

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE, INC.,
Patent Owner.

Case IPR2023-00656
Patent 10,713,366

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.....	3
A.	Overview	3
V.	LEGAL STANDARDS.....	9
A.	Burden of Proof	9
B.	Anticipation and Obviousness.....	10
1.	Anticipation.....	10
2.	Obviousness.....	11
C.	Independent Claims and Dependent Claims	14
D.	Claim Construction.....	15
VI.	LEVEL OF ORDINARY SKILL IN THE ART	16
VII.	BACKGROUND	18
A.	Priority Date of the ‘366 Patent.....	18
B.	Overview of the ‘366 Patent.....	18
C.	File History of the ‘366 Patent	24
VIII.	SUMMARY OF REFERENCES	25
A.	U.S. Patent No. 11,200,228 (“Keenan”)	25
B.	U.S. Patent No. 10,503,907 (“Zheng”)	30
C.	U.S. Patent Pub. 2014/0236665 (“Baker”).....	31

D.	U.S. Patent No. 9,602,529 (“Jones”).....	31
E.	U.S. Patent No. 10,681,068 (“Galliano”).....	31
IX.	CLAIM CONSTRUCTION.....	32
A.	“Threats”.....	32
B.	“Threat Model Components”	39
C.	“Visual Representations of the Threat Model Components”	40
D.	“Mapping Files”	42
X.	SUMMARY OF OPINIONS.....	43
XI.	OPINIONS CONCERNING THE CHALLENGED CLAIMS	44
A.	Ground 1: Keenan Does Not Anticipate the Challenged Claims	44
1.	Keenan Does Not Disclose the Claimed “Threats”	44
2.	Keenan Does Not Disclose the Other “Threat” Claim Terms Including “Threat Model,” “Threat Model Components,” “Visual Representations of the Threat Model Components,” or “Threat Report”	54
3.	Keenan Does Not Disclose Dependent Claims 2, 3, 9, 10, 17, or 18.....	55
4.	Keenan Does Not Disclose Dependent Claim 5	58
5.	Keenan Does Not Disclose Claims 6 and 14	60
B.	Ground 2: Alleged Obviousness of Claims 1-4, 7-11, 15-18 over Zheng In View of Baker and Jones	61
C.	Grounds 3-5: Alleged Obviousness of: (1) Claims 2, 9, and 17 over the Combination of Zheng, Baker, Jones, and Galliano (<i>i.e.</i> , Ground 3); (2) Claims 1–20 over the Combination of Zheng, Baker, Jones, and Keenan (<i>i.e.</i> , Ground 4); and (3) Claims 2, 5-6, 9, 12–14, 17, and 19-20 over the Combination of Zheng, Baker,	

Jones and “the knowledge of a POSITA” (<i>i.e.</i> , Ground 5)	64
XII. CONCLUSION	66
XIII. AVAILABILITY FOR CROSS-EXAMINATION	66
XIV. RIGHT TO SUPPLEMENT	67
XV. DECLARATION	67

EXHIBITS

Exhibit No.	Description
EX-2001	Patent Owner's December 4, 2023 Power of Attorney
EX-2002	Transcript of Robert Hurlbut Deposition taken December 18, 2023
EX-2003	CIO Article dated August 23, 2016
EX-2004	Draft NIST Special Publication 800-154 entitled "Guide to Data-Centric System Threat Modeling," March 2016
EX-2005	Excerpts from <i>Measuring and Managing Information Risk, A FAIR Approach</i> , by Jack Freund and Jack Jones, 2015
EX-2006	NIST Special Publication 800-30, Rev. 1, entitled "Guide for Conducting Risk Assessments, Sept. 2012
EX-2007	Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, April 6, 2015
EX-2008	Excerpts from <i>Threat Modeling</i> by Frank Swiderski and Window Snyder, 2004
EX-2009	Declaration of Seth James Nielson

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. 10,713,366 (“the ‘366 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 '366 Patent (EX-1001) and its prosecution history (EX-1002), IriusRisk's petition (Paper 1) and its associated exhibits, including U.S. Patent No. 11,200,228 ("Keenan") (EX-1004), U.S. Patent No. 10,503,907 ("Zheng") (EX-1005), U.S. Patent Pub. No. 2014/0236665 ("Baker") (EX-1006), U.S. Patent No. 9,602,529 ("Jones") (EX-1007), U.S. Patent No. 10,681,068 ("Galliano") (EX-1008); ThreatModeler's preliminary response and associated exhibits (Paper 6); the Board's institution decision (Paper 7); and the transcript of Mr. Robert Hurlbut's December 18, 2023 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.

V. LEGAL STANDARDS

26. 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

27. 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

28. 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.”

29. 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

30. 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.

31. 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.

32. 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

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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

41. 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

42. 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.

43. 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.

44. 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.

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

46. 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

47. 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.

48. 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.

49. 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.

50. 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 ‘366 Patent

51. The U.S. Patent Application No. 16/542,263 (“the ‘263 Application”) was filed on August 15, 2019. The ‘263 Application issued as the ‘366 patent on July 14, 2020. The ‘263 Application claims priority to four U.S. Provisional Applications, the earliest of which was filed on May 17, 2017.

52. I further 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 ¶ 45). Accordingly, my opinions contained within this declaration are also based on the perspective of a POSITA as of May 17, 2017.

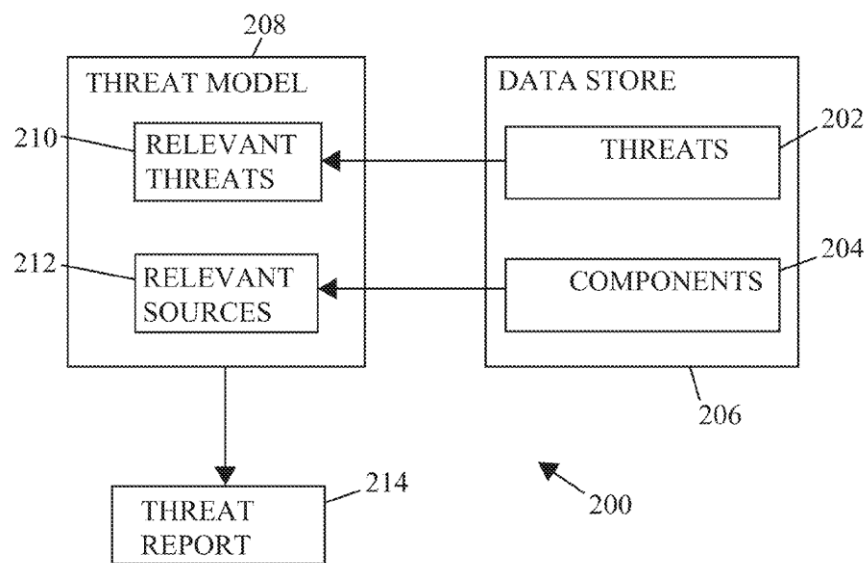
B. Overview of the ‘366 Patent

53. The ‘366 Patent is entitled “Systems and Methods for Automated Threat Model Generation from Third Party Diagram Files” and relates to threat modeling systems and processes. EX-1001, cover page. The ‘366 Patent explains that “[t]hreat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized.” EX-1001, 1:56-57.

54. Threat modeling can be applied to a broad range of environments or activities. EX-1001, 1:62-66. “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, 2:3-7.

55. Figure 2 of the ‘366 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, 8:65-9:1.



56. The ‘366 Patent explains that threat models are created from defined threats and threat model components, which are stored within a database. *Id.*, 9:10-16 (“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.” ’366 Pat., 10:8-12.

“[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.” ’366 Pat., 24:26-32.

57. One obstacle to widespread use of threat modeling techniques and tools has been creation of the threat model objects and relationships between the objects within the context of a threat model, i.e. creation of the threat model itself, which can be a laborious project (especially within large and complicated systems, such as networked enterprise computing platforms.

