarchy; however, how it chooses to decompose (which elements get included in the $n+1$ decomposition) is up to the decomposer, indicating that there is no “predefined” component group. Jones states, “In these examples, the decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows there between. The

decomposer may then provide feedback of its decomposition to the DFD creator

106....” EX-1004, 6:15-20.

103. Element 1[f] explains that adding the component group to the first threat model “thereby redefine[s]” the first threat model “by including in it a second threat model associated with the component group.” Thus, the component group must have its own “second threat model” before it is added to the first threat model because the claim requires that the addition of the component group is what causes the first threat model to be “redefined.” This is supported by the specification of the ‘008 Patent as well. *See* Section IX.A, *supra*.

104. Because Jones does not teach or suggest a “predefined, interrelated” “component group,” Jones necessarily does not teach or suggest such a “component group” that has a “second threat model” associated with the “component group” before the “component group” is added to the first threat model.

105. Jones does not teach or suggest Element 1[f].

2. Jones Does Not Disclose “Display[ing] a Relational Diagram ... Using ... Visual Representations of One or More of the Compensating Controls” as Required by Element 1[e]

106. Element 1[e] from claim 1 of the ‘008 patent requires “configuring the diagram interface to display a relational diagram” using “visual representations of

one or more of the compensating controls.” Jones does not teach or suggest a relational diagram using “visual representations of one or more of the compensating controls.” Jones Figure 9 does show visual representations of threat model components and threats. But visual representations *of compensating controls* are not depicted at all.

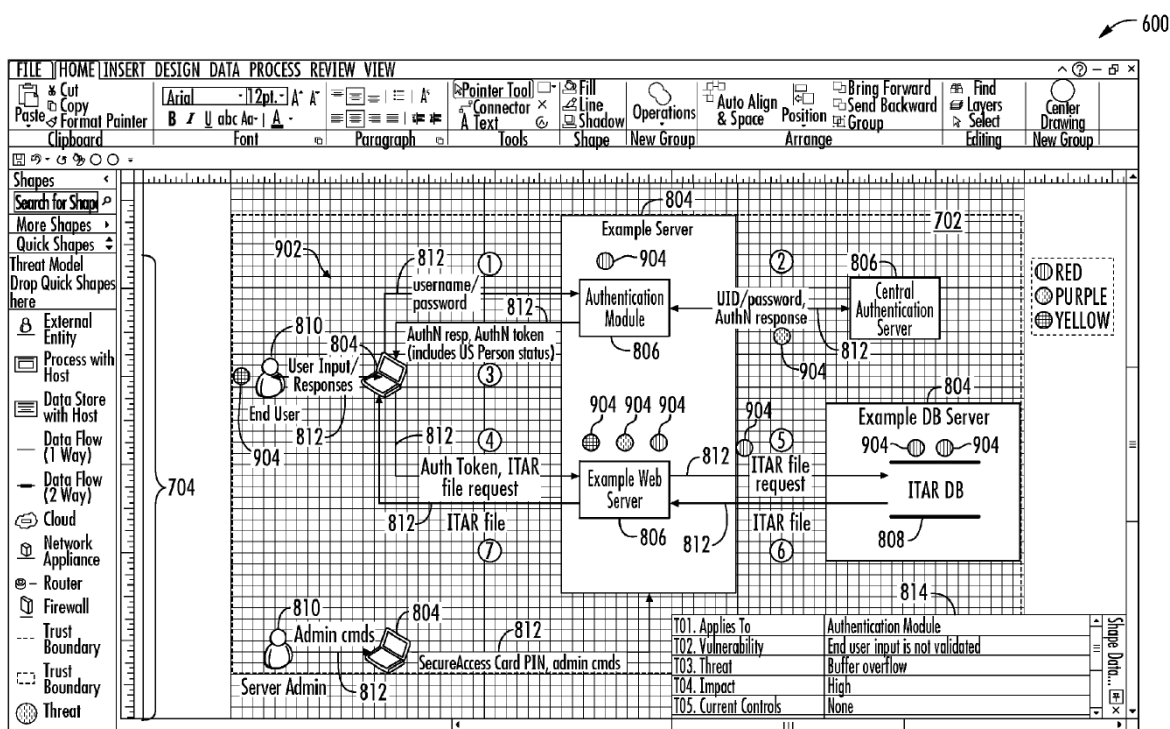


FIG. 9

107. As support for their assertion that Jones discloses Element 1[e], Petitioner and Mr. Hurlbut cite to Jones’ Figures 7-9 and 10B, col. 18:44-19:28, and the analysis for Element 1[d]. Petition, 33; EX-1003, ¶80. Figure 9 is a more complete version of Figures 7 and 8. As shown above, none of those figures disclose visual representations of compensating controls on a relational diagram.

Jones states that Figure 10B is a “report” – not a relational diagram. EX-1004, 3:29-30. The paragraphs at Jones’ column 18:44-19:28 are the textual descriptions of Figures 7-9. That portion of Jones does not even mention the concept of compensating controls. Finally, Petitioner’s and Mr. Hurlbut’s reliance on the analysis of Element 1[d] is misplaced. Element 1[d] has nothing to do with compensating controls or visual representations of compensating controls. Element 1[d] recites a diagram interface displayed on a a user computing device communicatively coupled to a database. At deposition, Mr. Hurlbut testified that he was not relying on an inherency argument for Element 1[e]. EX-2002, 30:9-31:21. Thus, there is no argument that Jones inherently discloses a “relational diagram” using “visual representations of one or more compensating controls.”

108. Jones does not teach or suggest a “relational diagram” using “visual representations of one or more compensating controls” as required by Element 1[e].

3. Jones Does Not Teach or Suggest Claim 3

109. Dependent claim 3 recites:

The threat model chaining method of claim 1, further comprising configuring the one or more interfaces to, in response to receiving one or more user inputs, store one or more additional threat model components in the one or more databases, store one

or more additional threats in the one or more databases, associate each additional threat with at least one of the additional threat model components through the one or more databases, store one or more additional compensating controls in the one or more databases, and associate each additional compensating control with at least one of the additional threats through the one or more databases.

EX-1001, 36:4-15 (emphasis added).

110. Claim 3 (and claim 1 from which claim 3 depends) is a method claim. Claim 3 requires the storing of “additional” threat model components, threats, and compensating controls. Claim 3 further requires that “each additional threat” is associated with “at least one of the additional threat model components.” Claim 3 also requires that “each additional compensating control” is associated with “at least one of the additional threats.”

111. At deposition, Mr. Hurlbut confirmed that in his analysis the “additional” threats, threat model components, and compensating controls recited in claim 3 were not satisfied by the threats, threat model components, and compensating controls identified in connection with claim 1. EX-2002, 82:17-84:6.

112. None of the portions of Jones cited by Mr. Hurlbut or the Petition disclose the storing of a second set of threats, threat model components, and

compensating controls and making associations among those threats, threat model components, and compensating controls, as required by claim 3. Column 4:13-21 of Jones only says that one or more of the functions of its system can be performed manually or automatically. None of Figures 7-10B show a second set of threats, threat model components, and compensating controls being stored in a database with the claimed associations among themselves. Figure 9 shows multiple threats and components, but there is no teaching or suggestion of storing additional threats, threat model components, and compensating controls as required by claim 3. Similarly, the report shown in Figures 10A and 10B shows multiple threats and mitigations, but there is no teaching or suggestion of storing additional threats, threat model components, and compensating controls and making the associations among themselves recited in claim 3.

113. Jones does not teach or suggest claim 3.

B. Ground 2: Alleged Obviousness of Claims 1-20 Over Jones, Zheng, and Keenan

1. Dependent Claim 2

114. Claim 2 recites:

The threat model chaining method of claim 1, further comprising configuring the diagram interface to, in response to receiving a user selection of one of the diagrammed threat model components of the first threat model, visually display attack

paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.

EX-1001, 35:64-36:3.

115. Petitioner and Mr. Hurlbut solely rely on Zheng for the teaching or suggestion of the elements of claim 2. Petition, 42; EX-1003, ¶87, EX-2002, 85:15-24. No other reference is alleged to teach or suggest these claim features.

116. Zheng does not teach or suggest visually displaying attack paths of all threats associated with a threat model component “in response to receiving a user selection of one of the diagrammed threat model components of the first threat model.” As the claim language states, a user selects “one” of the threat model components which in turn causes all attack paths of all threats associated with the selected component to be displayed.

117. Zheng does not teach or suggest the selection of any threat model components much less the selection of “one” threat model component. The central thrust of Zheng is the creation and display of various layers, such as a base layer, a threat modeling layer, security controls layer, a real-time actual threats layer, and a simulated data flow layer. EX-1005, 4:5-12, *see also* 3:35-39. Zheng explains that “[t]hese additional layers 204-210 can overlay the foundational map layer 202, similar to how traffic and other information (in addition to basic cartographical

details) is represented on maps.” EX-1005, 4:13-16. Zheng further explains that “[t]hese additional layers 204-210 can overlay the base layer 202 in the order as illustrated in FIG. 2 or any other order.” EX-1005, 4:16-18. In Zheng, the display of information in various layers is an all or nothing proposition – the entire layer is displayed or the entire layer is not displayed. Zheng neither teaches nor suggests any other option because the layering concept is central to the system in Zheng.

