

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner

v.

THREATMODELER SOFTWARE INC.,
Patent Owner

IPR2023-00821

U.S. Patent No. 10,699,008

**DECLARATION OF ROBERT HURLBUT IN SUPPORT OF PETITION
FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 10,699,008**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND AND QUALIFICATIONS.....	1
III.	DOCUMENTS AND OTHER MATERIALS RELIED UPON	4
IV.	STATUTORY GROUNDS FOR CHALLENGE	5
V.	RELEVANT PATENT LAW AND LEGAL STANDARDS.....	5
A.	Date of Invention	5
B.	Anticipation.....	6
C.	Obviousness.....	6
D.	Standard of Proof	9
VI.	LEVEL OF ORDINARY SKILL IN THE ART	9
VII.	RELEVANT TECHNOLOGY BACKGROUND	10
VIII.	THE '008 PATENT AND ITS PROSECUTION HISTORY	15
A.	Overview of the '008 Patent	15
B.	Priority Date	17
C.	Prosecution History	18
IX.	CLAIM CONSTRUCTION.....	19
A.	“Threat Model Components”	19
B.	“Attack Paths”	19
X.	INVALIDITY OF THE CHALLENGED CLAIMS OF THE '008 PATENT	20
A.	Overview of the Prior Art.....	20
1.	Jones (EX-1004)	20
2.	Zheng (EX-1005)	23
3.	Keenan (EX-1006)	24
4.	Yu (EX-1007)	24
5.	Reith (EX-1008).....	25

B.	Ground 1: Jones Anticipates the Claims 1 and 3.	26
1.	Claim 1	27
2.	Claim 3: “The threat model chaining method of claim 1, further comprising configuring the one or more interfaces to, in response to receiving one or more user inputs, store one or more additional threat model components in the one or more databases, store one or more additional threats in the one or more databases, associate each additional threat with at least one of the additional threat model components through the one or more databases, store one or more additional compensating controls in the one or more databases, and associate each additional compensating control with at least one of the additional threats through the one or more databases.”	48
C.	Ground 2: The Combination of Jones, Zheng, and Keenan Render Claims 1-20 Obvious	49
1.	Claim 2: “The threat model chaining method of claim 1, further comprising configuring the diagram interface to, in response to receiving a user selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.”	50
2.	Claim 4:	51
3.	Claim 5: “The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces, visually display one or more attack paths which pass through multiple diagrammed threat model components of the first threat model.”	53

4. **Claim 6: “The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving a user toggle of one of the diagrammed compensating controls (hereinafter “first control”) of the first threat model to a on state through the one or more interfaces, toggle all attack paths mitigatable by the first control to a mitigated display state.” 53**
5. **Claim 7: “The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving a user toggle of the first control to an off state through the one or more interfaces, toggle all attack paths mitigatable by the first control to an unmitigated display state.....54**
6. **Claim 8: “The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces to remove the first control from the first threat model, toggle all attack paths mitigatable by the first control to an unmitigated display state.” 55**
7. **Claim 9: “The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.” 56**
8. **Claim 10: “The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces to alter a profile of an attacking component, alter the visually displayed attack paths.” 56**

9. **Claim 11: “The attack simulation method of claim 3, further comprising configuring the diagram interface to receive one or more user inputs to add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.” 57**
10. **Claim 12: 57**
11. **Claim 13: “The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving a user input to toggle one of the diagrammed compensating controls (hereinafter “first control”) to an on state, toggle all attack paths mitigatable by the first control to a mitigated display state.” 58**
12. **Claim 14: “The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to receiving a user input to toggle the first control to an off state, toggle all attack paths mitigatable by the first control to an unmitigated display state.” 58**
13. **Claim 15: “The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to receiving one or more user inputs removing the first control from the first threat model, toggle all attack paths mitigatable by the first control to an unmitigated display state.” 59**
14. **Claim 16: “The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.” 59**

15.	Claim 17: “The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, alter a profile of an attacking component, wherein the alteration alters the visually displayed attack paths.”	59
16.	Claim 18: “The attack simulation system of claim 12, wherein the one of a system, an application, and a process comprises a computing network.”	59
17.	Claim 19: “The attack simulation system of claim 18, wherein the diagram interface is further configured to, in response to receiving one or more user inputs, diagram a communication protocol between two of the diagrammed threat model components, the diagrammed communication protocol including an alphanumeric indicator.”	60
18.	Claim 20: “The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.”	63
19.	A POSITA Would Have Been Motivated to Combine Jones, Zheng, and Keenan.....	63
D.	Ground 3: The References of Ground 2 and Yu Render Claims 1-20 Obvious	65
E.	Ground 4: The References of Ground 3 and Reith Render Claims 1-20 Obvious	68
F.	Ground 5: The References of Ground 4 and the Knowledge of a POSITA Render Claims 5-8 and 13-15 Obvious	70
XI.	CONCLUSION	71

EXHIBITS

Exhibit No.	Description
EX-1001	U.S. Patent No. 10,699,008 (“the ’008 patent”)
EX-1002	Prosecution History of the ’008 patent
EX-1003	Declaration of Robert Hurlbut
EX-1004	U.S. Patent No. 9,602,529 (“Jones”)
EX-1005	U.S. Patent No. 10,503,907 (“Zheng”)
EX-1006	U.S. Patent No. 11,200,228 (“Keenan”)
EX-1007	U.S. Patent No. 9,948,652 (“Yu”)
EX-1008	U.S. Patent No. 10,216,938 (“Reith”)
EX-1009	Scheduling Order, Case No. 1:22-cv-00912-MN
EX-1010	Email from Petitioner’s Counsel to PO’s Counsel
EX-1011	Excerpts from <i>Risk Centric Threat Modeling</i> , by Tony Uceda Velez and Marco M. Morana, John Wiley and Sons, Inc., 2015
EX-1012	Excerpts from <i>Threat Modeling Designing for Security</i> , by Adam Shostack, John Wiley and Sons, Inc., 2014
EX-1013	Excerpts from <i>Threat Modeling</i> , by Frank Swiderski and Window Snyder, Microsoft Press, 2004
EX-1014	Excerpts from <i>The Security Development Lifecycle</i> , by Michael Howard and Steve Lipner, Microsoft Press, 2006
EX-1015	Electric Power Research Institute, <i>Integrating Electricity Subsector Failure Scenarios Into a Risk Assessment Methodology</i> , 2013

I. INTRODUCTION

I, Robert Hurlbut, declare as follows:

1. My name is Robert Hurlbut. I have been asked by Petitioner IriusRisk Inc. to provide my expert opinions in support of the above-identified petition for *inter partes* review of U.S. Patent No. 10,699,008 (the “’008 patent,” EX-1001), challenging the validity of claims 1-20 (the “Challenged Claims”).

2. I currently hold the opinions set forth in this declaration.

3. In summary, it is my opinion that the references cited below anticipate or render obvious the Challenged Claims. My detailed opinions on the claims are set forth below and in the attached claim chart.

4. I am being compensated for my time at the rate of \$250 per hour. This compensation is not contingent upon my performance, the outcome of this matter, or any issues involved in or related to this matter.

II. BACKGROUND AND QUALIFICATIONS

5. I have extensive experience in threat modeling and application security.

6. My professional experience and expertise is described in **Exhibit A**, which is my current CV.

7. I obtained a Bachelor of Science in Mathematics from Oklahoma State University in 1990.

8. I obtained a Master of Science in Cyber Security from Southern New Hampshire University in 2020.

9. During the 33 years after my undergraduate education, including while I was obtaining my Master's degree, I worked in industry as a software developer, software architect, and technical consultant for numerous companies that are listed in Exhibit A.

10. Since 2015, a significant amount of my work has been in designing and building threat models.

11. Between 2015 and the present, I have provided threat modeling consulting services for numerous clients. I design and build threat models for these clients and train their employees regarding the designing, building, and use of threat models. The threat models assist the clients in identifying potential risks to various portions of their businesses and infrastructure. This can include identifying potential threats in any applications or products the client may create as well as recommended mitigations to remediate those threats.

12. Between September 2017 and November 2021, I was the Senior Vice President and Threat Modeling Senior Architect/Lead at Bank of America, where I started, led, and further developed Bank of America's threat modeling program. I co-wrote materials for threat model training sessions that was required of all software developers within Bank of America. I worked with teams to build over

1,000 threat models within three years. These threat models identified potential threats to dozens of aspects of Bank of America's business areas, including threats to its storage and processing systems, its communication networks, its employees, its physical buildings, and personal information of customers.

13. Between November 2021 and the present, I have been the Principal Application Security Architect and Threat Modeling Lead at Aquia, Inc. I lead the threat modeling program at Aquia and for many of Aquia's client's, including a federal government agency.