58. Typically, an enterprise will have some sort of model of their computing platforms, such as for inventory, troubleshooting, and the like. However, such reports lack information relating to threats and threat relationships between elements. As noted at ’366 Pat., 2:47-49 “[s]oftware exists for converting a diagram file of one type to another type of diagram file, though not into a threat model.” In other words, at the time of filing the ’366 patent there was a need for a tool to convert existing diagrams into threat models that include the necessary elements and relationships of threat models. The challenged claims are directed generally to a software-based threat modeling system or method that “may be able

to take any diagram, in any file format, and convert it into a threat model.” ’366 Pat., 43:9-11.

59. As noted by Petitioner, conventionally, specific diagrams, such as Data Flow Diagrams, were required to produce a threat model. The Data Flow Diagram at EX-1003, Paragraph 35, is specific to the use case and requires identifying Actors, Processes, Data Stores or Assets, and Data Flows of the specific use case. *See* Petition at pp. 5-6. Petitioner states that “[t]he Data Flow Diagram helps identify potential threat actors (Customer, Thief) and various countermeasures to create an initial threat model known in the art before the ’366 patent’s priority date. EX-2011-2014; EX-1003, ¶¶35-37”. While not incorrect, this statement glosses over the complex process required to create a threat model from a Data Flow Diagram. For example, threats, *i.e.*, potential events that, if they occurred, would have an adverse effect on a specified asset, must be identified and correlated with the assets. Then the threats must be considered within the context of the data flow of the Data Flow Diagram.

60. The claimed invention leverages two novel data structures of: (1) threat model components stored in a database in association with “threats”; and (2) “a mapping file which correlate the threat model components with visual diagram components of a third-party software application. These two data structures, when

used in the claimed manner, provide a mechanism for correlating a visual diagram to threats to thereby allow creation of a threat model from existing visual diagrams (such as network architecture diagrams). Note that the threat model components, as stored in the database are not part of a threat model, but can be correlated to elements in a diagram, to define a threat model.

61. 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.

62. The '366 Patent describes each "threat model component" as "a potential relevant source for one or more threats." EX-1001, 9:55-57. 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, 9:55-59. 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.” ’366 Pat., 24:64-25:1.

63. Similar to the described embodiments above, the challenged claims of the ’366 Patent recite a “database,” and in claim 1, the database comprises, in relevant part, “a plurality of threat model components stored therein; and a plurality of threats stored therein, wherein each of the threats is associated with at least one of the threat model components through the one or more databases.” Independent claims 8 and 16 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.”

64. Further, the ’366 Patent expressly distinguishes between “threats” and the concept of “risk.” “[A]n interface of the system may list the most vulnerable

components in ascending/descending order, along with the risk level for each listed component, the number of total threats to that component, and the number of open or unmitigated threats for that component.” ’366 Pat., 25:8-12. As discussed, a “threat” may be associated with a risk level as disclosed in Figure 8 and the specification, but a risk level is different from a threat. Describing FIG. 8, the ’366 Patent discloses, “The title ‘threats’ is shown near the top of a list of threats which are organized into rows and columns showing each threat's name, risk level, and attached labels.” ’366 Pat., 14:5-9. Exemplary risk levels are relative values, *i.e.*, very high, high, or medium, but risk levels do not disclose threats to the system’s components. ’366 Pat., FIG. 8; 25:20-26.

C. File History of the ‘366 Patent

65. The ‘366 Patent was filed as U.S. Patent Application No. 16/542,263 (“the ‘263 application”) on August 15, 2019. EX-1002. The ‘366 Patent issued on July 14, 2020 after the Examiner found that the cited prior art did not disclose “determining using the one or more computing devices, for the subset of third party diagram components, correlated threat model components as defined in the one or more mapping files,” as recited in the context of claim 1. EX-1002, p.516. The cited art also did not disclose “the one or more mapping files correlating the threat model components with visual diagram components of a third party software

application,” as recited in the context of claim 1. EX-1002, p.517. The Examiner found that the cited art did not disclose the corresponding features of independent claims 8 and 16, and that the dependent claims were patentable because of their dependence from the independent claims. EX-1002, p.517.

VIII. SUMMARY OF REFERENCES

66. I understand that Petitioner requests review of the ‘366 Patent on the following grounds:

Ground	Claims	Statutory Basis	Alleged Prior Art
1	1-20	§102	Keenan
2	1-4, 7-11, 15-18	§103	Zheng in view of Baker and Jones
3	2, 9, 17	§103	The references of Ground 2 in further view of Galliano
4	1-20	§103	The references of Ground 2 in further view of Keenan
5	2, 5-6, 9, 12-14, 17, 19-20	§103	The references of Ground 2 in further view of the knowledge of a POSITA

Petition, 12.

A. U.S. Patent No. 11,200,228 (“Keenan”)

67. 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 makes this clear in the specification:

Design of object classifications is suited to capture the properties of the information assets in a way that associates the risk, cost, quality, accountability of the assets to the product chain that produces calc[ulation]s which the business utilizes to *set premiums and reserves, manage investment risk and produce financial reports and compliance reports.*

Keenan, 1:33-38 (emphasis added).

68. Keenan refers to the “risk” as a property. Keenan, 1:42 (“[t]hese properties (e.g. costs, risks and accountability)”). Keenan also refers to the risk as a “value.” For example, in Table 3 in its specification, Keenan discloses that the PALETTE view name includes an option called Model Risk. Keenan, 14:32-38. Under this view and option, an object shape’s color is “based on the *value* of the risk characteristics for the models in the view.” *Id.* (emphasis added). Keenan also

refers to “risk” as a characteristic that is “preset.” Keenan, 16:4-5. Keenan views may “fill[] the object shapes based on the *value* of the technical risk ranking characteristics of that object.” Keenan, 16:21-23 (emphasis added). These portions of Keenan make it clear that “risk” in Keenan is a preset value as property of an object. Keenan does not identify any “threats” as claimed.

69. Keenan further teaches that “risk” can be calculated based on a predetermined “metric.” Keenan teaches that:

The GUI also preferably includes an option for calculating and displaying the Riskiest Path. The user selects one of the risk metrics and the IOE computes based on pre-loaded formulae the path with the highest risk based on the metric selected by the user. The riskiest path will appear highlighted (e.g., in red) as seen in FIG.

11. A sample list of risk metrics include: Model Risk without exposure; Model Risk with exposure; Data Quality; Ops Risk; Tech Risk; and Aggregated Risk.

EX-1004, 17:44-52. Further, Keenan discloses that a user can “calculate the risk of the selected View,” and even the “Calculate Aggregate risk by View” report “depicts risk values of the objects of the View aggregated based on an *aggregation*

formula.” Keenan, 18:6-8, 18:20-22 (emphasis added).

70. Keenan teaches that different “views” can display colors according to different properties, including the risk level, associated with various objects.

Keenan teaches:

The system may permit user-defined dimensions in the case of special Views. For instance, a shape fill color may represent platform association in the default view, but represent model risk in a specific Palette View (see below). The number of characteristic or sub-class values possible for each visual component is thus limited only by the differences the normal human eye can detect on today’s screens.

EX-1004, 13:16-22. Keenan further states that “[a] shape’s fill color may depict model risk levels in model objects when selecting the model risk palette View.”

EX-1004, 13:41-42 (emphasis added). Similarly, the “Technical Threat Vector” palette View is described as a view in which “color fills the object shapes based on the value fo [sic: of] the technical risk ranking characteristic of that object.” EX-1004, 14:61-63 (emphasis added); also 16:21-23. The Operational Risk palette View is described as “colors fills the object shapes based on the value of operational risk characteristic of the object or its associated control.” EX-1004,

14:64-67 (emphasis added); also 16:27-29. The term “threat level vector” is a value of risk and this terminology was apparently selected only to distinguish from “technical risk” from “operational risk.” Keenan’s “risk” is a risk value or risk level. A POSITA would have understood that a “threat level” is different from a “threat” or a “threat model,” and this is consistent with Keenan’s usage as well.

71. Indeed, Keenan discloses using the risk values in formulas to calculate aggregate risk, therefore confirming that risk is simply a number, and neither discloses nor informs anything about any “threats” as claimed. As disclosed, Keenan allows a user to “calculate the risk of the selected View,” and even the “Calculate Aggregate risk by View” report “depicts risk values of the objects of the View aggregated based on an *aggregation formula*.” EX-1004, 18:6-8, 18:20-22 (emphasis added).