118. Because Zheng either displays an entire layer or not, Zheng teaches that all potential paths from a threat to all potential targets can be displayed. In Figure 8, the threat model layer is represented by threat actor 912, and connections 914, 916, 918, and 920. All threat model connections for all applications 1-5 are shown. There is no user selection of one threat model component for which all associated threat and attack paths are shown.

119. The Petition and Mr. Hurlbut fail to provide an adequate explanation of how and why the teachings of Zheng and Jones can be combined. In Jones’ visual diagram, Jones shows threats placed above or in the component with which they are associated. EX-1004, Fig. 9. Figure 9 depicts the threats as circles 904 just above the associated component. In the context of this diagram interface, Jones expressly teaches looking at the attributes of threats one at a time. Jones explains that a pop-up window 814 can be displayed to show a diagram shape’s

attributes. EX-1004, 19:23-25. In Figure 9, window 814 shows that the threat is associated with the “authentication module.” The vulnerability is described as “end user is not validated.” The specific threat is “buffer overflow.” Other attributes of the threat are also displayed. EX-1004, Fig. 9. With this information displayed in window 814, Jones has no need (and in fact does not) display vectors from threat actors to threat targets.

120. As explained above, Zheng on the other hand teaches displaying an entire layer or not displaying the layer at all. To the extent Zheng display attack paths, Zheng displays all attack paths for all threats for all diagram components, or Zheng displays none at all.

121. Jones teaches displaying attributes of a single threat – not even all threats for a particular diagram component. Zheng is on the other end of the spectrum. Zheng displays all threats for all diagram components. The Petition and Mr. Hurlbut do not attempt to reconcile these divergent teachings. Petitioner and its expert have not explained why a POSITA would discard Jones’ teaching to display attributes about a single threat in favor of Zheng’s teaching to display all threats for all diagram components in a single layer. Jones’ single threat approach is more beneficial than Zheng’s approach because Jones allows a user to edit the attribute information for a threat. EX-1004, 19:18-25. Zheng does not offer that

feature. In fact, Zheng teaches away from building a threat model based on “manual input.” EX-1005, 1:1:24-27. Jones allows a user to delve deeper into a threat model on a threat-by-threat basis. Zheng does not allow that threat-by-threat analysis. A POSITA would have wanted the detailed analysis offered by Jones coupled with the ability to edit the attributes of threat available in the system of Jones in order to allow for a more accurate modeling of threats found in the system being modeled. A POSITA would have found Zheng’s all or nothing approach (without the ability to edit threat attributes) to be substantially inferior to Jones’ system. Thus, contrary to the Petition and Mr. Hurlbut’s analysis, a POSITA would not have combined Zheng’s teachings with those of Jones.

122. The portion of Keenan cited in the Institution Decision does not teach or suggest “visually display[ing] attack paths of all threat associated with the diagrammed threat model components which compromise the selected threat model component,” as recited in claim 2. Instead, Keenan 17:12-20 relates to displaying upstream and downstream data flows or paths for objects. EX-1006, 17:12-20. At most, it teaches toggling display features on and off.

2. Independent Claim 4

123. Independent claim 4 has many claim elements in common with claims 1 and 2. In mapping their invalidity contentions, Petitioner and its expert omitted

the paragraph of claim 4 that begins “configuring the diagram interface to display a relational diagram” Institution Decision, 9 n.1. The omitted paragraph from claim 4 is identical to Element 1[e]. For the reasons Patent Owner provided above, Jones does not teach or suggest Element 1[e]. Jones does not teach or suggest “display[ing] a relational diagram ... using ... visual representations of one or more of the compensating controls.” See Section XI.A.2, *supra*.

124. In addition, Element 4[e] in the petition is nearly identical to the substance of claim 2. Thus, for the reasons provided above for claim 2, Jones does not teach or suggest Element 4[e]. See Section XI.B.1, *supra*.

3. Dependent Claims 6 and 7

125. Claim 6 recites:

6. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving a user toggle of one of the diagrammed compensating controls (hereinafter “first control”) of the first threat model to an on state through the one or more interfaces, toggle all attack paths mitigatable by the first control to a mitigated display state.

126. Claim 7 depends from claim 6 and recites the inverse action:

7. The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving a user toggle of the first control to an off state through the one or

more interfaces, toggle all attack paths mitigatable by the first control to an unmitigated display state.

127. As explained above in connection with claims 1 and 4, Jones does not teach or suggest the display of “compensating controls” on the relational diagram recited in claim 4. Thus, the “compensating controls” of claims 6 and 7 are not taught or suggested by the cited prior art. See Sections XI.A.2 and XI.B.2, *supra*.

128. Second, none of the cited references teach or suggest “security controls” or “mitigations” that can be set to an on state and cause the system to “toggle all attack paths mitigatable by the first control to a mitigated display state.” Petitioner and its expert provide no analysis of this claim requirement whatsoever. Petition, 45-46; EX-1003, ¶¶97-99.

129. Instead, for the teachings of “compensating controls,” Petitioner and Mr. Hurlbut cite back to the analysis of Elements 1[c] and 1[c]. But neither of those elements related to “toggle all attack paths mitigatable by the first control to a mitigated display state.”

130. For the concept of “attack paths,” Petitioner and Mr. Hurlbut cite to Zheng and their analysis for claims 2 and 5. But as explained above in the analysis of claim 2, neither Petitioner nor its expert provided a reasoned analysis how Jones’ analysis on a threat-by-threat basis can be reconciled with Zheng’s disclosure of displaying entire layers which would include all threats for all

diagram components. *See* Section XI.B.1, *supra*. In fact, a POSITA would not modify Jones to include the so-called “attack path” teachings of Zheng because, as explained above, Jones offers a more robust and flexible system compared to Zheng.

4. Dependent Claim 8

131. Instead of turning off a compensating control as recited in claim 7, claim 8 requires that the compensating control be removed entirely from the relational diagram. Specifically, claim 8 recites:

8. The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces to remove the first control from the first threat model, toggle all attack paths mitigatable by the first control to an unmitigated display state.

132. Petitioner and Mr. Hurlbut make no effort to show that it would have been obvious to remove a compensating control from the relational diagram. Instead, they simply assert that claims 7 and 8 are “substantively identical.” Petition, 47; EX-1003, ¶100. The difference is that if the control is turned off, it can be easily turned back on without having to reinstall it into the threat model. Removing the control does not allow for it to be easily turned back on. Instead, the user would have to choose what compensating control to add to the relational diagram, select where to add the control, and choose or edit its parameters, if

desired. I understand that claims having different words are presumed to have different meanings.

5. Dependent Claim 9

133. Dependent claim 9 recites:

9. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.

134. In relevant part, claim 9 requires “visually display[ing] only attack paths of all threats associated with a subset of the diagrammed threat model components.” EX-1001, 37:1-6 (emphasis added). Neither Petitioner nor Mr. Hurlbut make any effort to show that the prior art teaches or suggests displaying attack paths of threats associated with “a subset” of the diagrammed threat model components. Petition, 47, EX-1003, ¶101. Instead, they simply make the conclusory allegation that this element would have been obvious. Petitioner failed to establish that claim 9 would have been obvious.

6. Dependent Claim 10

135. Dependent claim 10 recites:

10. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one

or more user inputs through the one or more interfaces to alter a profile of an attacking component, alter the visually displayed attack paths.

136. Again, Petitioner and Mr. Hurlbut make no effort to show that claim 10 would have been obvious. Instead, Petitioner and Mr. Hurlbut argue that because Keenan allegedly discloses modifying or editing a display, it would have been obvious to allow for the modification of individual attacking components and attack paths. Petition, 48, EX-1003, ¶102. But, as explained above in the context of claim 2, Zheng teaches displaying an entire layer or not displaying the layer at all. *See* Section XI.B.1, *supra*. The point of Zheng is to have different layers displaying different aspect of its system. For claim 10, Petitioner is relying on Keenan's ability to modify individual components. That capability is similar to Jones' ability to view the attributes of individual components. But Jones' and Keenan's ability to view or edit individual components is at the opposite end of the spectrum of Zheng which only display layers with no ability to modify or even view individual components. Petitioner provides no explanation of how to reconcile these divergent teachings. In fact, a POSITA would not modify Zheng to allow for the viewing and editing of individual components because that runs contrary to the entire purpose of Zheng, which is to display a threat model in various layers.