14. I am a co-author of the Threat Modeling Manifesto, published in 2020, which was intended to inform, educate, and inspire practitioners to adopt threat modeling and improve security and privacy during the software development process. This is a "best practices" guide that my co-authors and I wanted to share with the public.

15. Since 2022, I am a co-Founding Member and one of the Speaker / Facilitators of a community endeavor called Threat Modeling Connect, which is an open forum to inform, educate, and inspire practitioners to adopt threat modeling and improve security and privacy during the software development process. This volunteer organization also provides community meetups, training events, and will host a first threat modeling conference in late 2023.

16. I have been a Certified Secure Software Lifecycle Professional (CSSLP) for the years 2014-2023 (renewed annually). This is a certification provided by the cybersecurity professional organization known as (ISC).

17. I am a frequent speaker at user groups and national and international conferences on threat modeling and application security.

III. DOCUMENTS AND OTHER MATERIALS RELIED UPON

18. In forming the opinions set forth in this declaration, I have reviewed the documents in the following table:

Exhibit No.	Description
EX-1001	U.S. Patent No. 10,699,008 (“the ’008 patent”)
EX-1002	Prosecution History of the ’008 patent
EX-1004	U.S. Patent No. 9,602,529 (“Jones”)
EX-1005	U.S. Patent No. 10,503,907 (“Zheng”)
EX-1006	U.S. Patent No. 11,200,228 (“Keenan”)
EX-1007	U.S. Patent No. 9,948,652 (“Yu”)
EX-1008	U.S. Patent No. 10,216,938 (“Reith”)
EX-1009	Federal Judiciary Report
EX-1010	Scheduling Order, Case No. 1:22-cv-00912-MN
EX-1011	Excerpts from <i>Risk Centric Threat Modeling</i> , by Tony Uceda Velez and Marco M. Morana, John Wiley and Sons, Inc., 2015
EX-1012	Excerpts from <i>Threat Modeling Designing for Security</i> , by Adam Shostack, John Wiley and Sons, Inc., 2014
EX-1013	Excerpts from <i>Threat Modeling</i> , by Frank Swiderski and Window Snyder, Microsoft Press, 2004

Exhibit No.	Description
EX-1014	Excerpts from <i>The Security Development Lifecycle</i> , by Michael Howard and Steve Lipner, Microsoft Press, 2006
EX-1015	Electric Power Research Institute, <i>Integrating Electricity Subsector Failure Scenarios Into a Risk Assessment Methodology</i> , 2013

19. Additionally, I have utilized my own experience and expertise, including regarding the knowledge and capabilities of a person of ordinary skill in the relevant art in the timeframe of the claimed priority date of the '008 patent.

IV. STATUTORY GROUNDS FOR CHALLENGE

20. In this declaration, I offer opinions on the following grounds that are the basis for this IPR proceeding:

Ground	Claims	Basis	Reference(s)
1	1, 3	§102	Jones
2	1-20	§103	Jones, Zheng, and Keenan
3	1-20	§103	The references of ground 2 and Yu
4	1-20	§103	The references of ground 3 and Reith
5	5-8 and 13-15	§103	The references of ground 4 and the knowledge of a POSITA

V. RELEVANT PATENT LAW AND LEGAL STANDARDS

A. Date of Invention

21. I have been asked to use the date of the filing of the earliest application to which priority is claimed (*i.e.*, May 17, 2017) as the date of invention for purposes of my analysis.

B. Anticipation

22. I am informed and understand that a patent claim is invalid under 35 U.S.C. §102 if a prior art disclosure teaches every element required by the claim, either expressly or inherently. The identical invention must be shown in as complete detail as is contained in the claim. When a claim covers several structures or compositions, either generically or as alternatives, the claim is deemed anticipated if any of the structures or compositions within the scope of the claim is known in the prior art.

C. Obviousness

23. I am informed and understand that a patent claim is invalid under 35 U.S.C. § 103 if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time of the invention to a person having ordinary skill in the art to which the subject matter pertains. Obviousness, as has been explained to me, is based on (i) the scope and content of the prior art, (ii) the differences between the prior art and the claim, (iii) the level of ordinary skill in the art, and (iv) any secondary indicia of non-obviousness (*e.g.*, “secondary considerations” such as commercial success in the market place of the claimed invention), to the extent that they exist.

24. I further understand that obviousness may be demonstrated by showing that it would have been obvious to combine the teachings of more than

one item of prior art. In determining whether a piece of prior art could have been combined with other prior art or with other information within the knowledge of a person having ordinary skill in the art, the following are examples of approaches and rationales that may be considered:

- 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 devices (methods, or products) in the same way;
- Applying a known technique to a known device (method or product) ready for improvement to yield predictable results;
- Applying a technique or approach that would have been obvious to try (choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success);
- Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to a person having ordinary skill in the art; and

- Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

25. I further understand that an invention may be obvious if one of ordinary skill in the art, facing a wide range of needs created by developments in the field, would have seen an obvious benefit to the solutions tried by the applicant. When there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, it may be obvious to a person of ordinary skill to try the known options. If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique would have been obvious.

26. I further understand that a person of ordinary skill in the art is a hypothetical person who is presumed to be aware of all of the relevant art at the time of the invention. The person of ordinary skill may be able to fit together the teachings of multiple patents and/or printed publications employing ordinary creativity and the common sense that familiar items may have uses in another context or beyond their primary purposes.

27. I also understand that when considering the obviousness of a patent claim, one should consider whether a teaching, suggestion, or motivation to combine the references exists so as to avoid impermissibly applying hindsight when combining or modifying the prior art. I understand this test should not be applied rigidly, but that the test can be important to avoid such hindsight.

28. I also understand that one of ordinary skill in the art must have a reasonable expectation of success in combining or modifying prior art references.

29. I also understand that all elements of a claim must be considered in an obviousness analysis.

D. Standard of Proof

30. I understand that the standard to prove unpatentability in an *inter partes* review proceeding is by a preponderance of the evidence, which means more likely than not.

VI. LEVEL OF ORDINARY SKILL IN THE ART

31. I have considered the level of ordinary skill in the art relevant to the '008 patent. I understand that factors such as the education level of those working in the field, the sophistication of the technology, the types of problems encountered in the art, the prior art solutions to those problems, and the speed at which innovations are made may help establish the level of skill in the art.

32. After reviewing the '008 patent, the relevant portions of the prosecution history of the '008 patent, and cited references, it is my opinion that the relevant art of the '008 patent is in the field of threat modeling.

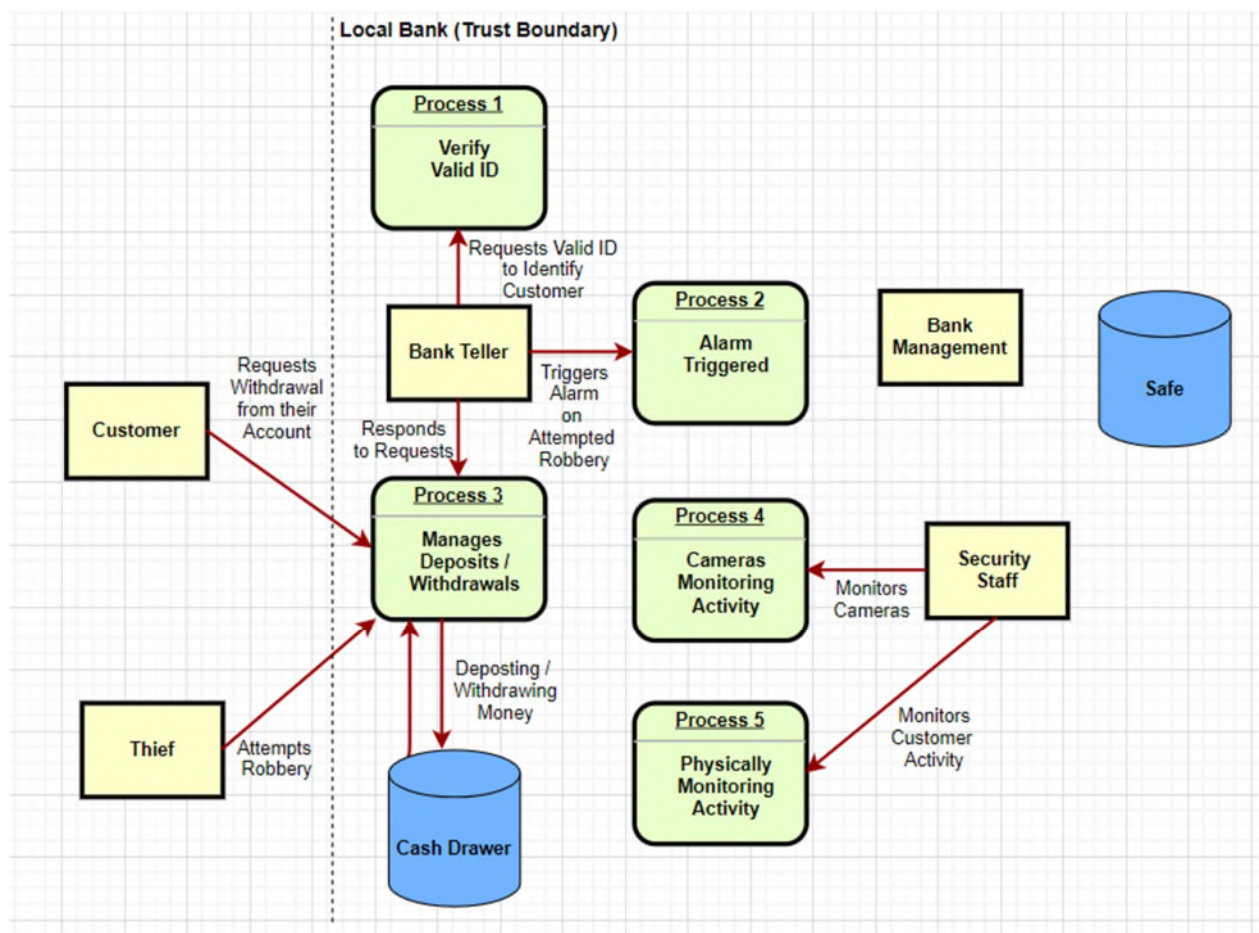
33. Based upon my knowledge of this field, I conclude that a person of ordinary skill in the art ("POSITA") at the time of the earliest filing date of the '008 patent (May 17, 2017), and for that matter, at all subsequent times through the present, would have had a Bachelor's degree in computer engineering, computer science, mathematics, or a similar discipline, with at least three years of relevant industry or research experience, including experience designing or implementing threat models and experience designing or developing software applications. Additional work or research experience can substitute for less or different education, and vice-versa.