72. Keenan’s alerts can inform an owner of a change in risk, but this is also based on formulas and values, not “threats.” Keenan discloses that “[c]hanges to characteristics can also include formulas that calculate risk parameters based on new raw values put into ... characteristics of one object but flow downstream to other objects.” EX-1004, 20:34-37. “Entire paths are preferably monitored for changes to aggregate characteristics values.” EX-1004, 20:37-38. This disclosure indicates that a risk value or parameter can be changed by a user, *e.g.*, from 5 to 6,

and that new value can require recalculations of the formulas using that value as an input. Keenan's risk is a numeric value as a property or characteristic.

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

73. Although Zheng relates to threat modeling, the portions and teachings from Zheng relied upon in the Petition do not support the conclusion that Zheng discloses certain claim elements of the '366 Patent (*e.g.*, the “mapping files”). As stated in the Institution Decision, Zheng discloses a system comprising “a visualization module for *rendering, on a computer display, a map* with components representative of the suite of software applications and relationships among the software applications,” where “[t]he components are *displayed* in a base layer of *the map*.” Ex. 1005, 1:48–53 (emphases added). Zheng explains that, “by utilizing *a visualization approach like cartography*, application architecture can be represented in a compressible view that enhances security and risk analysis,” and that “*mapping techniques* and concepts can be used *in the context of data visualization* to create a graphical representation of application connectivity and security.” *Id.* at 3:28–34 (emphases added). On its face, Zheng appears to use the term “map” consistently in the context of cartography, *i.e.*, creating a digital view of components and their interconnections (like drawing for someone a map of how computer network components are interconnected). Institution Decision, 25-26.

Zheng does not disclose “mapping techniques” in the context of “correlating” component, specifically correlating claimed “threat model components with visual diagram components of a third party software application.”

C. U.S. Patent Pub. 2014/0236665 (“Baker”)

74. Baker is directed to an “automated risk management system.” EX-1006, ¶1. Baker does not disclose the use of “mapping files,” as argued in the Petition. Instead, Baker stores the “text and shape of each element of the flowchart . . . in the process database 30” and “automatically assign[s] or associate[s] predetermined objectives or controls according to the shapes of the imported flowcharts.” EX-1006, [0025]; *see also id.*, [0009]. Baker simply searches for a flowchart shape without disclosing any “mapping files” providing correlations as recited in the claims.

D. U.S. Patent No. 9,602,529 (“Jones”)

75. Jones discloses that “[t]he reporter may be configured to generate one or more reports from the threat analysis, at least one of which may include an organized arrangement of at least some of the attributes of at least some of the components, data flows or cybersecurity threat.” EX-1007, 6:59-63 (emphasis added).

E. U.S. Patent No. 10,681,068 (“Galliano”)

76. The Petition relies on Galliano for allegedly disclosing the elements of

Claims 2, 9, and 17. In essence those claims recite “wherein the one or more mapping files are not stored in the one or more databases but are stored in the one or more computing devices.” EX-1001, claim 2. The sole portion of Galliano cited by the Petition is Figure 3 which states that the “[m]odel is either stored in a back-end repository (ex. database) or in memory within a computing system.” EX-1008, Figure 3. I find no other portion of Galliano that elaborates further on this statement. The cited portion of Galliano does not disclose “mapping files” or where they may be stored.

IX. CLAIM CONSTRUCTION

77. In the Institution Decision, the Board invited the parties to address the proper construction of the following claim terms: “threats”, “threat model components,” “visual representations of the threat model components,” and “mapping files.” Decision Granting Institution of Inter Partes Review, 12. Each of those terms are addressed below.

A. “Threats”

78. The specification of the ‘366 Patent does not provide an express definition of the word “threat.” Nevertheless, “threat” is a term of art within the field of threat modeling. As explained below, the term “threat” should be construed to mean “one or more potential events that, if they occur, can cause

adverse effects to a target system.”

79. The specification of the ‘366 Patent provides examples of “threats.” For example, Figure 6 shows a list of threat model components under the “components” heading. EX-1001, 11:54-12:26. When a user clicks on one of the components, such as the “login” component, its corresponding properties are shown in the panel on the right hand side. Under the properties heading, the section labeled “threat” shows each of the threats that correspond to the “login” component. In this case, the “login” threat model component has the following threats: inducing account lockout, session hacking, and click jacking. If any of those potential events occur, the event would have an adverse effect on the system.

80. Figure 8 shows a view of the “threats” sub-menu. The threats listed in this figure include buffer overflow, session hijacking, physical theft, etc. Again, if any of those potential threats occur, the threat would have an adverse effect on the system. Note that in Figure 8 that “threats” and “risk” are distinct concepts. A “threat” is a potential event. Whereas “risk” is the potential impact on a system due to a threat that occurs coupled with the likelihood that a threat will occur. The terms “risk” and “risk level” are used synonymously in the ‘366 Patent, as they are typically used in the threat modeling field. In Figure 8, the “risk” for the various threats are categorized as medium, high, or very high. There is not necessarily a

one-to-one correspondence between “threats” and “risk.” Indeed, the same threat can have different risk levels depending on the system in which the threat may occur. Similarly, knowing the risk level does not identify a particular threat. In Figure 8, a “very high” risk could correspond to any one of six different threats. EX-1001, Fig. 8.

81. Petitioner’s expert agreed that knowing risk does not allow one to necessarily determine the threat that may have caused the risk and that there was not a one-to-one relationship between risk and threats. Mr. Hurlbut testified that:

7 Q. Okay.

8 But if you are just given the

9 risk, can you derive the threat from that?

10 MR. MIDDLETON: Objection.

11 Form.

12 A. You have -- well, some possible

13 threats. Some possible threats. And I gave

14 an example already. The example I gave was

15 unavailability. I have a risk of

16 unavailability. But what's the threat?

17 Well, the threat could be several things.

18 It could be a denial-of-service attack, it

19 could be the thing I'm relying on is not

20 available to me. So, therefore, I have that

21 risk, and so I don't have exactly a one to

22 one, but I certainly have a pretty good idea
23 of what it could be, so I've narrowed down
24 my possibilities.

EX-2002, 61:8-24; *see also* 64:14-25, 66:2-9.

82. Figures 11 and 12 of the ‘366 Patent also show multiple threats, the potential “source” of those threats (which correspond to the claimed “threat model components”), and the risk associated with each threat in the context of the system being examined. Again, there is not a one-to-one relationship between a threat and its associated risk. Knowing a particular risk (or risk level) does not identify or determine a particular threat.

83. The article “Threat Modeling Approaches for Securing Cloud Computing” was submitted to the Patent Office during prosecution of the ‘366 Patent. EX-1002, 480-495. That article includes definitions of both “threat” and “risk.” “Threat” is defined as “harm or unauthorized access that might occur due to vulnerability and destroy organization assets, organization operations or system information.” EX-1002, 482. The article cites to the Open Web Application Security Project (“OWASP”) in which “risk” is defined as “Risk = Likelihood x Impact.” EX-1002, 493. “Likelihood” is the probability that a threat may occur, and “impact” is the damage that may occur to a system or organization if the threat occurs.

84. The extrinsic evidence is consistent with Patent Owner’s construction of “threat” – *i.e.*, one or more potential events that, if they occur, can cause adverse effects to a target system. For example, the Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-154, Guide to Data-Centric System Threat Modeling (hereafter, “NIST 800-154”), is a well-accepted and widely-consulted standard in the field of threat modeling. EX-2004. NIST 800-154 references NIST Special Publication 800-30 (hereafter, “NIST 800-30”) which defines “threat” as:

any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Emphasis supplied.

EX-2006, B-13 [NIST 800-30]. NIST 800-30 also defines “risk” as:

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a

function of: (i) the adverse impacts that would arise if the
circumstance or event occurs; and (ii) the likelihood of
occurrence.

EX-2006, B-9 [NIST 800-30]. Using these definitions, a “threat” is the
“circumstance or event.” The “risk” is the “measure of the extent to which an
entity is threatened” by the threat. “Risk” is a function of the impact of the
potential threat (if it were to occur), and the likelihood that the threat may occur.
See also EX-2007 at p.104 and p.122 [Committee on National Security Systems
Instruction (CNSSI) 4009, National Information Assurance (IA)] (same definition
of “risk”).