7. Dependent Claim 11

137. Dependent claim 11 is substantively the same as Element 1[f] and Petitioner and Mr. Hurlbut do not argue otherwise. Thus, for the reasons provided above with respect to Element 1[f], claim 11 is not obvious. *See* Section XI.A.1, *supra*.

8. Independent Claim 12

138. The elements of independent claim 12 overlap with elements of prior claims. Element 12[d] recites:

a diagram interface configured to, in response to receiving one or more user inputs, diagram one of a system, an application, and a process, the diagram including one or more of the threat model components and one or more of the compensating controls, to define a first threat model, the first threat model including all threats associated through the one or more databases with the diagrammed threat model components

EX-1001, 37:36-43 (emphasis added).

139. Petitioner and Mr. Hurlbut assert that “Jones discloses this element.” Petition, 49, EX-1003, ¶107. As explained above with respect to Element 1[e], Jones does not teach or suggest the inclusion of “compensating controls” on a diagram that defines a threat model. *See* Section XI.A.2, *supra*.

140. Element 12[e] recites:

wherein the diagram interface is configured to, in response to receiving a selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.

EX-1001, 37:43-38:3. Element 12[e] is nearly identical as claim 2 and Element 4[e]. Thus, for the reasons provided above for claim 2, Jones does not teach or suggest Element 12[e]. *See* Section XI.B.1, *supra*.

9. Dependent Claim 13

141. Dependent claim 13 is substantively the same as dependent claim 6. Thus, for the reasons provided above for claim 6, claim 13 is not obvious as alleged in the Petition. *See* Section XI.B.3, *supra*.

10. Dependent Claim 14

142. Dependent claim 14 is substantively the same as dependent claim 7. Thus, for the reasons provided above for claim 7, claim 14 is not obvious as alleged in the Petition. *See* Section XI.B.3, *supra*.

11. Dependent Claim 15

143. Dependent claim 15 is substantively the same as dependent claim 8. Thus, for the reasons provided above for claim 8, claim 15 is not obvious as alleged in the Petition. *See* Section XI.B.4, *supra*.

12. Dependent Claim 16

144. Dependent claim 16 is substantively the same as dependent claim 9.

Thus, for the reasons provided above for claim 9, claim 16 is not obvious as alleged in the Petition. *See* Section XI.B.5, *supra*.

13. Dependent Claim 17

145. Dependent claim 17 is substantively the same as dependent claim 10.

Thus, for the reasons provided above for claim 10, claim 17 is not obvious as alleged in the Petition. *See* Section XI.B.6, *supra*.

14. Dependent Claim 19

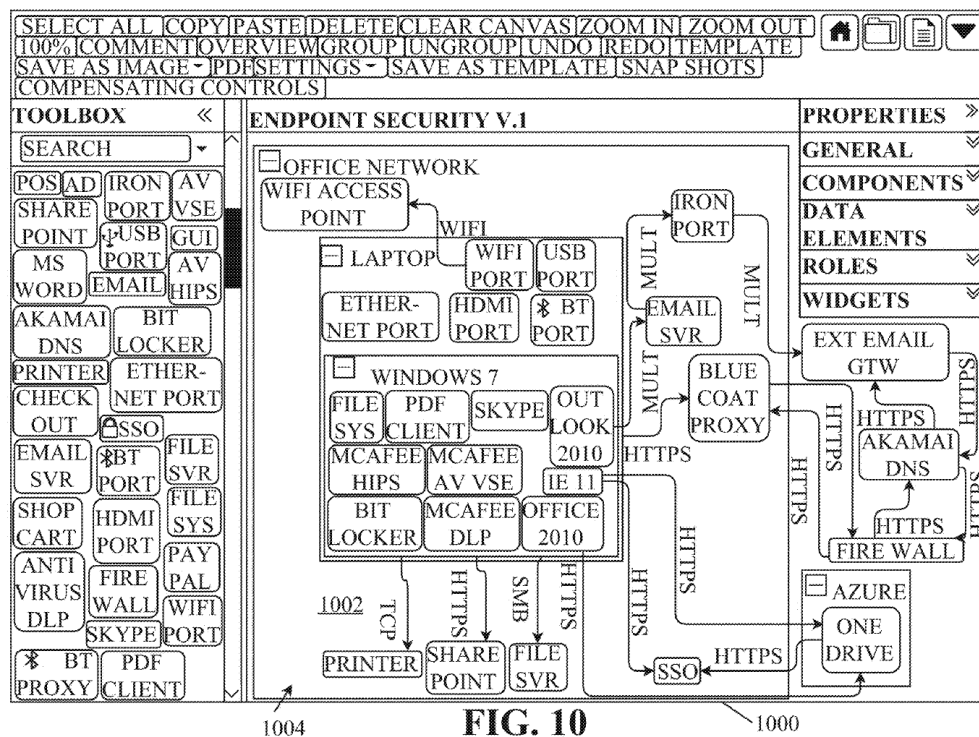
146. Dependent claim 19 recites:

19. The attack simulation system of claim 18, wherein the diagram interface is further configured to, in response to receiving one or more user inputs, diagram a communication protocol between two of the diagrammed threat model components, the diagrammed communication protocol including an alphanumeric indicator.

147. Claim 19 requires that “a communication protocol” is diagrammed in response to one or more user inputs “between two of the diagrammed threat model components, the diagrammed communication protocol including an alphanumeric indicator.” Petitioner and Mr. Hurlbut argue that Jones discloses this limitation. Petition, 52, EX-1003, ¶115. Petitioner and Mr. Hurlbut specifically point to

Jones' disclosure of "User Input/Responses" between end user 810 and computing device 804 in Jones' Figure 9. They also cite to the disclosure of "Auth N token" and "ITAR file requests" between computing device 804 and the example server(s) 806. Petition, 54, EX-1003, ¶116.

148. The '008 Patent provides several examples of communication protocols, some of which are depicted in Figure 10. In Figure 10, the communication protocols include HTTPS, TCP, SMB, and WiFi.



149. Contrary to Petitioner's assertion, "User Input/Responses," "Auth N token" and "ITAR file requests" are not communication protocols, they are data. Mr. Hurlbut admitted this distinction at his deposition. Mr. Hurlbut effectively

contradicted his declaration and admitted that information such as usernames and passwords were just data and were not communication protocols. EX-2002, 108:9-24.

150. Indeed, Zheng discloses a long list of communication protocols, none of which include the “User Input/Responses,” “Auth N token” and “ITAR file requests” relied upon by Petitioner and in Mr. Hurlbut’s declaration. EX-1005, 13:60-14:4.

151. The Petition and its cited prior art does not teach or suggest Claim 19.

C. Ground 3: Alleged Obviousness of Claims 1-20 Based on Jones, Zheng, Keenan, and Yu

152. The Petition and Mr. Hurlbut do not rely on Yu to remedy all of the deficiencies identified previously with respect to Grounds 1 and 2. Yu is only relied upon as teaching particular aspects of certain of the “compensating controls” and “attack path” limitations. Petition, 57-60, EX-1003, ¶¶122-128. The remaining deficiencies identified with respect to Grounds 1 and 2 remain and show that Petitioner has failed to meet its burden of establishing that claims 1-20 are invalid.

153. Further, the Petition fails to provide sufficient reasons why a POSITA would have combined Yu with the combination of Jones, Zheng, and Keenan. Even if Yu relates to the same general technology as that of Jones, Zheng, and

Keenan, that does not provide sufficient basis for adding Yu to the combination.

Moreover, at best, Keenan relates to risk modeling – not threat modeling.

154. Petitioner and Mr. Hurlbut argue that Yu would add “compensating controls” and “attack paths” to the Jones, Zheng, and Keenan combination. But the claims of the ‘008 Patent do not simply recite those concepts as claim elements. “Compensating controls” and “attack paths” are recited in the claims as having specific relationships to other elements of the claims. Even if Yu discloses “compensating controls” and “attack paths,” that is not sufficient to establish that all aspects of the claims of the ‘008 Patent are taught or suggested.

155. The addition of Yu does not render claims 1-20 obvious.

D. Ground 4: Alleged Obviousness of Claims 1-20 Based on Jones, Zheng, Keenan, Yu, and Reith

156. The Petition and Mr. Hurlbut rely on Reith for allegedly disclosing the so-called “threat model chaining” features of Element 1[f] and claims 11 and 20.

Petition, 60, EX-1003, ¶129.

157. The claim phrase “redefine the first threat model by including in it a second threat model associated with the component group” appears in Element 1[f] and dependent claims 11 and 20. This claim language requires that the “component group” is “add[ed]” to the first threat model. This means that the component group could not have been part of the first threat model prior to being

added. The claim language also explains that the addition of the component group to the first threat model “thereby redefine[s]” the first threat model “by including in it a second threat model associated with the component group.” Reith’s Recombinant Threat Models do not teach or suggest any of these claim features.