34. I am and was at the time of the earliest filing date at least a person of skill in the relevant art, of a level at least as high as or more than ordinarily skilled persons, and I am able to provide insight and opinions into the understandings of such persons at all relevant times by virtue of my education, training and experience.

VII. RELEVANT TECHNOLOGY BACKGROUND

35. Threat modeling is a process by which potential threats to a system are identified. The system can be almost anything that is vulnerable to threats and

that humans wish to protect. For example, it can be a physical structure, such as an office building or a power plant, or it can be a digital asset, such as financial data or customer information. A threat model is a useful tool for human beings to systematically understand a system's vulnerabilities. Historically, threat models were often developed by people drawing on a white board or a piece of paper. A simple example of a threat model is the following, which shows potential threats to physical branch of a bank:



In this diagram, called a Data Flow Diagram (DFD), which is commonly used for Threat Modeling, the following elements are depicted:

- Actors: Customer, Thief, Bank Teller, Bank Management, Security Staff
- Processes: Verify Valid ID, Manages Deposits / Withdrawals, Alarm Triggered, Camara Monitoring Activity, Physically Monitoring Activity
- Data Stores or Assets: Cash Drawer, Safe
- Data Flows: Arrows in the diagram to show actions or data flowing between Actors and Processes or between Processes and Data Stores or Assets

In determining threats, this Data Flow Diagram (DFD) helps identify potential threat actors (Customer, Thief) and various countermeasures to create an initial threat model:

1. Threat: Customer requests the Bank Teller to withdraw cash from their Account
 - a. Countermeasure(s):
 - i. Bank Teller requests Valid ID
 - ii. Bank Teller verifies Valid ID

2. Threat: Thief attempts robbery by requesting the Bank
Teller to withdraw cash from the Cash Drawer

a. Countermeasure(s):

- i. Bank Teller triggers an Alarm
- ii. Security Staff monitors the camera for
suspicious activity
- iii. Security Staff monitors actions by customers
for suspicious activity

36. It is common for software developers to utilize threat models during the software development process so that they can identify potential risks and build in safeguards against those risks in the software as they are developing it. This is discussed, for example, in the well-known treatise *Risk Centric Threat Modeling*, by Tony Uceda Velez and Marco M. Morana, John Wiley and Sons, Inc., 2015, which states, “There are several good reasons to integrate threat modeling activities within the SDLC (software development lifecycle). Threat models help information security reviews of software projects and assess the risks posed by vulnerabilities identified during the various type security activities that are built into SDLC such as design reviews, secure coding, and penetration tests. A threat model helps risk managers to assess application security risks by correlating the analysis of threats to the vulnerabilities to application data and functional assets. A

risk analysis that factors threats, vulnerabilities, and assets can also factor likelihoods and impacts to determine the risk level and to apply security measures to reduce this level of risk.” EX-1011 (excerpts of treatise), p. 94. Many other treatises from the early 2000s reiterate the commonality of different threat models. EX-1012, *Threat Modeling Designing for Security*, by Adam Shostack, John Wiley and Sons, Inc., 2014 (“Everyone threat models.” Page xxii); EX-1013, *Threat Modeling*, by Frank Swiderski and Window Snyder, Microsoft Press, 2004 (“The process of threat modeling is not new.” Page xi); EX-1014, *The Security Development Lifecycle*, by Michael Howard and Steve Lipner, Microsoft Press, 2006 (“Chapter 9: Threat Modeling Artifacts.”).

37. In the late 1990s, computer software emerged for preparing threat models. For example, Microsoft introduced the SDL Threat Modeling Tool that allowed users to build threat models using a computer running the tool. I personally used the Microsoft tool for the first time around 2009.

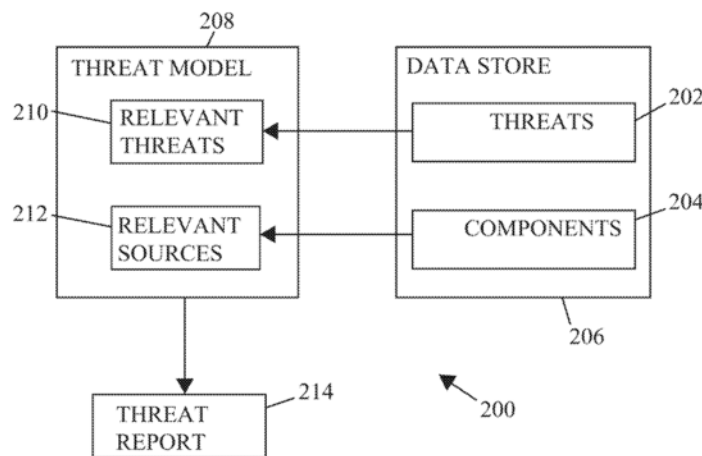
38. It is well known in the art that threat models are used to visually represent threats associated with the threat target or source of the threat, as well as various mitigation strategies. One such mitigation strategy known in the art is referred to as “compensating controls.” EX-1007, 5:29-32. “A compensating control is a cyber security control implemented as an alternative to a recommend control that provides equivalent or comparable control.” EX-1015, 1-4.

VIII. The '008 PATENT AND ITS PROSECUTION HISTORY

A. Overview of the '008 Patent

39. The '008 patent, entitled “Threat model chaining and attack simulation systems and related methods,” relates to threat modeling. EX-1001. The patent explains that “[t]hreat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized.” EX-1001, 1:48-49. Threat modeling involves the identification and visualization of potential threats, which typically involves generating diagrams on a whiteboard or in a computer application to represent the potential threats to a particular system.