85. Another well-known reference is “Measuring and Managing
Information Risk: A FAIR Approach” by Jack Freund and Jack Jones (“FAIR”).
This book relies on the Factor Analysis of Information Risk (FAIR) standard
(<https://www.fairinstitute.org/>). FAIR notes that “[a] reasonable definition for
threat is anything (e.g., object substance, human, etc.) that is capable of acting in a
manner that can result in harm.” EX-2005 [FAIR], 4. FAIR defines “risk” as
“[t]he probable frequency and probable magnitude of future loss.” EX-2005
[FAIR], 5.

86. Similarly, an August 23, 2016 article in CIO magazine was entitled

“Risk = Likelihood x Impact.” EX-2003 [CIO article].² That article explained that “the total amount of risk exposure is the probability of an unfortunate event occurring, multiplied by the potential impactor damage incurred by the event.” EX-2003 [CIO article], 2. The “event” corresponds to a “threat,” whereas the “risk” is a calculated value that may be derived from a threat assuming that the likelihood and impact of the threat can be determined.

87. Many view the book “Threat Modeling” by Frank Swiderski and Window Snyder as the first authoritative on the topic of threat modeling. EX-2008. While “Threat Modeling” was written several years before the invention of the ‘366 Patent, “Threat Modeling” defines “threat” and “risk” as two separate concepts. “Threat” is defined as “[t]he adversary’s goals, or what an adversary might try to do to a system.” EX-2008, 28. “Risk” is defined as “[a] characterization of the danger of a vulnerability or condition.” EX-2008, 27. While these definitions are not identified for their accuracy in 2017 when the technology of the ‘366 Patent was developed, the definitions are consistent with those proffered by Patent Owner and demonstrate that “threat” and “risk” are distinct concepts.

88. At deposition, Petitioner’s expert, Mr. Hurlbut, testified a “threat” was

² The term “CIO” refers to the Chief Information Officer of an organization.

different from a “risk.” Specifically, Mr. Hurlbut testified that a good definition of “risk” was the likelihood of a threat occurring multiplied by the impact the threat would have if it occurred. EX-2002 [Hurlbut depo], 24:3-25:5, 31:5-33:2. Mr. Hurlbut also testified that knowing the risk does not determine the specific threat that gave rise to the risk. EX-2002 [Hurlbut depo], 61:8-24. Mr. Hurlbut testified that there was not a one-to-one correspondence between a threat and a risk. EX-2002 [Hurlbut depo], 61:8-24.

89. Thus, the extrinsic evidence also supports Patent Owner’s construction of “threat,” and in addition demonstrates how “threat” and “risk” have different meanings. The term “threat” should be construed to mean “one or more potential events that, if they occur, can cause adverse effects to a target system.”

B. “Threat Model Components”

90. The ‘366 Patent describes each “threat model component” as “a potential relevant source for one or more threats.” EX-1001, 9:55-57. 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, 9:55-59. 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.” ’366 Pat., 24:64-25:1.

91. Further, the ‘366 Patent explains that threat model components are not limited to physical components. Components can be steps, actions, or a physical component. EX-1001, 9:65-10:13. 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, 9:66-10:7.

92. Figure 10 of the ‘366 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, 17:36-41.

93. 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, 14; EX-1003, ¶¶40, 60; EX-2002 [Hurlbut depo. Tr.], 20:22-21:25.

C. “Visual Representations of the Threat Model Components”

94. In the prosecution history of the ‘366 Patent, the Examiner issued an

indefiniteness rejection based on the claim 1 recitation of “using visual representations of threat model components correlated with the subset of third party diagram components.” The Examiner stated that his understanding was that “third party diagram components” are visual representations. Thus, the Examiner alleged, a POSITA would not be able to determine how the claimed “visual representations” relate to the “third party diagram components.” EX-1002, 408. In essence, the Examiner argued that it was confusing as to how the claimed “visual representations of threat model components” were correlated with “third party diagram components” which the Examiner understood were also “visual representations.”

95. In response and after an interview, the applicant explained that the “third party components” were distinct elements from the “visual representations of the threat model components.” The “third party diagram components” (or third party components) were components of an independent (*i.e.*, “third party”) software application (*e.g.*, used, for example, in some other system that does not necessarily have anything to do with threat modeling and is not related to the software performing the steps of the claim). The “visual representations of the threat model components” were elements of the “native” software that is performing the steps of the claim. These elements of the “native” software are

used to visually represent potential components of a target system being analyzed.
EX-1002, 505 and 462.

96. The term “visual representations of the threat model components” means “representations of threat model components that can be visually displayed on a diagram.” One of ordinary skill in the art would have readily recognized this based on the disclosure of the ‘366 patent. For example, FIG. 21 of the ‘366 patent illustrates a user interface in which threat model components (such as ETHERNET PORT) are represented visually for manipulation.

D. “Mapping Files”

97. In the context of the claims of the ‘366 Patent, a “mapping file” is “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application.” During prosecution of the ‘366 Patent, the applicant explained that “[t]he mapping file correlates the internal threat model components with the external third party diagram components so that the system can read a file created with the third party software program and generate its own diagram using internal components that are, through the mapping file, correlated to the external third party components.” EX-1002, 506.

98. The ‘366 Patent gives examples of “mapping files.” For example,

Figures 28 and 29 show comma separated value (“CSV”) files that are each “mapping files.” EX-1001, 37:14-18. While these mapping files are CSV files, the claimed mapping files can be in a file format other than CSV. EX-1001, 38:33-34. In addition, the “mapping files” can also be one or more tables in a database or multiple databases. EX-1001, 38:34-36. If the mapping file is not stored in the database, the file can be stored in one of the computing devices (*e.g.*, computers, servers, etc.) that make up the threat modeling system. EX-1001, 38:36-40.

99. The term “mapping file” should be construed to mean “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application.”

X. SUMMARY OF OPINIONS

100. Petitioner, IriusRisk, did not show that any challenged claim is anticipated by Keenan, or would have been obvious over Zheng 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.

101. To summarize:

- It is my opinion that claims 1-20 are not anticipated by Keenan (Ground 1).

- It is my opinion that claims 1-4, 7-11, 15-18 are not obvious based on Zheng in view of Baker and Jones (Ground 2).
- It is my opinion that claims 2, 9, and 17 are not obvious based on Zheng in view of Baker and Jones and in further view of Galliano (Ground 3).
- It is my opinion that claims 1-20 are not obvious based on Zheng in view of Baker and Jones and in further view of Keenan (Ground 4).
- It is my opinion that claims 2, 5-6, 9, 12-14, 17, and 19-20 are not obvious based on Zheng in view of Baker and Jones and in further view of the knowledge of a person of ordinary skill in the art (Ground 5).

XI. OPINIONS CONCERNING THE CHALLENGED CLAIMS

A. Ground 1: Keenan Does Not Anticipate the Challenged Claims

1. Keenan Does Not Disclose the Claimed “Threats”

102. All claims of the ‘366 Patent include various recitations of “threats.”

The preambles of independent claims 1, 8 and 16 each recite a “threat modeling system” or a “threat modeling method.” Each of these claims recites “a plurality of threats” stored in a database. EX-1001, 43:26, 44:29, 45:29. Additionally, “each of the threats is associated with at least one of the threat model components through the one or more databases.” EX-1001, 43:26-29, 44:29-33, 45:29-33.

Further, each independent claim recites “a threat report displaying each threat.”

EX-1001, 43:57-58, 44:61-62, 45:20-21. The term “threat” is obviously an aspect of other claim terms including “threat model,” “threat model components,” and

“threat report” which appear in each of independent claims 1, 8, and 16.