158. The Petition relies on Reith’s Figure 4 and its associated description. Petition, 60-61, EX-1003, ¶129. Figure 4 shows that there is a hierarchy having individual threat models at the bottom level, multiple threat landscapes that include their respective individual threat models at the middle level, and a single threat matrix that includes each of the threat landscapes. Reith states that a Recombinant Threat Model may stand on its own within the threat landscape or multiple Recombinant Threat Models may be interconnected together. EX-1008, 4:32-35. “Interconnected” merely means that the threat models may be connected to each other. There is no teaching or suggestion that a predefined component group having its own threat model is “added” to a first threat model and “thereby redefining” the first threat model, as required by the ‘008 Patent claims.

159. Moreover, the alleged reasons provided for combining Reith with the other references is entirely based on hindsight and has no evidentiary support. The Petition and Mr. Hurlbut argue that a POSITA would have been motivated to combine Reith with the other references because “Reith saves time when the user

is building the threat model because it allows the user to incorporate existing threat models into the new threat model without ‘recreating the wheel.’” Petition, 61, EX-1003, ¶131.

160. This “reason” comes right out of the ‘008 Patent. The ‘008 Patent explains that:

When a user adds any of these component groups to a blank or existing diagram/threat model the threat model of the component group is added to (and/or nested within) the threat model of the existing diagram/threat model. In this way the user can modify a threat model by incorporating previously defined threat models. This ability is generally termed “threat model chaining” herein and is a useful mechanism for allowing a user to diagram complex systems/processes without having to repeatedly build common elements among the systems/processes.

EX-1001, 20:26-36. The rest of the reasons why a POSITA would have combined Reith with the other references is simply a recitation of various *KSR* categories for showing that an invention would have been obvious – namely, “would have been within the skillset of a POSIA,” “would require no undue experimentation,” “an easily predictable result,” “reasonable expectation of success,” “very predictable technologies,” and “would not encounter any insurmountable challenge[s].”

Petition, 61-62, EX-1003, ¶132. Petitioner and Mr. Hurlbut provided no evidence

supporting these conclusions.

161. Petitioner has not established that claims 1-20 are obvious based on the references of Ground 4.

E. Ground 5: Alleged Obviousness of Claims 5-8 and 13-15 Based on the References of Ground 4 and the Knowledge of a POSITA

162. Petitioner and Mr. Hurlbut rely on the knowledge of a POSITA to teach the toggling limitations of claims 5-8, and 13-15. Petition, 62, EX-1003, ¶133. This alleged knowledge of a POSITA does not address all of the reasons why Petitioner has not shown why claims 1-20 are invalid as explained above with respect to Grounds 1-4. Toggling is only one aspect of certain claims.

163. The Petition and Mr. Hurlbut make assertions about what a POSITA would have understood about toggling and why a POSITA would have combined the knowledge of a POSITA with the other references. But the Petition provides no evidence supporting any of the assertions of Ground 5 other than citing to Mr. Hurlbut's declaration. Petition, 62-63. But Mr. Hurlbut's declaration fails to cite to any evidence itself. EX-1003, ¶¶133-134.

164. The reasons why a POSITA would have combined the knowledge of a POSITA with the references of Ground 4 is a recitation of various *KSR* categories for showing that an invention would have been obvious – namely, “reasonable expectation of success,” “very predictable technologies,” and “would not encounter

any insurmountable challenge[s].” Petition, 62-63, EX-1003, ¶134. Neither Petitioner nor Mr. Hurlbut provided any evidence supporting these conclusions.

XII. CONCLUSION

165. For the reasons discussed above, it is my opinion that the challenged claims are not anticipated and/or rendered obvious over the references relied upon in the Petition.

XIII. AVAILABILITY FOR CROSS-EXAMINATION

166. In signing this declaration, I recognize that the declaration will be filed as evidence in a case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

XIV. RIGHT TO SUPPLEMENT

167. I reserve the right to supplement my opinions in the future to respond to any arguments that the Petitioner may raise and to take into account new information as it becomes available to me.

XV. DECLARATION

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

Dated: February 14, 2024

A handwritten signature in black ink, appearing to read 'Seth James Nielson', written over a horizontal line.

Seth James Nielson, Ph.D.

Appendix A: The Challenged Claims of the '008 Patent

1. A threat model chaining method, comprising:

providing one or more databases, the one or more databases comprising:

a plurality of threat model components stored therein;

a plurality of threats stored therein, each threat associated with at least one

of the threat model components through the one or more databases;

and

a plurality of compensating controls stored therein, each compensating

control associated with at least one of the threats through the one or

more databases;

providing one or more interfaces, including a diagram interface, configured to be

displayed on one or more end user computing devices communicatively

coupled with the one or more databases;

configuring the diagram interface to display a relational diagram of one of a

system, an application, and a process, using visual representations of one or

more of the threat model components and visual representations of one or

more of the compensating controls, the relational diagram defining a first

threat model, and;

configuring the diagram interface to, in response to receiving one or more user

inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.

2. The threat model chaining method of claim 1, further comprising configuring the diagram interface to, in response to receiving a user selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.
3. The threat model chaining method of claim 1, further comprising configuring the one or more interfaces to, in response to receiving one or more user inputs, store one or more additional threat model components in the one or more databases, store one or more additional threats in the one or more databases, associate each additional threat with at least one of the additional threat model components through the one or more databases, store one or more additional compensating controls in the one or more databases, and associate each additional compensating control with at least one of the additional threats through the one or more databases.

4. An attack simulation method, comprising:

providing one or more databases, the one or more databases comprising:

a plurality of threat model components stored therein;

a plurality of threats stored therein, each threat associated with at least one

of the threat model components through the one or more databases;

and

a plurality of compensating controls stored therein, each compensating

control associated with at least one of the threats through the one or

more databases;

providing one or more interfaces, including a diagram interface, configured to be

displayed on one or more end user computing devices communicatively

coupled with the one or more databases;

configuring the diagram interface to display a relational diagram of one of a

system, an application, and a process, using visual representations of one or

more of the threat model components and visual representations of one or

more of the compensating controls, the relational diagram defining a first

threat model; and

configuring the diagram interface to, in response to receiving a user selection of

one of the diagrammed threat model components of the first threat model

through the one or more interfaces, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.

5. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces, visually display one or more attack paths which pass through multiple diagrammed threat model components of the first threat model.
6. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving a user toggle of one of the diagrammed compensating controls (hereinafter “first control”) of the first threat model to an on state through the one or more interfaces, toggle all attack paths mitigatable by the first control to a mitigated display state.
7. The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving a user toggle of the first control to an off state through the one or more interfaces, toggle all attack paths mitigatable by the first control to an unmitigated display state.
8. The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving one or more user inputs

through the one or more interfaces to remove the first control from the first threat model, toggle all attack paths mitigatable by the first control to an unmitigated display state.

9. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.
10. The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces to alter a profile of an attacking component, alter the visually displayed attack paths.
11. The attack simulation method of claim 3, further comprising configuring the diagram interface to receive one or more user inputs to add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.
12. An attack simulation system, comprising:

one or more computing devices communicatively coupled with one or more

databases, the one or more computing devices displaying, on one or more displays of the one or more computing devices:

one or more input interfaces configured to, in response to receiving one or more user inputs, store a plurality of user-defined threat model components in the one or more databases, store a plurality of threats in the one or more databases, associate each of the threats with at least one of the threat model components through the one or more databases, store a plurality of compensating controls in the one or more databases, and associate each compensating control with at least one of the threats through the one or more databases, and;

a diagram interface configured to, in response to receiving one or more user inputs, diagram one of a system, an application, and a process, the diagram including one or more of the threat model components and one or more of the compensating controls, to define a first threat model, the first threat model including all threats associated through the one or more databases with the diagrammed threat model components;

wherein the diagram interface is configured to, in response to receiving a selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.

13. The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving a user input to toggle one of the diagrammed compensating controls (hereinafter “first control”) to an on state, toggle all attack paths mitigatable by the first control to a mitigated display state.

14. The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to receiving a user input to toggle the first control to an off state, toggle all attack paths mitigatable by the first control to an unmitigated display state.

15. The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to receiving one or more user inputs removing the first control from the first threat model, toggle all attack paths mitigatable by the first control to an unmitigated display state.

16. The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.
17. The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, alter a profile of an attacking component, wherein the alteration alters the visually displayed attack paths.
18. The attack simulation system of claim 12, wherein the one of a system, an application, and a process comprises a computing network.
19. The attack simulation system of claim 18, wherein the diagram interface is further configured to, in response to receiving one or more user inputs, diagram a communication protocol between two of the diagrammed threat model components, the diagrammed communication protocol including an alphanumeric indicator.
20. The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the

component group, wherein the component group comprises a predefined
interrelated group of two or more of the threat model components.