40. The '008 patent describes that threat models are created from defined threats and threat model components, which are stored within a database. *Id.*, 9:10-27. This is shown in Figure 2:



41. Each threat model component “is a potential relevant source for one or more threats.” *Id.*, 9:28-61.

42. The '008 patent further describes compensating controls stored in the database and associated with the threats that “mitigate different threats emanating from different components.” *Id.*, 25:57-59. FIG. 19 shows the claimed system with six compensating controls (each labeled “CC”):

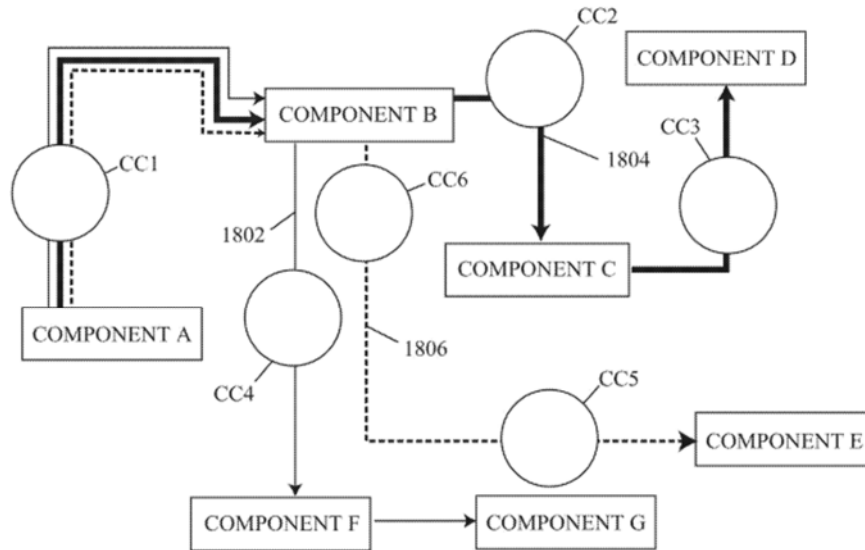


FIG. 19

43. The patent explains that “[t]he term ‘compensating control’ in implementations herein may be an alternative mechanism to a security requirement or standard,” *id.*, 6:14-20, or a compensating control may have a more general definition as any alternative to a security requirement, *id.*, 6:49-68. For example, the patent explains that “a ‘security requirement’ may be defined as a hardware solution and a ‘compensating control’ may be defined as a software solution, such as a change in the code or software added to a system.” *Id.*, 6:49-68.

44. The patent provides an interface including a diagram interface, configured to display a relational diagram to visualize the aforementioned threats associated with threat model components and compensating controls using visual representations, such as shapes. *Id.*, 16:3-14, 23:36-45.

45. A user may also select a set of components to create a group of components or each grouping of components could be diagrammed separately as an independent threat model. *Id.*, 15:65-16:2. The threat model may then be saved as a component so that it may be imported into another threat model/diagram, therefore adding or nesting one threat model to another—incorporating the previously-defined model into a new model. *Id.*, 20:23-36. The patent explains that “[t]his ability is generally termed ‘threat model chaining’” and “is a useful mechanism for allowing a user to diagram complex systems/processes without having to repeatedly build common elements among the systems/processes.” *Id.*

46. The patent owner (“PO”) was not the first to devise the claimed invention, as shown through the prior art discussed below.

B. Priority Date

47. The ’008 patent claims priority to four provisional applications, the earliest of which was filed on May 17, 2017. For the purposes of this IPR only, Petitioner applies a priority date of May 17, 2017 to this IPR.

C. Prosecution History

48. The application leading to the '008 patent was filed on December 20, 2018. EX-1002. On August 8, 2019, the Examiner issued a non-final rejection as to all claims under 35 U.S.C. §101 as reciting only “high level of generally well-known [computer] components” which performed abstract ideas as well as rejections and under non-statutory double patenting, stating that, although the claims were not identical, the claims were obvious variants over U.S. Patent Nos. 10,200,399 and 10,255,439. *See id.*, 8/8/2019 Non-final Rejection. The Applicant overcame the §101 rejection with argument that the Examiner failed to analyze and compare the claim language to the example claim language of other abstract patents. *See id.*, 10/25/2019 Applicant Arguments/Remarks Made in an Amendment page 18.¹ Applicant overcame the double patenting rejection with a terminal disclaimer. *Id.*

49. The Examiner issued the claims as-filed, *original*, without any citations or comparison to any prior art nor any rejections under Sections 102/103. As reasons for allowance, the Examiner stated that the art did not disclose the relational diagram and threat model chaining elements in independent claims 1 and

¹ The double patenting rejection was initially made final, but the Examiner withdrew the rejection after Applicant informed the Examiner that Applicant filed a terminal disclaimer. *See id.*, 1/11/2020 Applicant summary of interview with examiner.

4. For independent claim 12, the Examiner held the Examiner noted claim 12 was “substantively similar” to claims 1 and 4, and thus “allowed under the same rationale. *See id.*, 2/24/2020 Notice of Allowance at 2.

IX. CLAIM CONSTRUCTION

50. In my opinion, the '008 patent and its file history establish the following definitions for certain terms in the Challenged Claims, and I have applied those definitions in my analysis. For all other terms, I applied the plain and ordinary meaning that a POSITA would have for the terms.

A. “Threat Model Components”

51. Based on the specification, the term “threat model components” means “a potential relevant source for one or more threats.” Referring to FIG. 2, the patent explains that a threat model “component” is “a potential relevant source for one or more threats,” stating “[f]or example, one threat may be Bluejacking and one component, which would be correlated to this threat through the database, could be “Bluetooth port.” EX-1001, 9:28-61.

B. “Attack Paths”

52. The '008 patent describes “attack paths” consistent with the plain and ordinary meaning of the term as “[t]he routes from all potential attackers to a selected asset are the ‘attack vectors’ or attack paths to that asset.” EX-1001 at 22:65-68.

X. INVALIDITY OF THE CHALLENGED CLAIMS OF THE '008 PATENT

53. In my opinion, the Challenged Claims are invalid for the reasons discussed below and in the attached Exhibit B (which is an anticipation chart for Jones for claims 1 and 3 only).

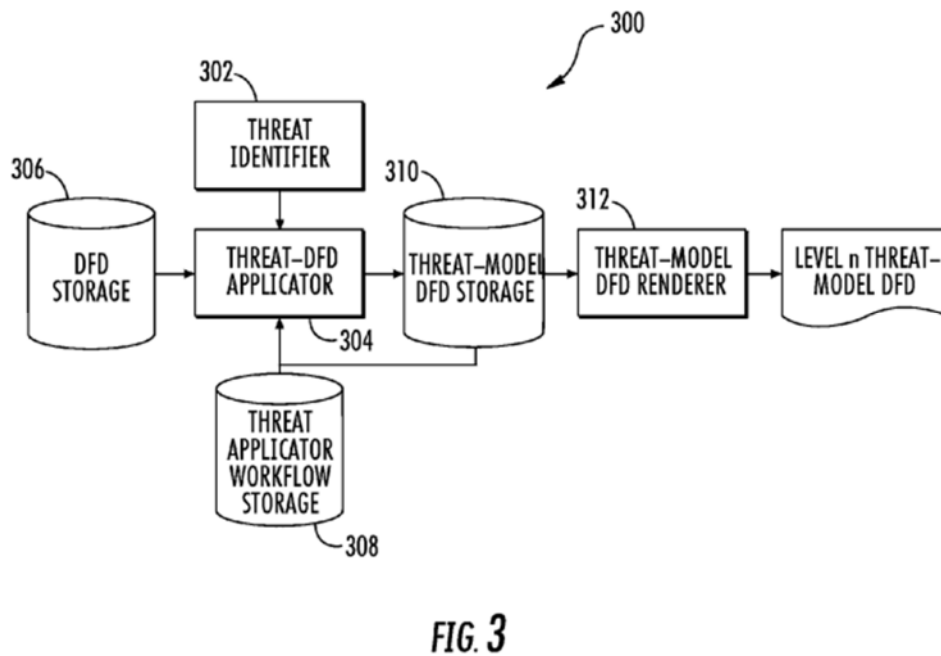
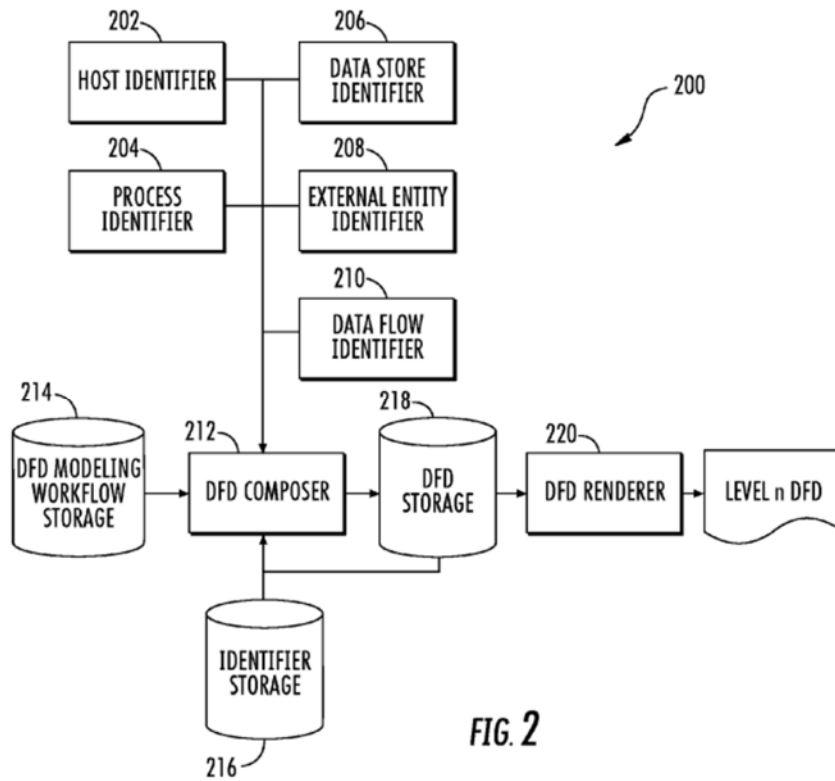
A. Overview of the Prior Art

1. Jones (EX-1004)

54. Jones, entitled “Threat Modeling and Analysis,” discloses a system for modeling and analysis of cybersecurity threats. This system includes a data flow diagram (DFD) creator, threat indicator, and threat analyzer. The DFD creator identifies elements of the information system and composes a DFD including nodes and edges representing components and data flows of the information system. The threat indicator identifies cybersecurity threats to a particular element of the information system and adds a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system.