103. Keenan does not disclose threats at all. Keenan is all about viewing and analyzing risk. This makes sense since the assignee of Keenan is the well-known insurance company, American International Group, Inc. or “AIG” for short. As Keenan explains, the purpose of the Keenan system in part is to “capture the properties of the information assets in a way that associates the risk, cost, quality, accountability of the assets to the product [sic: production] chain that produces calcs [i.e., calculated outputs] which the business utilizes to set premiums and reserves, manage investment risk and produce financial reports and compliance reports.” EX-1004, 1:33-38 (emphasis added). It is immaterial to Keenan’s system whether a threat (or group of threats) gave rise to the risk. Keenan is focused on assessing the risk, cost, quality, etc. so that the business can make business decisions such as setting premiums, and determining asset reserves.

104. Keenan also does not expressly or inherently determine a threat that may be associated with the risk. As explained above, risk is a calculated value based on properties (likelihood of occurrence and impact) that may be associated with a threat. Thus, to the extent that one or more threats gave rise to a risk, the risk is a *downstream* product of properties associated with the one or more threats. As I explained above, in the context of a threat, risk is equal to the likelihood of the

threat occurring multiplied by the impact that the threat may have if it occurs.

Keenan starts with the risk and thus, has no need to determine or otherwise know what, if any, threat(s) gave rise to the risk. In Keenan, threats cannot be determined from a risk value.

105. Keenan only mentions the word “threat” two times. In Keenan’s “palette” view, Keenan lists “technical threat vector” as one of the view options. EX-1004, 14:61-63. The “technical threat vector” is described as “color fills the object shapes based on the value fo [sic: of] the technical risk ranking characteristic of that object.” EX-1004, 14:61-63.³ “Risk ranking” refers to one of two things. “Risk ranking” either means a risk value, such as a value between 0 and 100. Alternatively (and less likely), “risk ranking” refers to the amount of risk for a particular object relative to the amount of risk for other objects in the view. In either case, the “technical threat vector” is just a risk ranking and has nothing to do with the identification or determination of a threat associated with the risk. See EX-2002 [Hurlbut depo], 77:5-11 (“technical risk ranking is actually equivalent to a risk level”).

106. In many circumstances (such as those described in Keenan), the risk

³ The second occurrence of “technical threat vector” is the same explanation of what a “technical threat vector” is. EX-1004, 16:21-23.

of a loss can be known without ever determining the threat or threats that may have contributed to the risk. For example, if a company were selling life insurance to individuals who live in a particular county, the insurance company may know that the risk of a person in that county dying in a particular year is one out of one thousand. The insurance company does not know (or even care) what the causes of death are (*i.e.*, the threats). It does not matter that some people died from car accidents, murder, heart disease, cancer, or freak accidents. Each of those threats to life is immaterial to the insurance company who is setting the premium for the life insurance. The company merely needs to know the risk level. That is the point of Keenan.

107. Moreover, knowing the risk to a system alone does not allow one to determine the threat that may have given rise to the risk. In other words, there is no one-to-one correspondence between a risk and a threat. Many different threats can lead to the same risk. Figure 8 of the '366 Patent shows that six different threats have the same "very high" risk level. If one only knew that the risk to the system was "very high," one could not determine which of the six threats led to that risk. Similarly, the same threat can have different risk levels depending on its context. If the threat is physical theft of an automated teller machine ("ATM"), the risk associated with that threat varies depending on where the ATM is located. If

the ATM is located in a sparsely populated area of a city, the risk of the theft occurring can be high compared to the risk of the same ATM being physically stolen from inside a bank lobby that is only open during business hours.

108. When asked about certain texts related to threats and risk, Petitioner's expert said that threats and risk were different concepts. For example, at his deposition, Petitioner's expert, Mr. Hurlbut, downplayed the relevance of the definition of "risk" contained in Exhibit 2005,⁴ Mr. Hurlbut testified that FAIR was "not considered to be a threat modeling book because it looks at risks." EX-2002 [Hurlbut depo.], 44:6-22. Mr. Hurlbut testified that "FAIR is an approach to do risk management, which is a whole other area of security, so, again, I would understand this definition [of risk] in that context as opposed to in relation to threat modeling to somebody with skill in the art in May of 2017." EX-2002 [Hurlbut depo.], 45:6-14.

109. The Petitioner seems to make an inherency argument that Keenan discloses threats. The Petition states that "[a] POSITA would understand that Keenan's 'risk' includes threats because measuring risk includes a determination of threats." Petition, 23. The Petition cites Keenan at 16:40-51 for support. But

⁴ Exhibit 2005 is an excerpt from the book entitled "Measuring and Managing Risk, A FAIR Approach" by Jack Freund published in 2015 ("FAIR").

that portion of Keenan relates to different palette view that show risk levels, including the “technical risk measurement” view. Indeed, the word “threat” does not even appear in that passage. Substantively, that passage relates to different views of risk. The Petition also cites to paragraph 79 of Mr. Hurlbut’s declaration. In that paragraph, Petitioner’s expert makes the point that allegedly a “POSITA would understand that a determination of threats is included within a risk analysis.” EX-1003, ¶79. But as explained above, that is not correct. Knowing risk does not mean that any threat determination occurred, much less knowing what the specific threat was. Neither Petitioner nor its expert provide any reasoned explanation allegedly why “measuring risk includes a determination of threats.”

110. Recall that the claims of the ‘366 Patent require that “a plurality of threats [are] stored” in one or more databases.⁵ Not only does Keenan not disclose a determination of threats, Keenan certainly does not disclose storing a plurality of threats in a database.

111. The Petition and Petitioner’s expert state that “[a] POSITA would understand that Keenan discloses a threat modeling system and method.” Petition, 23, EX-1003, ¶79. That too is incorrect. A POSITA would understand that, at

⁵ This same language appears in all three independent claims – namely, claims 1, 8, and 16.

best, Keenan discloses a risk modeling system/method. See EX-2002 [Hurlbut depo], 89:22-90:5 (testifying that Keenan's Figure 7 discloses a risk model); 90:11-23 (testifying that Keenan's Table 3 describe different types of views to observe a risk model). Keenan's system allows a business to assess system-level risk to determine insurance premiums and asset reserve levels. EX-1004, 1:33-38. Keenan does not disclose threat modeling to a POSITA. That is consistent with Mr. Hurlbut's testimony where he described a threat model as a tool to allow someone deal with threats, not risk. EX-2002 [Hurlbut depo.], 19:8-15.

112. Mr. Hurlbut's declaration states that:

Keenan discloses methods and system of measuring risk through threat modeling by providing "visual depictions" and models of the risk (which includes threats), *i.e.*, through visually depicting threats against IOE objects and creating "Views" through threat vectors, which may be combined with other Views, such as "model risk."

EX-1003, ¶79 (p.40). The Petition contains virtually the same sentence. Petition,

24. Parts of this sentence are correct, and other parts are incorrect. Keenan does disclose a method and system of storing and viewing risk. EX-1004, Abstract.

Keenan does not disclose a system for measuring risk. The risk for objects is determined before the objects are imported into the IOE. Keenan does not make that measurement. Mr. Hurlbut's testimony quoted immediately above, that risk includes threats, is contradicted by his deposition testimony in which he stated that

risk and threats are distinct. EX-2002 [Hurlbut depo], at 19:17-25, 24:11-25:5, 61:8-24. I agree that Keenan discloses “models of the risk.” As I said above, at best Keenan discloses risk modeling. But Keenan does not disclose threat modeling, for the reasons provided above. I disagree that “the risk” “includes threats.” Neither generally nor in the context of Keenan does risk “include threats.” Risk might be based on a threat. But risk does not include a threat and determining risk does not require identifying or determining a threat. I disagree that Keenan “depict[s] threat against IOE objects.” Risk and other characteristics of IOE objects are depicted, but a threat is not depicted. It is also not clear that palette options “model risk” and “technical threat vector” can be combined in a single view. Model Risk is described as “color fills the object shapes based on the value of the risk characteristics for the models in the view.” EX1004, 14:36-39. Technical Threat Vector is described as “color fills the object shapes based on the value [of] the technical risk ranking characteristic of that object.” For Model Risk, the color is based on the “risk characteristics for the models in the view,” whereas for Technical Threat Vector, each object is filled with color based on risk ranking of that object. These descriptions run contrary to each other, thus leading to the conclusion that those two options cannot be combined in a single view.