Appendix B: Materials Reviewed

- U.S. Patent No. 10,699,008 to Agarwal (“the ‘008 Patent)
- Prosecution History for the ‘008 Patent
- Declaration of Robert Hurlbut (EX-1003)
- U.S. Patent No. 9,602,529 (“Jones”) (EX-1004),
- U.S. Patent No. 10,503,907 (“Zheng”) (EX-1005),
- U.S. Patent No. 11,200,228 (“Keenan”) (EX-1006),
- U.S. Patent No. 9,948,652 (“Yu”) (EX-1007),
- U.S. Patent No. 10,216,938 (“Reith”) (EX-1008);
- IPR2023-00821 Petition (Paper 1)
- IPR2023-00821 Patent Owner Preliminary Response (Paper 6)
- IPR2023-00821 Decision on Institution (Paper 7)
- February 5, 2024 Deposition Transcript of Mr. Robert Hurlbut (EX-2002)
- All other documents/materials cited or referred to in this declaration.

Case IPR2023-00821

Patent 10,699,008

Declaration of Seth James Nielson, Ph.D.

Appendix C: Seth James Nielson, Ph.D. Curriculum Vitae

Seth James Nielson's Vita

(512) 387-4310

seth@crimsonvista.com

January 2024

Academic Degrees

2009	Ph.D. Computer Science , Rice University, Houston, TX
2004	M.S. Computer Science , Brigham Young University, Provo, UT
2000	B.S. Computer Science , Brigham Young University, Provo, UT

Certifications

CISSP

Current Appointments

Founder and Chief Scientist	Crimson Vista, Inc.
Director of Cybersecurity Research	Curuvar LLC
Adjunct Assistant Professor	University of Texas at Austin Law School
Cybersecurity Fellow	Robert Strauss Center for International Security and Law

Professional Advising

2019-Present	Advisory Board	Syccure Inc.
--------------	----------------	--------------

Non-profit and Community Engagement

2021-Present	Founding Director	The Crypto Done Right Foundation
2019-2021	Cyberlab Advisory Board	The SEED School of Maryland

Grants and Research Awards

Decentralizing Zero-Trust Infrastructure to Combat Advanced Persistent Threats and Malicious Insiders (Senior Personnel), NSF 2020 SBIR solicitation. Award number 2051989, Curuvar LLC.

Mitigation of Ransomware, DoD 2018.B STTR solicitation (Army), Topic: A18B-T010, Crimson Vista, \$150,000 (2019)

An Enabling Repository of Cryptographic Knowledge (Co-PI), Cisco Grant, Johns Hopkins University Information Security Institute, \$150,000 (2017-2021)

University Research Funding

Sel4 Security Appliance Capstone, funded by Crimson Vista to Brigham Young University Department of Computer Science. 2021

Academic Awards

Brown Fellowship
John and Eileen Tietze Fellowship

Professional Service

International Cryptographic Module Conference, 2023 Program Committee
International Cryptographic Module Conference, 2022 Program Committee
International Cryptographic Module Conference, 2021 Program Committee
International Cryptographic Module Conference, 2020 Program Committee
International Cryptographic Module Conference, 2019 Program Committee
International Cryptographic Module Conference, 2018 Program Committee

Subject Matter Expertise and Selected Projects

Forensic Analysis (e.g., Code/IP Theft)

Investigation of cryptocurrency transfers and fraud (Crimson Vista, 2023-)
Investigation of website content development and provenance (Crimson Vista, 2023-)
Investigation of server, laptop, and hard drives for indications of tampering (Crimson Vista, 2023)
Investigation of voting machine software for vulnerabilities (Crimson Vista, 2022-)
Investigation of altered/forged emails (Crimson Vista, 2022)
CLE training related to source code analysis/trade secrets (Source Code Discovery, 2021)
Investigation of IP/code theft related to MTA, spear-phishing, and email (Crimson Vista, 2019-2021)
Investigation of code theft related to housing and rental software (Crimson Vista, 2019-2022)
Investigation of code theft related to digital mobile radios (Crimson Vista, 2017-2021)
Investigation of code theft related to financial trading software (Crimson Vista, 2016-2017)
Investigation of code theft related to e-commerce (Harbor Labs, 2015)
Investigation of IP theft embedded in source code related to domain anti-abuse (Harbor Labs, 2015)
Investigation of IP theft embedded in source code related to high-frequency trading (Harbor Labs, 2010-2011)

Applied Cryptography

Cryptography training modules (UT Austin, 2022-)
Analysis of compromised password hashes (Crimson Vista, 2020)
“Crypto Done Right”, Cryptographic Knowledge Base Non Profit (2020-)
“Crypto Done Right”, Cryptographic Knowledge Base with Cisco (Johns Hopkins, 2017-2020)
Simulated implementation of Vehicle-to-Vehicle authentication (Crimson Vista, 2018-2019)

Cryptographic protocol analysis and design for Syccure Inc. (Crimson Vista, 2017-2023)

Timing attacks on Hardware Security Modules with Diamond Key Security (Johns Hopkins, 2018)

Technical consulting for U.S. Dpt. of Justice (Antitrust Division, Transportation, Energy & Agriculture) (Crimson Vista, 2018)

Aircraft/drone anti-collision protocol security with OnBoard Security (Johns Hopkins, 2017)

Cryptographic communication library for Security First Corp (ISE, 2010-2011)

Encryption library, file system encryption, GPU for Security First Corp (ISE, 2005-2011)

Security Operations, Compliance, Oversight

Virtual Chief Information Security Officer for IperionX (Crimson Vista, 2022-2023)

IoT Devices and IoT Security

Traffic lights and systems software analysis (Crimson Vista, 2023-)

Vulnerability and exploitation analysis of voting machine hardware (Crimson Vista, 2023-)

High-security appliance based on formal methods (Crimson Vista, BYU, 2021)

Hadoop security research (Crimson Vista, 2021-2022)

IoT data sensors for agricultural operations (Crimson Vista, 2020-2023)

Contributor, reviewer for the Institute of Assured Autonomy (Johns Hopkins, 2019)

IoT data aggregation security with Armored Things (Johns Hopkins, 2018-2019)

Automated IoT device profiling with the Physics Lab (Johns Hopkins, 2018)

Physical forensics from IoT devices (Johns Hopkins 2017)

Network Security

Web security, cookies, XSS, XSRF training modules (UT Austin, 2023-)

Phishing samples analysis (Crimson Vista, 2022-2023)

WiFi transmission analysis, packet capture (Crimson Vista, 2023-)

Security-Focused Data Discovery Methods and Practice (Crimson Vista, 2022-2023)

Analysis of weaknesses in two-factor authentication (Crimson Vista, 2022-2023)

Secure distributed computing (Curuvar, 2021-2023)

Hadoop deployment and security considerations (Crimson Vista, 2021-2022)

SSO technology evaluation and test (UT Austin, Crimson Vista, 2021-2022)

Information risk assessment with respect to data breach (Crimson Vista, 2020-2021)

Data breach analysis with respect to password authentication (Crimson Vista, 2020-2021)

Network security curriculum design for Law and Policy (University of Texas at Austin, 2020-)

Network security curriculum design for undergraduates (University of Texas at Austin, 2020-2021)

Network security curriculum design (Johns Hopkins, 2013-2019)

Security analysis of financial services vendor for Fortune-100 client (Crimson Vista, 2018-2019)

Analysis of secure e-mail transmission for confidential client (Crimson Vista, 2018-2019)

Cloud storage system security evaluation for confidential client (Harbor Labs, 2015)

Secure gateway security and compliance evaluation for SecurityFirst Corp (Harbor Labs, 2015)

Gateway caching security/privacy engineering (Google, 2005)

Malware and Viruses

Ransomware training modules (UT Austin, 2022-)

Ransomware recovery research and development (Crimson Vista, 2018-2019)

Advanced malware and malware defenses analysis (Johns Hopkins, 2018)

Malware Analysis for Confidential Client (Crimson Vista, 2016)

Privacy

Investigation of location tracking in mobile devices (Crimson Vista, 2021-)

Development of an auditing tool for cookies and other web tracking (Crimson Vista, 2020)

Audit of a large hospital network for cookies and web tracking (Confidential client, 2020)

Development of a privacy curriculum for data architects (Crimson Vista, 2019)

Anonymization of threat indicators with the Applied Physics Lab (Johns Hopkins, 2017)

Analysis of anti-piracy vendor for Center for Copyright Information (Harbor Labs, 2013-2014)

Miscellaneous Security Technologies

Distributed ledger technology for secure state replication (Curuvar, 2021-2023)

Blockchain technology for sale and/or licensing of intellectual property (Crimson Vista, 2021-2022)

Blockchain technology analysis for a start-up (Crimson Vista, 2019-2020)

Analysis of cyber security norms for a confidential Fortune 100 client (Crimson Vista, 2018-2019)

Analysis of vulnerabilities in portable chemical manufacturing system (Johns Hopkins, 2018)

Open-Source Contribution and Sponsorship for The PyPy Project (Crimson Vista, 2018-2019)

Blockchain and smart contract design for confidential start-up (Crimson Vista, 2018)

Medical device system security evaluation for confidential client (Harbor Labs, 2015)

Software Engineering and Software Analysis

Review of development practices, error handling, and robustness (Crimson Vista, 2023-)

Open-source licensing analysis, build, and test (Crimson Vista, 2023-)

GitHub analysis and statistics for effort estimation (Crimson Vista, 2022)

Software theft analysis and tool design for various clients (Crimson Vista, 2018-)

Cyber insurance investigations for Clyde & Co (Crimson Vista, 2018-2019)

Distributed code coverage analysis tool for a confidential Fortune 100 client (ISE, 2011)

Software engineering for Metrowerks Inc. (2001-2003, formerly Lineo Inc.)