55. In metadata associated with the nodes, edges and secondary node, the DFD creator and threat indicator provide structured information including attributes of the components, data flows, and cybersecurity threats. And the threat analyzer performs analyses of the cybersecurity threats based on the threat-model DFD and metadata associated with the nodes, edges and secondary node thereof.

56. Jones' process is shown in Figs. 2-5:



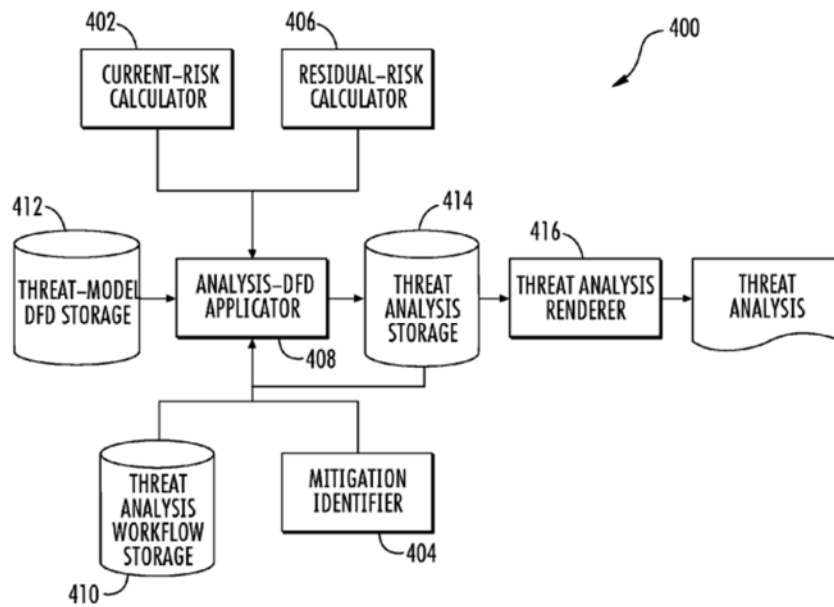


FIG. 4

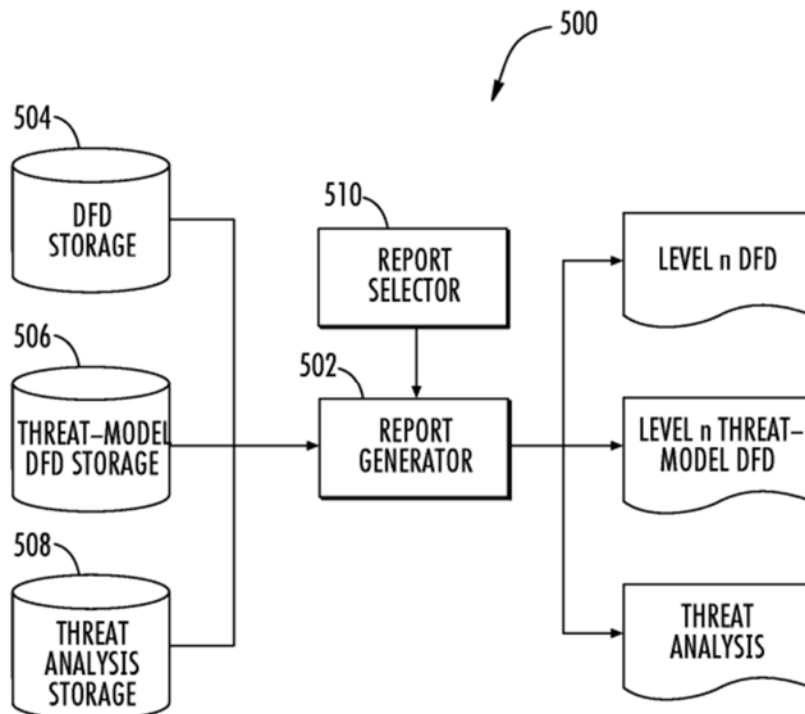


FIG. 5

57. Jones further discloses that “a process, host or data store—may include multiple nested components,” *i.e.*, the threat models may be chained or “nested” together, thus disclosing a threat model chaining method. Jones system produces a GUI as shown below:

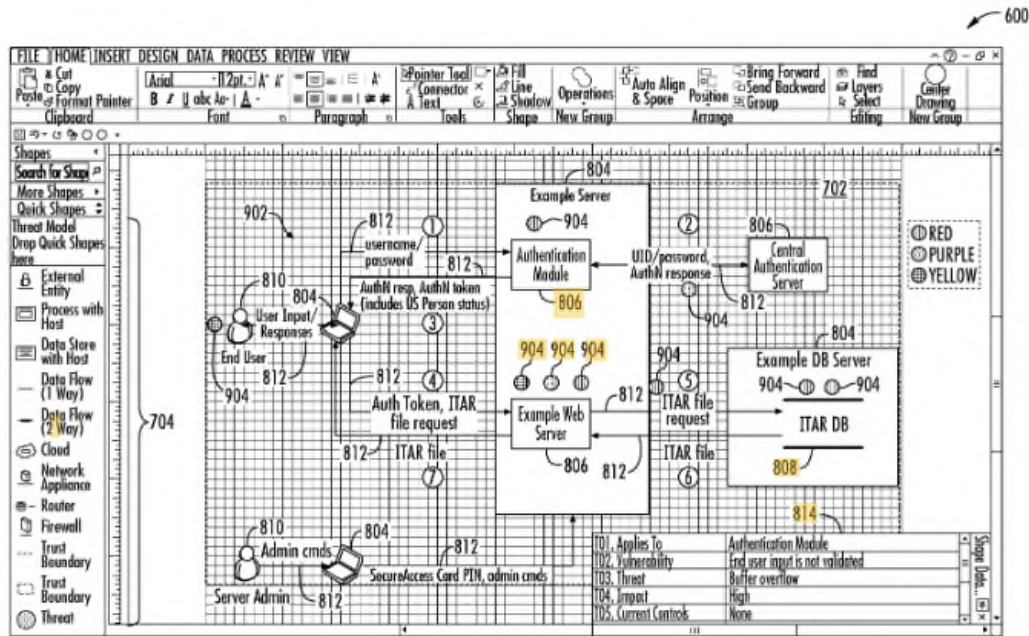


FIG. 9

2. Zheng (EX-1005)

58. Zheng is titled “Intelligent Threat Modeling and Visualization” and discloses “[a] computer-implemented system... for visualizing and analyzing security threats in a suite of software applications.” EX-1005, Abstract. “The system includes 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.” *Id.* “The threat modeling module is adapted to interact with the visualization module to graphically depict on the

computer display the one or more security threats on the map in a threat modeling layer.” *Id.*

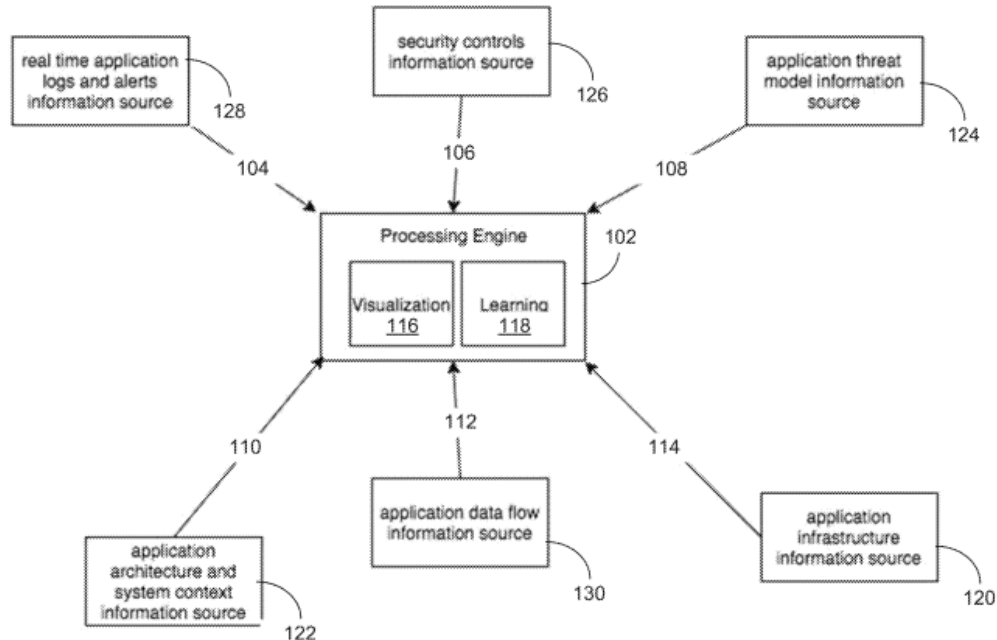


FIG. 1

3. Keenan (EX-1006)

59. Keenan discloses threat modeling and is relied upon in the Petition for its disclosure of toggling. Keenan describes threat modeling systems and method including a graphical user interface with the ability to “toggle” features on or off. Ex-1006 at 17:19-21.