113. The Petition and Mr. Hurlbut both cite to exhibits other than Keenan

to support the assertion that there is a close connection between risk analysis and threat modeling. Petition, 23-24, EX-1003, ¶79. I understand that for Keenan to anticipate any claims of the '366 Patent, Keenan (and not some other references) must disclose each element of the claim(s). Thus, I believe it is improper to rely on references other than Keenan to assert that Keenan discloses threats because of Keenan's risk-based system.

114. Petitioner argues that “the assets/objects in Keenan are ‘relevant sources of threats’ and thus threat model components, as defined by the '366 patent, because the assets/objects in Keenan are subject to risks that Keenan's system measures.” Pet. 28 (citing EX-1003 ¶82). However, nothing in Keenan describes threats (as demonstrated below) and the fact that the assets are subject to risk that is displayed does not teach, or even suggest a threat determination.

115. In the Institution Decision, the PTAB stated that “Patent Owner then merely concludes, without citing any factual support, that use of a color identifying the generic nature of a risk still fails to disclose any threats associated with the risk.” Institution Decision, p. 18. However, for all of the reasons stated above, the use of color identifying risk levels is not the same as teaching the presence of threats.

116. Petitioner essentially admits that threats are not expressly disclosed in

Keenan. Therefore, while Petitioner and its expert do not expressly argue “inherency,” in order for Petitioner’s argument to succeed, it is my understanding that threat determination and the storage of threats in the claimed manner would have to be inherent in the disclosure of Keenan. This is not the case. In my opinion, Keenan does not inherently disclose threat or the storage and use of threats as explained throughout this declaration.

117. When measuring risk (or displaying risk, in the case of Keenan), it does not necessarily follow that there has been a determination of a threat . Keenan fails to disclose or suggest any “threat” or any database storing threats, as claimed. Rather, Keenan discloses a risk value, which is a number, without identifying or storing any threat as claimed. Further, Keenan fails to disclose storing any threats in a database, as storing a value for a degree of risk is not what is claimed by the ’366 Patent. Even if we were to assume, for the sake of argument, that the Petitioner’s assertion that “measuring risk includes a determination of threats” is correct, such determination does not result in storing or using a threat in the claimed manner.

118. In my opinion, Keenan does not anticipate any of the claims of the ‘366 Patent. Keenan does not disclose threats explicitly or inherently. Keenan relates to analysis of risk. Knowing a particular risk does not determine what

threat, if any, gave rise to the risk. Keenan certainly does not disclose the storing of threats in one or more databases as claimed in the '366 Patent.

2. Keenan Does Not Disclose the Other “Threat” Claim Terms Including “Threat Model,” “Threat Model Components,” “Visual Representations of the Threat Model Components,” or “Threat Report”

119. Because Keenan does not disclose “threats” or the storing of multiple threats, Keenan does not disclose a “threat model,” “threat model components,” “visual representations of the threat model components,” or a “threat report.”

120. Throughout the analysis of Keenan in the Petition and in Mr. Hurlbut’s declaration, Petitioner and Mr. Hurlbut essentially conflate the concepts of “risk” and “threats” to argue that Keenan disclosed the claims of the '366 Patent. For example, with respect to Element 1[b], Mr. Hurlbut states that:

A POSITA would understand that the assets/objects in Keenan are “relevant sources of threats” and thus threat model components because the assets/objects in Keenan are subject to risks that Keenan’s system measures. A POSITA would further understand that “risk” as disclosed in Keenan includes threats because measuring risk includes a determination of threats.

EX-1003, ¶82. Mr. Hurlbut’s conclusion is necessarily based on the incorrect premise that risk somehow determines threats. At best, Mr. Hurlbut’s analysis is conclusory. As explained above, knowing risk does not determine the threat, if any, that caused the risk. The same conclusory analysis is contained in Mr.

Hurlbut's paragraph 83 (and elsewhere in his declaration, *e.g.* ¶106).

121. In his analysis of the preamble, Mr. Hurlbut states that:

A POSITA would understand that “types of risk,” as disclosed in Keenan are threats because the described examples are all types of threats (cyber, environmental, accidental). Thus, Keenan disclosed threats within its risk analysis.

EX-1003, ¶79 (p.38). But Mr. Hurlbut's conclusion ignores the plain language in Keenan. The cited portion of Keenan expressly says that “cyber, environmental, accidental, etc.” are all different types of risk – not threats. EX-1004, 16:45-48. Again, Mr. Hurlbut simply assumes that knowing risk determines a threat or that “risk” is synonymous with “threat.” That is incorrect, as explained above.

122. In my opinion, Keenan does not disclose a “threat model,” “threat model components,” “visual representations of the threat model components,” or a “threat report.” One or more of these terms are used throughout independent claims 1, 8, and 16, and in dependent claims 5, 7, 12-14, and 19-20.

3. Keenan Does Not Disclose Dependent Claims 2, 3, 9, 10, 17, or 18

123. Claim 2 depends from independent claim 1 and recites “wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.” Claim 3 depends from independent claim 1 and recites “wherein the one or more mapping files comprise one or more

tables stored within the one or more databases.” EX-1001, 43:62-67.⁶ Thus, for claim 2, the mapping files cannot be stored in the database(s). But for claim 3, the mapping files’ tables must be stored in the database(s). To the extent these claims recite where the mapping files are stored, these claims are mutually exclusive.

124. Before analyzing claims 2 and 3 themselves, it is useful to go back to the Petition’s and Petitioner’s expert’s analysis of the “mapping files” in claim 1. For Elements 1[c] and 1[d], Petitioner and its expert relied upon two distinct teachings for the “mapping files.” First, the Petition relied on the lone statement in Keenan that “[a] map is preset that maps Visio shapes and formats to IOE shapes and formats.” Petition, 29-30; EX-1003, ¶¶84-88. Second, the Petition relies on “diagrams and ‘Views’ on a Graphical User Interface.” *Id.*

125. It is important to understand that the second aspect of Keenan relied upon in the Petition (*i.e.*, the diagrams and Views) relates to the *topological* relationship among various objects. The diagrams and “View” are different ways of visually looking at objects within a system, their interconnections among the objects, and various information about the objects, such as their risk level. *E.g.*, EX-1004, Abstract.

⁶ Dependent claims 9 and 17, and claims 10 and 18 recite the same limitations as claims 2 and 3, respectively.

126. Keenan contains a set of definitions. “View” is defined in Keenan as “[d]epiction of topology in the IOE via GUI. A view that is exported or printed from the IOE is a ‘Diagram.’” EX-1004, 5:24-25. Keenan defines “topology” as “[r]epresentation of the relationships between objects in an analytical infrastructure.” EX-1004, 5:5-6. Examples of various topological “Views” are shown in Keenan’s Figures 4-11. Each figure shows the relationships among the objects in the View. These “Views” do not show any correlations between “threat model components” and “third party diagram components.” Thus, the various citations to “Views” and diagrams cannot relate to the claimed “mapping files.”

127. It is important to understand that the Views cannot correspond to the mapping files because dependent claims 2 and 3 are directed to where the mapping files (or their tables) are stored. Keenan describes the IOE as residing in a graph database and the Views on the GUI are generated based on information in the IOE. EX-1004, 5:45-49, 1:53-57, 5:24-25. Keenan also says the “all or part of [the] steps of the processes in the preceding embodiments” may be implemented by “computing hardware instructed by a program. The program may be stored in a computer readable storage medium. The storage medium may include a ROM, A RAM, a magnetic disk or a compact disk.” EX-1004, 21:27-33. A POSITA would understand this passage to refer to the application program that implements the

IOE. But Keenan does not describe the location of the “map [that] is preset that maps Visio shapes and formats to IOE shapes and formats,” which is the first Keenan teaching relied upon for the “mapping files.”

128. In an anticipation analysis, I understand that the reference must disclose, expressly or inherently, the location of the claimed “mapping files.” Keenan does not disclose that location. Keenan certainly does not indicate whether the alleged mapping files (or their tables) are stored in a file on a computing device and not in the claimed databases (claim 2), whether the mapping files’ tables are stored in the databases (claim 3), or whether the preset map is stored elsewhere such as in a cloud server.