Publications

Books

Seth James Nielson, *Discovering Cybersecurity: A Technical Introduction for the Absolute Beginner*. (December 2023).

Seth James Nielson, Christopher K. Monson, *Practical Cryptography in Python, Learning Correct Cryptography by Example*. (October 2019).

Refereed Publications

Joseph Kosturko, Eric Schlieber, Sean Futch, Seth James Nielson, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices*. In *Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security*. (September 2018)

Chanyang Shin, Prerit Chandok, Ran Liu, Seth James Nielson, Timothy Leschke, *Potential Forensic Analysis of IoT Data: An Overview of Amazon Echo, Z-wave, and Home Router Data Extraction and Analysis*. In *Proceedings of the 2017 IEEE International Conference on Internet of Things (iThings)*, Exeter, UK, pp. 705-710 (June 2017).

Seth James Nielson, *PLAYGROUND: Preparing Students for the Cyber Battleground*. *Computer Science Education*, volume 26, issue 4, pp. 255-276, (January 2017).

Seth James Nielson and Charles D. Knutson, *Design Dysphasia and the Design Patterns Maintenance Cycle*. *Information & Software Technology*, volume 48, number 8, pp. 660- 675, (August 2006)

Seth James Nielson, Scott S. Crosby, and Dan S. Wallach, *A Taxonomy of Rational Attacks*. In *Proceedings of the Fourth International Workshop on Peer-to-Peer Systems (IPTPS '05)*, Ithaca, New York, (February 2005)

Seth J. Nielson and Charles D. Knutson. *OO++: Exploring the Multiparadigm Shift*. *Proceedings of the Workshop on Multiparadigm Programming with Object-Oriented Languages (MPOOL 2004)*, Oslo, Norway, (June 2004)

Rob Kunz, Seth Nielson, Mark Clement, Quinn Snell, *Effective Bandwidth for Traffic Engineering*, *Proceedings of the IEEE Workshop on High Performance Switching and Routing (HPSR 2001)*, Dallas, TX, (May 2001)

Testimony Before Government Bodies

Testimony in support of *Maryland SB 151/HB 211 Criminal Law - Crimes Involving Computers – Ransomware*. Testimony given to the Judicial Proceedings Committee of the Maryland Senate and the Judiciary Committee of the Maryland House of Delegates (January/February 2019)

Invited Talks, Panels, and Technical Training

Seth James Nielson, *Data Security: Four Approaches to a Better Defensive Posture*, 2023 Enterprise Data World, Anaheim, CA (September 2023)

[CANCELED DUE TO VENUE CHANGE] Seth James Nielson, *Maintaining Data Security and Data Privacy in the 21st Century*, 2022 Enterprise Data World, San Diego, CA (March 2022)

Seth James Nielson, *Securing Your Data Assets Against Hackers*, 2021 Enterprise Data World, Boston, MA. (April 2021)

Seth James Nielson, *The Cybersecurity of IP*, 2020 Essential Cybersecurity Law, Austin, TX (Virtual). (July 2020)

[CANCELED DUE TO COVID 19] Seth James Nielson and Ellie Daw, *Correct Cryptography in Python*, a Tutorial for Cryptography Beginners, PyCon 2020, Philadelphia, PA. (April 2020)

[CANCELED DUE TO COVID 19] Seth James Nielson, *Protecting Your Data Assets*, 2020 Enterprise Data World, Boston, MA. (March 2020)

Seth James Nielson, *Security and Privacy for Data Architects*, 2019 Data Architecture Summit, Chicago, IL (October 2019)

Seth James Nielson, *Crypto Done Right, One Year In. Lessons Learned and Next Steps*. Presented in the International Cryptographic Knowledge Base 2019 (ICMC 2019), Vancouver, Canada (May 2019)

Panel Discussion, *Hardening US Unmanned Systems Against Enemy Counter Measures*. Accepted invitation to 7th Annual DoD Unmanned Systems Summit, Alexandria, VA (April 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2019 Enterprise Data World, Boston, MA (March 2019).

Seth James Nielson, *A Gentle Introduction to Blockchain*. 2018 Data Architecture Summit, Chicago, IL (October 2018).

Seth James Nielson, *Detecting Malicious Sandboxes*. Workshop on Defensive Deception and Trust in Autonomy, San Diego, CA (August 2018).

Seth James Nielson and Debra Baker, *Towards a Crowd-Sourced Cryptographic Knowledge Base*. Presented in the International Cryptographic Knowledge Base 2018 (ICMC18), Ottawa, Canada (May 2018).

Seth James Nielson, *The PyPy Sandbox*. Presented in the National Centers of Academic Excellence Tech Talk, Online (March 2018).

Theses

PhD Thesis: Designing Incentives for Peer-to-Peer Systems (defended 10/2009)

Master's Thesis: OO++ Design Patterns, GOF Revisited (defended 8/2004)

Technical Reports

Seth James Nielson and Dan S. Wallach, *The BitTorrent Anonymity Marketplace*, arXiv Technical Report 1108.2718, (August 2011)

Seth James Nielson, Caleb E. Spare, and Dan S. Wallach, *Building Better Incentives for Robustness in BitTorrent*, arXiv Technical Report 1108.2716, (August 2011)

Seth James Nielson, Seth J. Fogarty, and Dan S. Wallach, *Attacks on Local Searching Tools*, arXiv Technical Report 1108.2704 (Originally produced in December, 2004, available on arXiv as of August 2011)

White Papers and Trade Publications

Seth James Nielson, *Techniques for Discovering Unauthorized Copying in Software*, Crimson Vista White Paper, (January 2022)

Aviel D. Rubin, Seth J. Nielson, Christopher K. Monson, *Evaluation of the MarkMonitor AntiPiracy System*, Produced for the Center for Copyright Information (December 2013)

Aviel D. Rubin, Seth J. Nielson, Sam Small, Christopher K. Monson, *Guidelines for Source Code Review in Hi-Tech Litigation*, Harbor Labs White Paper (September 2013)

Undergraduate Advising

Independent Research and Capstones (University of Texas Austin)

Andrew Dang, *Individual Voice Recognition using Machine Learning*, CS 370, Independent Study,

Summer 2023

Monique Tran, *Malware Classification with SVM*, CS 370, Independent Study, Summer 2023

Gonzalo Tamariz-Martel Sánchez, *SMART CONTRACTS: Different approaches to introduce external (off-chain) data* (June 2022)

Graduate Advising

Capstones for Masters of Science in Security Informatics (Johns Hopkins)

Weizhou Wang, Runjie Zhang, *Research on defense next-generation malware on the Windows platform* (December 2018)

Yu-Tsern Jou, Ying Liu, Menghan Bai, *Open Source HSM Side Channel Analysis* (December 2018)

Bowen Shi, Hong Ma, Mengqi Qin, *Side Channel Attack on HSM Based on Machine Learning* (December 2018)

Dylan Richmond, Matthew Shonman, Jingcheng Yang, *An Exploration of the Usability of HTTPS* (December 2018)

Steven Cheng, Venkata Aditya Bollapragada, and Antara Sargam, *Using Selective RAM Journaling to Fight Ransomware* (December 2018)

Yongqiang Fan, Haiwen Sun, *Fault Tolerance System for IoT* (December 2018)

Weike Chen, Harry Luo, Prashanth Venkateswaran, *IoT Discovery* (August 2018)

Joseph "Jay" Kosturko, Eric Schlieber, Sean Futch, *Cracking a Continuous Flow Reactor: A Vulnerability Assessment for Chemical Additive Manufacturing Devices* (May 2018)

Chao Lei, Wenjun Li, *Anti-Honeypot Detection in Advanced Botnet Attacks* (December 2017)

Ritvik Sachdev, Purushottam Kulkarni, Praveen Malhan, *Securing ADS-B Based Airborne Collision Avoidance Systems* (December 2017)

Ningyuan Bao, Mengying Hu, *Security-Testing-Orientated Internet of Things(IoT) Simulator* (December 2017)

Zehuan Li, Shanshan Yang, Liangjia Fu, *AIS Data De-anonymization* (December 2017)