4. Yu (EX-1007)

60. Yu discloses threat modeling and is relied upon in the Petition for its compensating controls disclosure. Yu discloses that “resource owners still need to create a threat model to understand their potential exposures and find

compensating controls to mitigate against any damage.” EX-1007, 5:29-32; see also *id.*, 5:54-63. Yu also refers to compensating controls generally as “controls.” *E.g.*, *id.*, 16:11-33.

61. And Yu also explains that it displays “threat vectors” in its threat models. See *id.* Fig. 2.

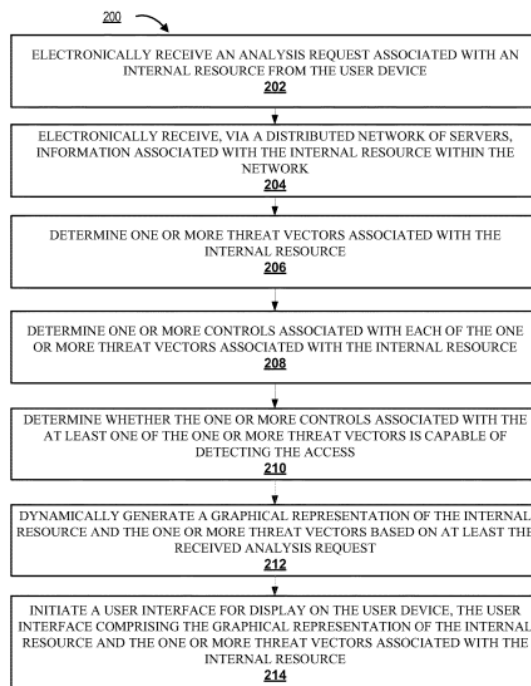


Figure 2

5. Reith (EX-1008)

62. Reith discloses threat modeling and is relied upon in the Petition for its chaining disclosure. Reith discloses “Recombinant Threat Models,” as shown in Fig. 4:

400

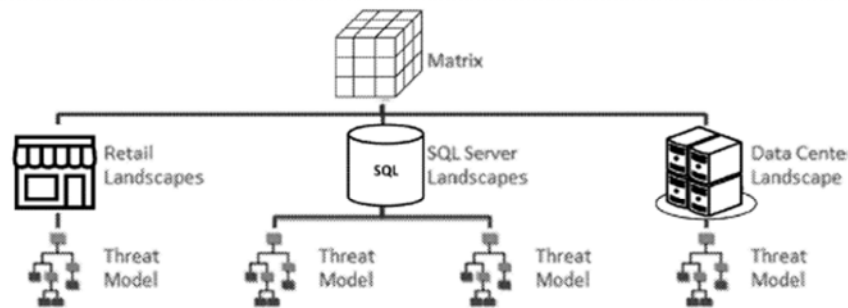


Figure 4

63. Reith discloses that “[a] Recombinant Threat Model may stand on its own within the threat landscape. Alternatively, multiple Recombinant Threat Models may be interconnected together.” EX-1008, 4:30-44; *see also id.*, 7:37-49, 7:65-8:2, 9:47-56.

B. Ground 1: Jones Anticipates the Claims 1 and 3.

64. In my opinion, Jones anticipated claims 1 and 3. All of the limitations of claims 1 and 3 are disclosed in Jones. My analysis comparing Jones to the claims 1 and 3 is contained below. I also have included additional analysis and citations to Jones for claims 1 and 3 in the chart attached as **Exhibit B**.

1. Claim 1

a. Element 1[p]. “A threat model chaining method, comprising:”

65. In my opinion, Jones discloses this preamble. Jones, entitled “Threat Modeling and Analysis,” relates generally to the “modeling and analysis of cybersecurity threats.” EX-1004, 1:5-7; *see also, e.g., id.*, 3:52-60 (“Example implementations of the present disclosure are generally directed to modeling and analysis of cybersecurity threats in a complex-system platform such as that of an aircraft. A complex-system (e.g., aviation) platform may 55 refer to a hardware architecture including one or more systems of a complex-system, and software framework including one or more application frameworks, that enable software such as particularly application software to operate the complex system or one or more of its systems.”). Jones discloses threat models including a cybersecurity threat mapped to a particular element of the information system by a threat indicator and a secondary node representing the threat to the data flow diagram (DFD). *Id.*, 2:20-32 (“The threat indicator may be configured to identify a cybersecurity threat to a particular element of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat model DFD for the information system. Similar to the DFD creator, the threat indicator may provide structured information including attributes of the cybersecurity threat, and may do so in metadata associated with the

secondary node of the threat-model DFD. This structured information may include, for example, a description of the cybersecurity threat and a Vulnerability giving rise thereto, a description of any current security controls designed to mitigate the cyber security threat or the like.”). Jones further discloses that its system “may include multiple nested components,” *i.e.*, the threat models may be chained or “nested” together, thus disclosing a threat model chaining method. *Id.* at 5:14-19. Jones’ system may “modify the threat-model DFD for the decomposed components to include their nested components ... thereby producing a level n+1 threat model DFD.” *Id.*, 6:12-34; *see also id.* at 4:22-35 (DFD “level establishment system”), 5:10-19 (discussing hierarchal breakdown of components at different levels), 5:20-44, 5:45-53, 5:64-6:11, 7:31-37, 8:23-31, 12:7-21, 12:43-63, 12:64-13:7 (threat model renderer composing a threat model from the components of multiple stored threat models), 15:43-61, 16:37-50, 17:16-31, 17:41-49, 18:44-57, 18:58-60, 19:10-28, 19:46-59, Figs. 1-5, 7-9; Element 1[f]. The creation of Jones’ level n+1 threat model DFD is shown, for example, by Figure 3 below:

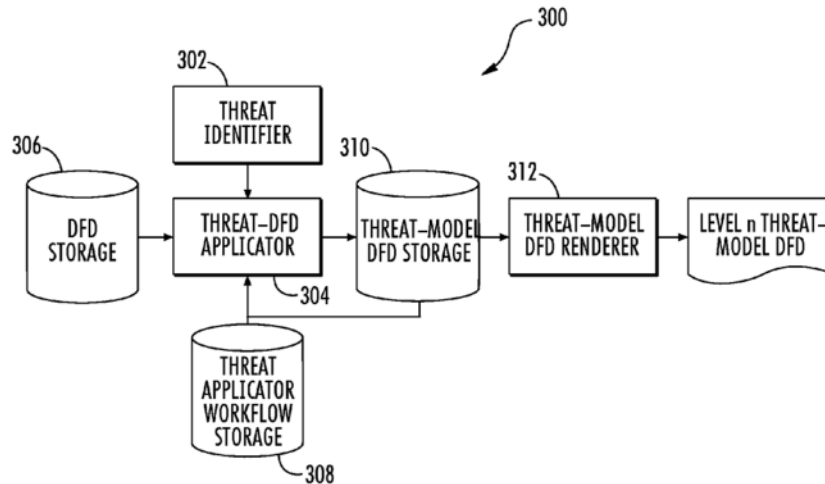


FIG. 3

66. In my opinion, a POSITA would understand that Jones’ disclosure of “multiple nested components” is a threat model chaining method as claimed in the ’008 patent. Indeed, the ’008 patent refers to chaining and nesting as the same concept. EX-1001, 20:23-36 (“When a user adds any of these component groups to a blank or existing diagram/threat model the threat model of the component group is added to (and/or nested within) the threat model of the existing diagram/threat model. . . . This ability is generally termed ‘threat model chaining’ herein.”), 20:46-58 (referring to “nested/chained” threat models), 23:1-13 (“nested or chained threat models”), 24:14-30, 25:18-23, 28:34-41.