4. Keenan Does Not Disclose Dependent Claim 5

129. Dependent claim 5 recites that the determination of the threat model components correlated to the third party diagram components comprises “first determining whether a user-defined name for one of the subset of third party diagram components has a match in the one or more mapping files and, if no such match is found, then determining whether a default title for the third party diagram component, as defined by the third party software application, has a match in the one or more mapping files.” EX-1001, 44:4-13 (emphasis added). Thus, claim 5 has a distinct order. The system first checks to see if the user-defined name has a

match, and if not, then the system determines whether a default title has a match.

130. Claim 1 introduces the “subset of the third party diagram components” as being included in the “data file” that is read by the threat modeling system, where the “data file” is “generated by the third party software application,” and “defin[es] one or more relationships between the subset of third party diagram components.” EX-1001, 43:40-45. According to claim 1, reading the “data file” is how the system obtains the “subset of the third party diagram components.” Claim 5 then requires that the system first check for “user-defined name” match, and if no match is found, the system checks for a “default title” match.

131. Keenan works in the opposite order. When importing a file into the Keenan system, the IOE “first checks to see if [the] object already exists in IOE based on external ID number first, then name match.” EX-1004, 18:36-50.

132. Petitioner and its expert argue that Keenan also discloses the opposite order. But that is not true when importing and reading data files from third party applications, such as Visio. The portion of Keenan cited by Petitioner relates to a user manually adding individual objects. EX-1004, 18:36-50. This passage does not relate to “reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components,” as recited in claim 1.

5. Keenan Does Not Disclose Claims 6 and 14

133. Claim 6 depends from claim 5 and recites that “if no match is found for the default title, matching the third party diagram component with a placeholder component and displaying the placeholder component on the relational diagram to indicate that no match was found.” EX-1001, 44:13-17. Claim 14 depends from claim 8 and recites that “for each of the subset of third party diagram components for which no correlated threat model component is found in the one or more mapping files, the diagram interface displays a placeholder component indicative of a match not being found.” EX-1001, 45:15-19.

134. The Petition and its expert cite to Keenan at 13:53-65, 11:7-11, 19:9-16, and Figures 12 and 13. Keenan at 13:53-65, 19:9-16, and Figures 12 and 13 all relate to a user modifying a “typology” and the system categorizing and saving it as a temporary typology. Keenan’s column 11:7-11 relates to searching the IOE and the results being returned and stored in temporary memory. None of these citations relate to displaying a placeholder component showing that one of the subset of third party diagram components did not have a matching threat modeling component in the mapping file. Thus, the cited passages from Keenan have nothing to do with the subject matter of claims 6 and 14. The only connection between the claim language and the cited passages of Keenan appears to be the

word “temporary” (in fact, these are the only uses of the word “temporary” in Keenan) but the actual usage of temporary is unrelated to the subject matter of the claims.

B. Ground 2: Alleged Obviousness of Claims 1-4, 7-11, 15-18 over Zheng In View of Baker and Jones

135. Zheng discloses a system comprising “a visualization module for rendering, on a computer display, a map with components representative of the suite of software applications and relationships among the software applications,” where “[t]he components are displayed in a base layer of the map.” Ex. 1005, 1:48–53. Zheng explains that “by utilizing a visualization approach like cartography, application architecture can be represented in a compressible view that enhances security and risk analysis,” and that “mapping techniques and concepts can be used in the context of data visualization to create a graphical representation of application connectivity and security.” *Id.* at 3:28–34. Zheng uses the term “map” consistently in the context of cartography, i.e., creating a digital view of components and their interconnections (like drawing for someone a map of how computer network components are interconnected).

136. Petitioner and Mr. Hurlbut argue “Zheng’s ‘mapping techniques’ and its ‘map’ convey, and necessarily include, a ‘mapping file’ as claimed because a mapping file would be required to perform mapping techniques.” Pet. 63 (citing

EX-1003 ¶162). However, Zheng’s ‘mapping techniques’ are related to visualization of the application architecture, ‘like cartography,’ and have nothing to do with ‘correlating the threat model components with visual diagram components of a third party software application’ as recited in the claims. Additionally, Zheng’s generic disclosure of ‘mapping techniques . . . in the context of data visualization’ does not necessarily require any ‘mapping files’ as claimed.

137. Petitioner and Mr. Hurlbut then turn to Baker (EX-1006) for allegedly disclosing limitation 1[d], namely, “the one or more mapping files correlating the threat model components with visual diagram components of a third party software application.” Pet. 64–65, EX-1003 ¶164. Baker discloses an “automated risk management system,” where a user is able to build a risk management flowchart (or multiple flowcharts) that “utilizes symbols of various shapes to indicate actions, determinations, or other elements of an activity or evaluation so that respective personnel of an organization can understand actions to be taken to successfully manage an activity or avoid a negative outcome.” EX-1006, ¶¶ 5, 20, 25. “Importantly, risk management or control flowcharts may be imported . . . from third party software such as that marketed as Microsoft Office Visio®.” *Id.* ¶ 25. By relying on Baker for the “correlating” feature, Petitioner acknowledges that Zheng itself does not disclose “mapping techniques” in the context of “correlating”

components in the claimed manner.

138. Petitioner and Mr. Hurlbut argue Baker discloses “visual diagram components of a third party software application” based on its disclosure of importing flowcharts from Visio, discussed above. Pet. 64. Petitioner further alleges that the skilled artisan would have been motivated to combine these teachings from Baker with the system of Zheng “to enable the importation of diagrams from Microsoft Visio into the threat modeling software of Zheng such that the mapping file of Zheng would correlate the threat model components with visual diagram components from the Visio diagrams.” Pet. 65 (citing EX-1003, ¶166); *see* Pet. 83–85 (alleged reasons to combine Zheng and Baker).

139. However, Zheng does not disclose any mapping file, either expressly or inherently, and even considered in view of Baker, fails to disclose or suggest the claimed correlations based on mapping files. Baker’s process has no need or use for any “mapping files” as recited in the claims. Baker stores the “text and shape of each element of the flowchart . . . in the process database 30” and “automatically assign[s] or associate[s] predetermined objectives or controls according to the shapes of the imported flowcharts.” Baker, [0025]; *see also id.*, [0009]. Baker simply searches for a flowchart shape without disclosing any “mapping files” providing correlations as recited in the claims.

140. To reach the claimed correlations recited in claim 1, Petitioner and Mr. Hurlbut first have to create a mapping file that exists in neither reference in order to capture the threat actor/threat target association of Zheng, and then have to create a modification to the non-existent/created mapping file to repurpose the associations. I have reviewed the alleged motivations to combine (e.g., EX-1003 ¶¶165-166) and find no technical explanations or motivations for creating the mapping file, nor for modifying the mapping file if it existed. Rather, the motivations for these additions appear to be hindsight-based creations of features not disclosed or suggested by the art. Neither Baker or Zheng teaches “correlating” (a) threat model components with (b) visual diagram components of a third party software application, let alone doing so using “mapping files.” Further, one of skill in the art would not have been motivated to combine the alleged teachings of Zheng and Baker to arrive at limitations 1[c] and 1[d], but for hindsight, *i.e.*, using claim 1 and the teachings of the ’366 patent as a roadmap.

C. Grounds 3-5: Alleged Obviousness of: (1) Claims 2, 9, and 17 over the Combination of Zheng, Baker, Jones, and Galliano (*i.e.*, Ground 3); (2) Claims 1–20 over the Combination of Zheng, Baker, Jones, and Keenan (*i.e.*, Ground 4); and (3) Claims 2, 5-6, 9, 12–14, 17, and 19-20 over the Combination of Zheng, Baker, Jones and “the knowledge of a POSITA” (*i.e.*, Ground 5)

141. Petitioner also contends certain claims are unpatentable under 35 U.S.C. § 103 as obvious over the following combinations:

- (1) claims 2, 9, and 17 over the combination of Zheng (Ex. 1005), Baker (Ex. 1006), Jones (Ex. 1007), and Galliano (Ex. 1008);
- (2) claims 1–20 over the combination of Zheng, Baker, Jones, and Keenan (Ex. 1004); and
- (3) claims 2, 5-6, 9, 12-14, 17, and 19-20 over the combination of Zheng, Baker, Jones and “the knowledge of a POSITA.”