Chanyang Shin, Prerit Chandok, Aurin Chakravarty, *Forensic Data Collection from IoT Devices* (December 2017)

Kevin Manzotti, Kashif Memon, Rahul Durgad, *Replication of CryptoDrop* (December 2016)

Harshneel More, Jingmiao Wang, Yuanqi Zhu, *Detecting XSS attacks using BRO IDS* (December 2016)

Asmaa Aljohani, Gyan Namdhari, Yue Zhu, *Feasibility, Security and Privacy Analysis of EMVCo Payment Tokenization Technology for Identity Enabled Transactions* (December 2016)

Richard Eaton, *The Emperor Has No Friends: Identifying Botnet Customers and Mapping Out Botnets on Twitter* (May 2015)

Jingru Chen, Yaning Liu, Yifan Yu, Zhiyue Zu, *Investigating the Heartbleed Vulnerability* (2015)

Kartik Thapar, *Security Techniques for Developing iOS Applications* (February 2015)

Jie Feng, Jianxiang Peng, Likai Zhang, *De-anonymizing BitCoin* (January 2014)

Teaching

University of Texas at Austin

Cybersecurity Tech/Law Policy (2020-)
Network Security and Privacy (2020-2021)

Johns Hopkins University

Advanced Network Security (2017 - 2019)
Network Security (2014 – 2019)

Rice University

Data Structures and Algorithms (Spring 2008)

Patents

Co-inventor: Nielson, S. 2021. Distributed Authentication Between Network Nodes. U.S. Patent 11,032,252 filed January 2, 2019 and issued June 8, 2021.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,372 filed November 24, 2010 and issued June 3, 2014.

Co-inventor: Orsini, R. 2014. Systems and methods for security data in motion. U.S. Patent 8,745,379 filed August 20, 2012 and issued June 3, 2014.

Co-inventor: O'Hare, R. 2014. Systems and methods for security data. U.S. Patent 8,677,148 filed January 27, 2012 and issued March 18, 2014.

In the News

"Johns Hopkins Researchers and OnBoard Security Team Up to Protect Drones," *Robotics Tomorrow*, 3/16/2018

"Rice University Computer Scientists Find a Flaw in Google's New Desktop Search Program." *New York Times*, 12/20/2004

Employment History

University of Texas at Austin
2020-

Adjunct Assistant Professor

Source Code Discovery, LLC.
2019-2021

Founder and Partner

Crimson Vista, Inc.

2016-Present

Founder and Chief Scientist

Johns Hopkins Applied Physics Lab

2018-2019

Senior Professional Staff (Temp/On-Call)

Johns Hopkins University

2016-2019

Director of Advanced Research Projects

2015-2019

Adjunct Associate Research Scientist

2014

Lecturer

Harbor Labs, LLC

2014-2015

Principal

2011-2014

Research Scientist

Independent Security Evaluators

2010-2011

Senior Security Analyst

2005-2009

Security Analyst

Google, Inc.

2005

Summer Intern

Metrowerks (Formerly Lineo, Inc.)

2001-2003

Software Engineer II

Expert Testimony

On behalf of Dennis Zeedyk in the United States vs. Dennis Zeedyk (2023-Present)

Counsel: Saul Euwing

Venue: Northern District of Indiana South Bend Division

Subject Matter: Website Forensics

Reports: 1 report November 2023

On behalf of OpenAI in OpenAI v Open Artificial Intelligence and Guy Ravine (2023-Present)

Counsel: Quinn Emanuel

Venue: Northern District of California

Subject Matter: Forensic investigation of website and related assets

Reports: 1 report October 2023

On behalf of Palo Alto Networks in Centripetal Networks v Palo Alto Networks (2021-Present)

Counsel: Norton Rose Fulbright and Ropes & Gray

Venue: Eastern District of Virginia

Subject Matter: Network security devices

Reports: 3 reports issued August 2023, September 2023, and October 2023

Deposition: October 2023

On behalf of Anchor Semiconductor in Elite v. Anchor (2022-Present)

Counsel: Venable
Venue: Northern District of California
Subject Matter: Forensic investigation of alleged sabotage and data destruction
Reports: 1 report July 2023

On behalf of Unified Patents in Ex Parte Reexamination of U.S. Patent 9,438,614

Counsel: Unified Patents
Venue: PTAB
Subject Matter: Machine learning and intrusion detection systems
Reports: 1 declaration Apr 2023

On behalf of Trend Micro in Trend Micro v. TaaSera Licensing (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 4 declarations Apr 2023

On behalf of Salesforce in WSOU Investments v. Salesforce (2022-Present)

Counsel: Quinn Emanuel
Venue: Western District of Texas
Subject Matter: Source code related to transmission of marketing emails
Reports: March 2023
Deposition: August 2023

On behalf of Trend Micro in Trend Micro v. Webroot (2022-Present)

Counsel: Marbury Law Group
Venue: PTAB
Subject Matter: Security technologies and devices (various)
Reports: 5 declarations Feb-Mar 2023, 5 declarations September 2023

On behalf of Fox News in Dominion Voting Systems v. Fox News (2022-2023)

Counsel: Winston and Strawn
Venue: Superior Court of the State of Delaware
Subject Matter: Voting machine security including forensic investigation
Reports: 1 Report December 2022
Deposition: February 2023

On behalf of Public Storage in Estch v. Public Storage (2022-2023)

Counsel: Orrick
Venue: Eastern District of Texas
Subject Matter: VoIP, authentication, authorization
Reports: 1 Report January 2023
Deposition: January 2023

On behalf of Lenovo/Motorola Mobility in Maxell Ltd v. Lenovo/Motorola Mobility (2022-2023)

Counsel: Kirkland and Ellis
Venue: ITC
Subject Matter: Authentication
Reports: 1 Declaration November 2022

Deposition: 2 Reports February 2023
March 2023

On behalf of Elon R Musk in Twitter Inc v. Elon R Musk (2022)
Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Court of Chancery of the State of Delaware
Subject Matter: Evaluation of Security in light of Whistleblower Report
Reports: 1 Report October 2022

On behalf of Bissell, Inc. in Bissell Inc. v. Tineco Intelligent Technology Co. Ltd., (2022)
Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: ITC
Subject Matter: Forensic evaluation of source code
Reports: 1 Report submitted September 2022
Deposition: November 2022
In Court: December 2022

On behalf of Hakkasan USA in Hakkasan USA v Endurance American Specialty Insurance (2022)
Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: District of Nevada (Clark County)
Subject Matter: Forensic evaluation of emails
Reports: 1 Report submitted May 2022
Deposition: July 2022

On behalf of JTC in Seimens vs JTC (2021-2022)
Counsel: Peckar and Abramson, PC
Venue: American Arbitration Association
Subject Matter: Software Engineering Efforts
Reports: 1 Report submitted in July 2021
1 Report submitted in September 2021
Deposition: October 2021
In Court: March 2022 (arbitration)

On behalf of Samsung in Samsung v. Proxense (2021-2022)
Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Western District of Texas (Waco)
Subject Matter: Authentication, Authorization, Device-to-device
Reports: 1 declaration submitted October 2021
Deposition: October 2022

On behalf of Bitglass in Netskope, Inc. v. Bitglass Inc. (2021-2022)
Counsel: Irell and Manela, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Authentication, Single-Sign-On
Reports: 1 declaration submitted September 2021
1 declaration submitted March 2021

On behalf of The State of Arizona in Arizona v. Google (2021-2022)
Counsel: Ruttenberg IP Law

Venue: Superior Court of the State of Arizona (Maricopa)
Subject Matter: Privacy, Location tracking, Data collection
Reports: 1 declaration submitted August 2021

On behalf of TLC in TLC v. Koninklijke Philips N.V., US Philips Corporation (2019-2021)

Counsel: Perkins Coie LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Cryptographic protocols
Reports: 1 declaration submitted February 2021

On behalf of Magic Micro in Monsoon v. Magic Micro (2020-2021)

Counsel: Gutnicki, LLP
Venue: International Centre for Dispute Resolution
Subject Matter: Blockchain, file storage
Reports: 1 declaration submitted October 2020
1 declaration submitted November 2020
In Court: In arbitration December 2020

On behalf of Juniper in Juniper Networks Inc. v. Huawei Digital Technologies Co. (2020-2021)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Network perimeter defense against malware
Reports: 1 declaration submitted June 2020
1 declaration submitted July 2021
Deposition: April 2021

On behalf of DivX in Netflix v. DivX (2020-2023)

Counsel: Lowenstein & Weatherwax, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Encryption of streaming media
Reports: 1 declaration submitted May 2020
1 declaration submitted December 2020
1 declaration submitted April 2021
Deposition: January 2021, February 2021

On behalf of Juniper in Juniper Networks Inc. v. Implicit LLC (2019-2020)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Packet classification
Reports: 1 declaration submitted February 2020

On behalf of the Dealership class in Dealer Management Systems Antitrust Litigation (2019-Present)