b. Element 1[a]. “providing one or more databases, the one or more databases comprising:”

67. In my opinion, Jones discloses this element. Jones discloses that “suitable types of storage as described herein include file storage, *database*

storage, cloud storage or the like.” EX-1004, 8:4-9; *see also id.*, 10:26-34, 12:10-20, 15:18-22. Jones further discloses that its threat model data flow diagrams (DFD) may be stored in a “DFD storage 218 for later retrieval,” and examples of such storage includes “database storage.” *Id.*, 8:10-21, 8:23-31, 12:7-21, 12:49-63, 12:67-13:7, 15:49-61, 17:1-15, 17:20-27, Figs. 2-3, 9. For example, Figures 2 and 3 shown below show a “Threat-Model DFD Storage” and “DFD Storage” connected to a DFD renderer that may create level n DFDs:

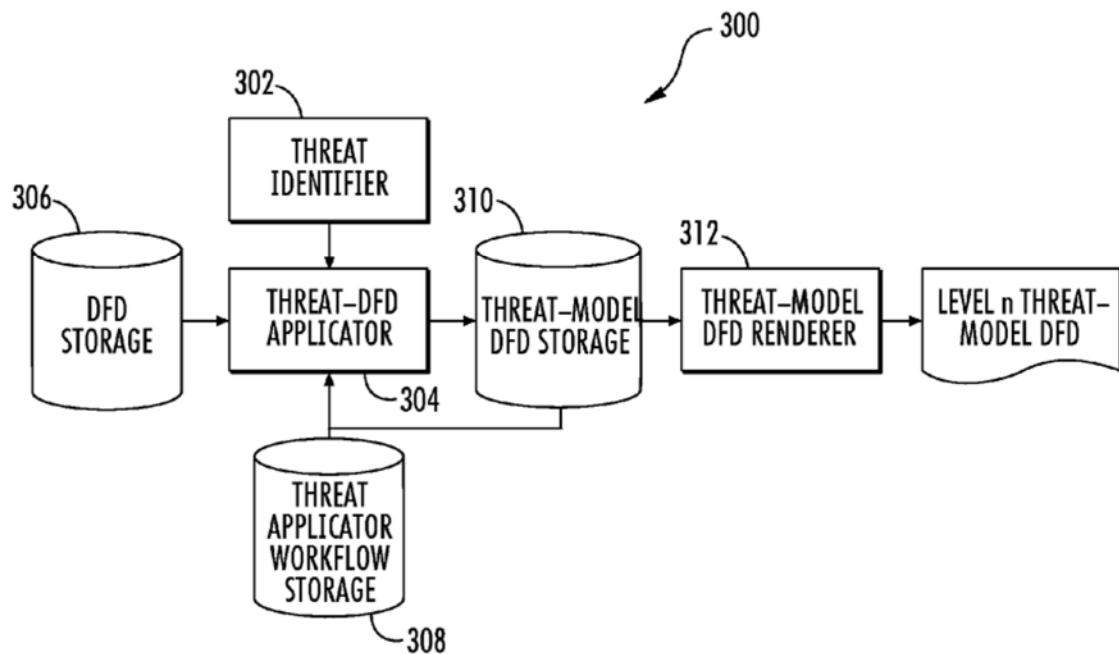
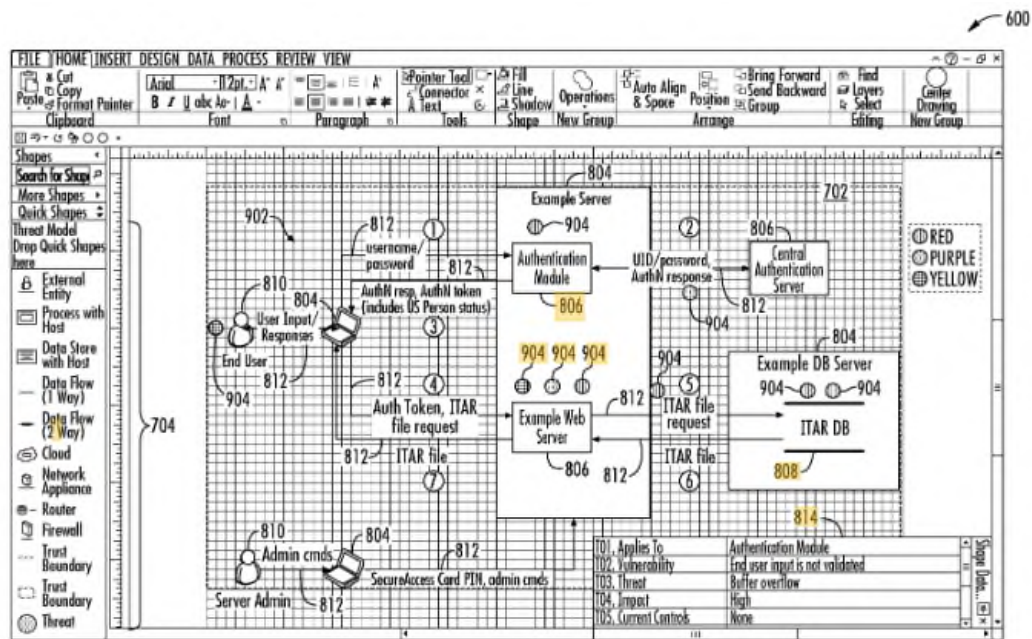
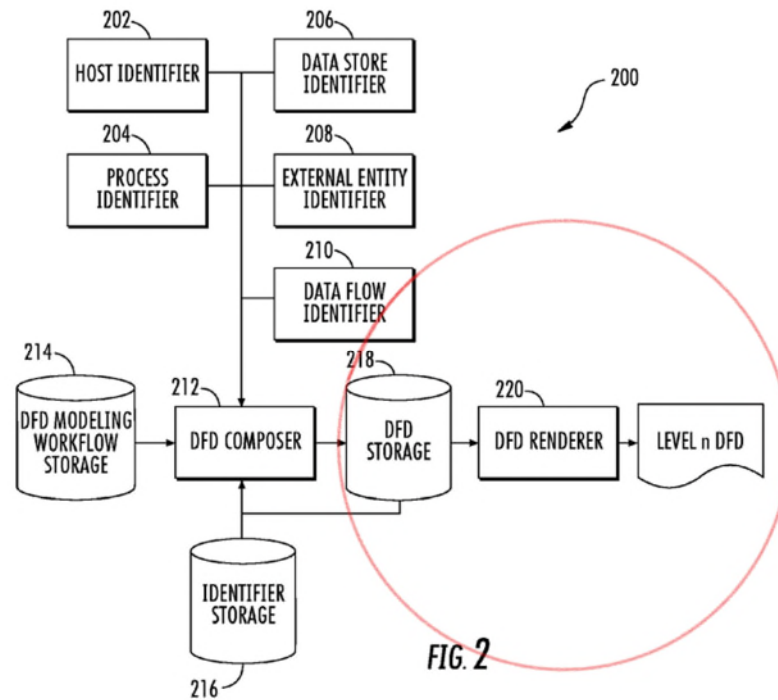


FIG. 3



- c. **Element 1[b]. “a plurality of threat model components stored therein; a plurality of threats stored therein, each threat associated with at least one of the threat model**

**components through the one or more databases;
and”**

68. In my opinion, Jones discloses this element. Jones discloses “a cybersecurity threat” is associated, modeled, and analyzed with “a particular element of the elements of the information systems,” such as a component or data flow, by a “threat indicator.” EX-1004, 5:64-6:3; *see also id.*, Abstract, 2:20-32, 2:33-41, 5:45-53, 5:64-6:11, 6:18-27, 6:35-45, 7:17-30, 11:59-12:6, 12:43-54, 14:33-48, 15:62-65, 16:37-42, 17:50-67, 18:18-29, 18:58-65 (“As shown, the DFD includes shapes for elements including various hosts 804, processes 806, data stores 808 and external entities 810, and data flows 812.”), 19:10-28, 19:29-37, Figs. 2-3, 6, 8-9, 10A-B. The elements of the information system “may include components such as hosts, processes, data stores and/or external entities, and data flows between the components.” *Id.*, 2:1-9. The “cybersecurity threat” further “may refer to a circumstance with a likelihood to have an adverse impact on the information system or a particular element of the information system.” *Id.*, 2:42-53; *see also id.*, 3:64-4:5, 6:46-58, 13:10-17.