Pet. 12, 85–89.

142. As for combination (1) above, Petitioner applies this combination only to dependent claims 2, 9, and 17, and does not appear to apply Galliano in any manner that would address any deficiencies I identified above, particularly with respect to independent claims 1, 8, and 16.

143. As for combination (2) above, Petitioner applies this combination to claims 1-20, and does not apply Keenan, in this obviousness context, in any manner that would address any deficiencies I identified above, particularly with respect to independent claims 1, 8, and 16. Further, while Keenan is cited as a basis for invalidity based on Combination (2), Petitioner has not presented any allegations as to how Keenan is applied in conjunction with teachings of Zheng, Baker, and Jones to arrive at claims 1-4, 7-11, and 15-18.

144. As for combination (3) above, Petitioner applies this combination only to dependent claims 2, 5-6, 9, 12-14, 17, and 19-20, and does not appear to apply any alleged “knowledge” of the skilled artisan, in this obviousness context, in any

manner that would address any deficiencies I identified above in Section XI.A, particularly with respect to independent claims 1, 8, and 16. *See* Pet. 88–89.

145. Because none of the references relied upon in Grounds 3-5 address the underlying deficiencies identified in my analysis of Grounds 1 and 2, it is my opinion that the Petition in conjunctions with Mr. Hurlbut's declaration fail to establish obviousness under any of Grounds 3-5.

XII. CONCLUSION

146. 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

147. 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.

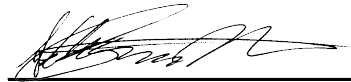
XIV. RIGHT TO SUPPLEMENT

148. 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

149. 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: January 12, 2024


Seth James Nielson, Ph.D.

Appendix A: The Challenged Claims of the ‘366 Patent

1. A threat modeling method, comprising:

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

a plurality of threat model components stored therein; and

a plurality of threats stored therein, wherein each of the threats is associated

with at least one of the threat model components through the one or more

databases;

providing one or more mapping files communicatively coupled with the one or

more databases, the one or more mapping files correlating the threat model

components with visual diagram components of a third party software

application (hereinafter “third party diagram components”); and

in response to receiving one or more user inputs, using one or more user interfaces

displayed on one or more computing devices communicatively coupled with

the one or more databases:

using the one or more computing devices, reading a data file generated by the

third party software application, the data file comprising a subset of the

third party diagram components, the data file defining one or more

relationships between the subset of third party diagram components;

determining using the one or more computing devices, for the subset of third party diagram components, correlated threat model components as defined in the one or more mapping files;

displaying on the one or more user interfaces a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and

generating, using the one or more computing devices, and displaying, on the one or more user interfaces, a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model.

2. The method of claim 1, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.
3. The method of claim 1, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.
4. The method of claim 1, wherein the data file comprises one of a VSD file, a VSDX file, a TMT file, an XML file, a JSON file, a PNG file, and a JPEG file.

5. The method of claim 1, wherein determining, for the subset of third party diagram components, correlated threat model components, comprises first determining whether a user-defined name for one of the subset of third party diagram components has a match in the one or more mapping files and, if no match is found, then determining whether a default title for the third party diagram component, as defined by the third party software application, has a match in the one or more mapping files.
6. The method of claim 5, further comprising, if no match is found for the default title, matching the third party diagram component with a placeholder component and displaying the placeholder component on the relational diagram to indicate that no match was found.
7. The method of claim 1, further comprising determining, for the one or more relationships defined by the data file, correlated threat model components as defined in the one or more mapping files.
8. A threat modeling system, comprising:
one or more computing devices communicatively coupled with one or more databases, the one or more databases comprising:
a plurality of threat model components stored therein; and

a plurality of threats stored therein, wherein each of the threats is associated with at least one of the threat model components through the one or more databases;

one or more mapping files communicatively coupled with the one or more databases, the one or more mapping files correlating the threat model components with visual diagram components of a third party software application (hereinafter “third party diagram components”);

an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user input, initiate reading of a data file by one of the one or more computing devices, the data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;

an interface configured to, in response to receiving user input, initiate a determination of which threat model components are correlated with the subset of third party diagram components in the one or more mapping files;

a diagram interface, displayed on the one or more computing devices, displaying a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the

subset of third party diagram components, the relational diagram defining a threat model; and

a threat report interface, displayed on the one or more computing devices, including a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model.

9. The system of claim 8, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.
10. The system of claim 8, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.
11. The system of claim 8, wherein the data file comprises one of a VSD file, a VSDX file, a TMT File, an XML file, a JSON file, a PNG file, and a JPEG file.
12. The system of claim 8, wherein the one or more mapping files includes a file correlating user-defined names of the third party diagram components with the threat model components.
13. The system of claim 8, wherein the one or more mapping files includes a file correlating default titles of the third party diagram components with the threat model components.

14. The system of claim 8, wherein, for each of the subset of third party diagram components for which no correlated threat model component is found in the one or more mapping files, the diagram interface displays a placeholder component indicative of a match not being found.
15. The system of claim 8, further comprising one or more mapping interfaces displayed on the one or more computing devices and configured to, in response to receiving user input, modify the one or more mapping files.
16. A threat modeling system, comprising:
one or more computing devices communicatively coupled with one or more databases, the one or more databases comprising:
a plurality of threat model components stored therein; and
a plurality of threats stored therein, wherein each of the threats is associated with at least one of the threat model components through the one or more databases;
one or more mapping files communicatively coupled with the one or more databases, the one or more mapping files correlating the threat model components with visual diagram components of a third party software application (hereinafter “third party diagram components”);

an import interface displayed on one of the one or more computing devices, the import interface configured to, in response to receiving user input, initiate reading of a data file by the one or more computing devices, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;

an interface configured to, in response to receiving user input, initiate a determination of which threat model components are correlated with the subset of third party diagram components in the one or more mapping files;

a diagram interface, displayed on the one or more computing devices, displaying a relational diagram of a computing network, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and

a threat report interface, displayed on the one or more computing devices, including a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model.

17. The system of claim 16, wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.
18. The system of claim 16, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.
19. The system of claim 16, wherein the one or more mapping files includes a file correlating user-defined names of the third party diagram components with the threat model components.
20. The system of claim 16, wherein the one or more mapping files includes a file correlating default titles of the third party diagram components with the threat model components.

Appendix B: Materials Reviewed

- U.S. Patent No. 10713366 to Agarwal (“the ‘366 Patent”)
- Prosecution History for the ‘366 Patent
- Declaration of Robert Hurlbut
- U.S. Patent No. 11,200,228 (“Keenan”) (EX-1004),
- U.S. Patent No. 10,503,907 (“Zheng”) (EX-1005),
- U.S. Patent Pub. No. 2014/0236665 (“Baker”) (EX-1006),
- U.S. Patent No. 9,602,529 (“Jones”) (EX-1007),
- U.S. Patent No. 10,681,068 (“Galliano”) (EX-1008);
- IPR2023-00656 Petition (Paper 1)
- IPR2023-00656 Patent Owner Preliminary Response (Paper 6)
- IPR2023-00656 Decision on Institution (Paper 7)
- December 18, 2023 Deposition Transcript of Mr. Robert Hurlbut (EX-2002)
- CIO Article dated August 23, 2016 (EX-2003)
- Draft NIST Special Publication 800-154 entitled “Guide to Data-Centric System Threat Modeling,” March 2016 (EX-2004)
- Excerpts from *Measuring and Managing Information Risk, A FAIR Approach*, by Jack Freund and Jack Jones, 2015 (EX-2005)
- NIST Special Publication 800-30, Rev. 1, entitled “Guide for Conducting Risk Assessments, Sept. 2012 (EX-2006)
- Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, April 6, 2015 (EX-2007)

Case IPR2023-00656

Patent 10,713,366

Declaration of Seth Nielson, Ph.D.

- Excerpts from *Threat Modeling* by Frank Swiderski and Window Snyder, 2004 (EX-2008)
- All other documents/materials cited or referred to in this declaration.

Case IPR2023-00656
Patent 10,713,366
Declaration of Seth Nielson, Ph.D.

Appendix C: Seth 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