Counsel: Milberg Phillips Grossman LLP
Venue: Case No. 18-cv-00864 (Northern District of Illinois)
Subject Matter: Cybersecurity, risk assessment, third-party access
Reports: 1 report submitted November 2019
Deposition: January 2020

On behalf of Symantec in the Trustees of Columbia University in the City of New York v. Symantec Corporation. (2018-2022)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. Civil Action No. 3:13-cv-00808-JRS (Eastern District of Virginia)
Subject Matter: Deception technologies, Honeypots
Reports: 1 report submitted October 2019
Deposition: January 2020

On behalf of Proofpoint in Proofpoint Inc. v. Vade Secure (2019-2021)

Counsel: Quinn Emanuel Urquhart & Sullivan, LLP
Venue: Case No. 3:19-cv-04238 (Northern District of California)
Subject Matter: Cloud-based email, malware detection, AI
Reports: 1 report submitted September 2019, 1 report submitted December 2019
1 report submitted February 2021, 1 report submitted April 2021
Deposition: April 2021
In Court: Expert testimony August 2021

On behalf of Bitdefender in Finjan Inc. v. BitDefender Inc. (2018-2021)

Counsel: Susman Godfrey LLP
Venue: Case No. 4:17-cv-4790-HSG (Northern District of California)
Subject Matter: Web threat detection, malware, gateways
Reports: 1 report submitted July 2019, 1 report submitted August 2019
Depositions: October 2019

On behalf of HTC in Koninklijke Philips N.V., US Philips Corporation v. HTC Corp., HTC America Inc. (2019-2020)

Counsel: Perkins Coie LLP
Venue: Case No. 4:18-cv-01887-HSG (Northern District of California)
Subject Matter: Cryptographic protocols
Reports: 1 report submitted May 2019, 1 report submitted June 2019
Depositions: August 2019

On behalf of Juniper in Juniper Networks Inc. v. Finjan Inc. (2018-2019)

Counsel: Irell and Manella, LLP
Venue: PTAB Petition for Inter Partes Review
Subject Matter: Malware, firewall/gateway, network security
Reports: 4 declarations submitted October 2018
Depositions: June 2019

On behalf of Redbox in Disney Enterprises, Inc., LucasFilm Ltd, LLC, and MVL Film Finance LLC v. Redbox Automated Retail, LLC. (2018)

Counsel: Robins Kaplan LLP
Venue: Case No. 2:17-cv-08655-DDP (AGRx) (Central District of California, Western Division)
Subject Matter: DRM, cloud security, media streaming
Reports: 1 declaration submitted May 2018

On behalf of Trend Micro in Trend Micro, Inc. v. Security Profiling, LLC (2017-2018)

Counsel: The Marbury Law Group, PLLC

Venue: Inter Partes Review Case No. IPR2017-02191 and IPR2017-02192
Subject Matter: Automated security patches
Reports: 2 declarations submitted September 2017
Depositions: June 2018

On behalf of TeleSign in Twilio Inc. v. TeleSign Corporation (2016-2021, multiple cases)

Counsel: Shook, Hardy & Bacon LLP
Venue: Inter Partes Review Case No. IPR2016-01688, IPR2016-00360, IPR2017-01976 IPR2017-01977, IPR2017-01978
Case No. 5:16-cv-6925-LHK (Nor. District of California, San Jose Div.)
Subject Matter: Telecommunications security
Reports: 1 declaration submitted August 2016, May 2017, and July 2017
Depositions: November 2016, July 2017, August 2017

On behalf of Blue Coat in Finjan Inc. v. Blue Coat Systems LLC (2017-2018)

Counsel: Originally Wilson, Sonsini, Goodrich and Rosati PC; later Morrison & Foerster LLP
Venue: Case No. 15-cv-03295-BLF-SVK (Nor. District of California, San Div.)
Subject Matter: Firewalls, gateway, security devices, malware
Reports: 1 report submitted April 2017
Depositions: April 2017
In Court: Tech tutorial February 2017, expert testimony November 2017

On behalf of Sedosoft in Sedosoft Inc. v Mark Burchett LTD and NFSx9 LLC (2016)

Counsel: McInnes and McLane LLP
Venue: Case No. Civil Action No. 1:15-cv-10244-RGS (District of Massachusetts)
Subject Matter: Code theft
Reports: 1 report submitted May 2016 and August 2016

On behalf of USAA in Asghari-Kamrani, et al. v. United Services Automobile Association, Inc.

Counsel: Fish and Richardson PC
Venue: Inter Partes Review Case No. IPR2015-01842, and CBM2016-00063, CBM2016-00064
Subject Matter: Applied cryptography, authentication
Reports: 1 report submitted September 2015, 1 report submitted April 2016
Depositions: March 2017

On behalf of WTS Paradigm in WTS PARADIGM, LLC v EDGEAQ, LLC (2015-2016)

Counsel: Quarles & Brady LLP
Venue: Case No. 3:15-CV-330 (Western District of Wisconsin)
Subject Matter: Software-assisted product configuration, presentation, and ordering
Reports: 1 report submitted March 2016
Depositions: April 2016

On behalf of Mr Leon Stambler in Mr. Leon Stambler v Mastercard IPR (2015-2016)

Counsel: Flachsbart & Greenspoon, LLC
Venue: CBM2015-00044
Subject Matter: Authentication, authentication codes
Reports: 1 declaration submitted October 2015

Deposition: December 2015

On behalf of Trusteer/IBM in Trusted Knight Corporation v. International Business Machines Corporation and Trusteer, Inc. (2015)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: C.A. No. 14-1063 LPS-CJB (District of Delaware)
Subject Matter: Key logging, protections against
Reports: 1 declaration submitted July 2015

On behalf of Sensus in Sensus USA, Inc. v. Certified Measurement, LLC (2015)

Counsel: Feldman Gale PA
Venue: Inter Partes Review Case No. IPR2015-01262, IPR2015-01311, IPR2015-01439, IPR2015-01454
Case number 3:14-cv-01069 (District of Connecticut)
Subject Matter: Applied cryptography, certification of data
Reports: 1 declaration submitted June 2015, 4 declarations submitted July 2015

On behalf of Chad Eichenberger in Chad Eichenberger v. ESPN (2015)

Counsel: Edelson PC
Venue: Case No. 2:14-cv-00463 (Western District of Washington)
Subject Matter: Consumer privacy
Reports: 1 declaration submitted January 2015

On behalf of Optimum Content Protection in Microsoft Corporation v. Optimum Content Protection LLC. (2014)

Counsel: Sidley Austin LLP
Venue: Inter Partes Review No. IPR2015-00048
Subject Matter: DRM, data streaming, protection
Reports: 1 declaration submitted October 2014

On behalf of Fortinet in Fortinet v. Sophos (2014-2015, multiple cases)

Counsel: Quinn Emanuel Urquhart & Sullivan LLP
Venue: Inter Partes Review No. IPR2015-00618
Case No. 3:13-cv-05831-EMC (DMR) (Nor. District of California, SF div.)
Case No. 1:14-cv-00100-GMS (District of Delaware)
Subject Matter: Antivirus, anti-malware
Reports: 2 declarations submitted September 2014, 1 submitted September 2015
1 report submitted October 2015, November 2015
Depositions: October 2014, October 2015
In Court: Tech tutorial December 2015

On behalf of Afiliis in Afiliis PLC v Architelos Inc and Alexa Raad (2015)

Counsel: Haynes Boone LLP
Venue: Case No. 1:15-cv-00014-LMB-JFA (Eastern District of Virginia)
Subject Matter: Domain name system anti-abuse
Reports: 1 report submitted April 2015, May 2015
Depositions: June 2015
In Court: Expert testimony August 2015

On behalf of Telit in M2M v. Motorola, Telit (2015-2016)

Counsel: Pearl Cohen Zedek Latzer Baratz LLP
Venue: Case No. 12-033-RGA (District of Delaware)
Subject Matter: Authentication
Reports: 1 declaration submitted May 2014,
1 report submitted July 2014, August 2014
Depositions: June 2015

On behalf of Rmail/Rpost in Rmail Limited, v. Amazon.com, Inc., and Paypal and Rmail Limited, Rpost Communications Limited, and Rpost Holdings Inc., v. Docusign, Inc. (2013-2014)

Counsel: Hudnell Law Group PC
Venue: Case No. 2:10-CV-258-JRG (Lead Case)
Case No. 2:11-CV-299-JRG (Member Case) (E.D. Texas)
Subject Matter: Email security
Reports: 2 reports April 2013, 1 declaration June 2013
Depositions: May 2013 (2 days)

On behalf of Via Vadis in Via Vadis v. Skype (2012-2014)

Counsel: WTP Law
Venue: Via Vadis v. Skype, Case No. 11-507 (RGA) (District of Delaware)
Subject Matter: P2P communications
Reports: 1 affidavit December 2012