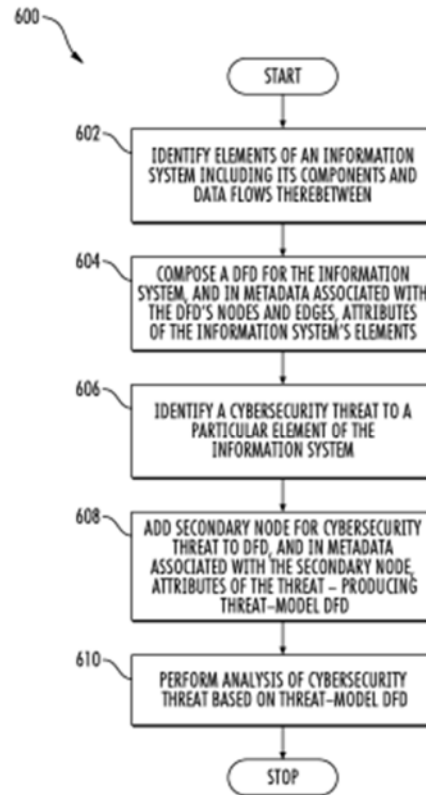


FIG. 6

69. Jones explains that “[t]he DFD creator may identify elements of an information system, and compose a DFD including nodes and edges representing components and data flows of the information system. The threat indicator may identify a cybersecurity threat to a particular element of the information system and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system.” *Id.*, Abstract.

70. Based on this disclosure, a POSITA would understand that the disclosed “cybersecurity threats” are threats as claimed, *see id.*, 2:42-53, and that these threats are associated with a particular element of the information system,

which are relevant sources of threats and thus threat model components because they include “hosts, processes, data stores and/or external entities,” which are relevant sources of threats in the information system being associated with the cybersecurity threats. *Id.*; *see also id.*, 2:1-9, Fig. 10B. Jones also discloses cybersecurity threats associated with “assets” of Jones’ system, which are also threat model components because assets in an information system are relevant sources of threats. *Id.*, 13:10-17 (“As explained above, a cybersecurity threat may refer to a circumstance or event with a likelihood to have an adverse impact on an asset such as the information system or complex-system platform used to implement the information system, such as through unauthorized access, 15 destruction, disclosure, modification of data and/or denial of service.”), 6:49-58.

1004

1000

Numbering for this table – this does not correspond to numbering in the Visio diagram.	Security controls that are recommended to bring the Current Risk rating lower.	Risk given that suggested mitigations are implemented.	The data flow diagram (DFD) element(s) that the threat applies to.	Additional clarifying information. If a finding is preliminary, meaning it needs further research indicate “Preliminary” here.	Use to note whether the review process has resulted in acceptance of this threat and associated impact and risk ratings.
REF #	SUGGESTED MITIGATIONS	RESIDUAL RISK	APPLIES TO	REMARKS	REVIEW STATUS
1	Encrypt client-server connections	Medium	Data flows between client app and server.	This is an information disclosure threat that may lead to a follow-on threat of spoofing threat.	Reviewed
2	Protect RPC connections with a protocol that provides integrity-protection (like SSL/TLS)	Medium	Master-to-Backup data flow		Likelihood rating not agreed
3	Fix buffer overflow.	Medium	Login process	CVSS rating of threat indicated high difficulty to reproduce, which is why likelihood is rated Medium	Not Reviewed
4	Use strong two-factor authentication.	Low	Database system	Preliminary: <Describe why finding is preliminary>	Waiting to clear Preliminary status
5	Implement a failover server in the same datacenter as primary server. Implement regional failover server.	Medium	Web server Application server	Preliminary: <Describe why finding is preliminary> Regional failover needed to bring residual risk to Low.	Waiting to clear Preliminary status
6	Background check	Low	Top level sys admins	Not a traditional STRIDE threat. Improper admin designation could result in all STRIDE threats.	Reviewed
7	Log admin success and fail actions.	Low	Application Server		Reviewed
8	Turn on host-based FW	Low	Web server	Type is “Undetermined” as the vulnerability is very general.	Not Reviewed

1002

● YELLOW ● GREEN

FIG. 10B

71. Fig. 9 shows an example display of threats and threat model components:

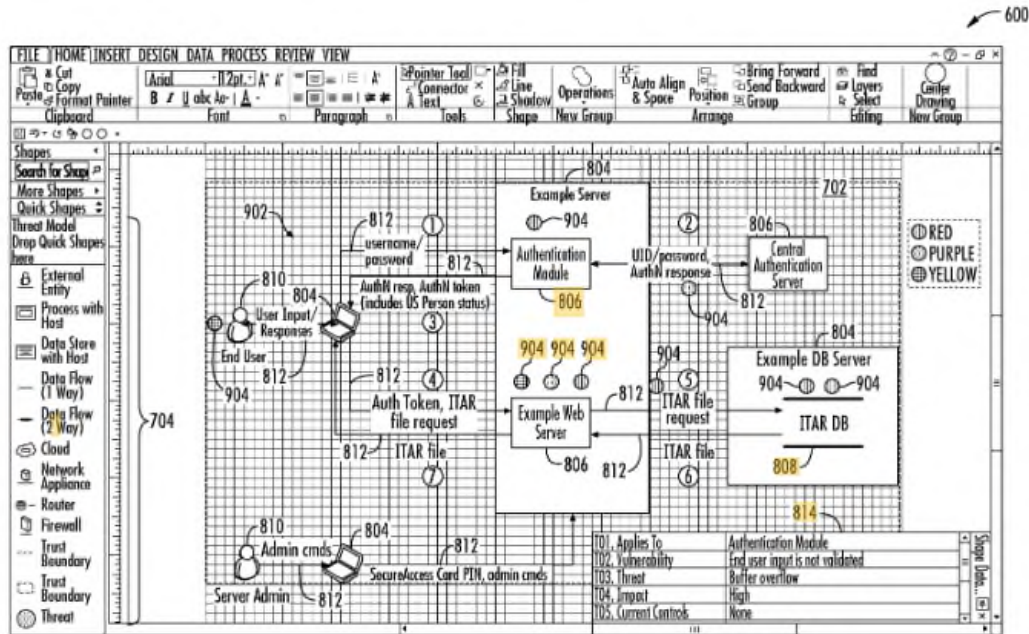


FIG. 9

	T01. Applies To	Authentication Module
	T02. Vulnerability	End user input is not validated
	T03. Threat	Buffer overflow
	T04. Impact	High
	T05. Current Controls	None

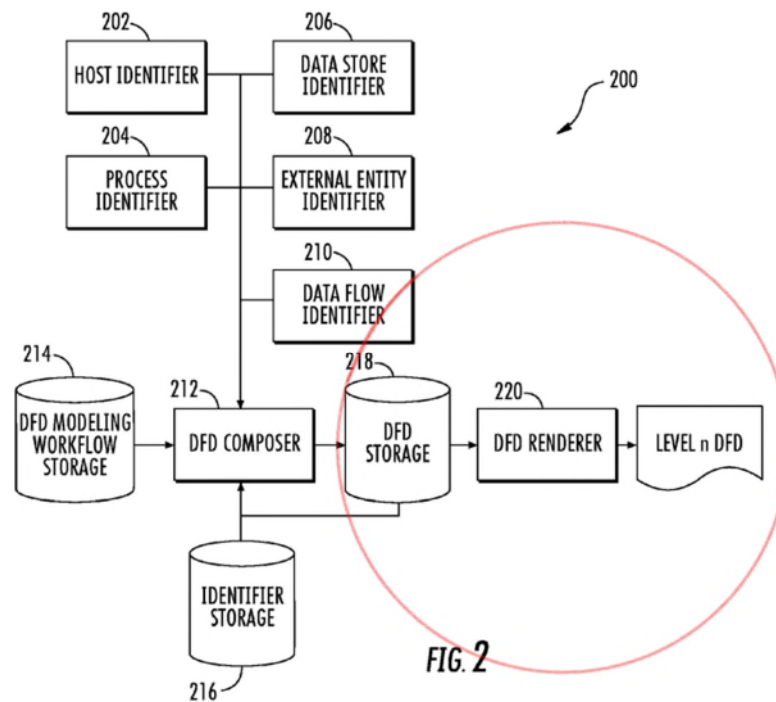
FIG. 9

The details of Fig. 9, 814 show “T03. Threat,” which displays the threat and T01 “Applies to,” which displays the threat model component.

72. Moreover, Jones also discloses that its system may apply threat model systems well known in the art, including the STRIDE threat model developed by Microsoft. *Id.*, 18:30-43, 13:30-60. A POSITA would understand that it is well

known in the art that the STRIDE model includes both threats and threat model components (and understood mitigations).

73. And Jones discloses that “each threat associated with at least one of the threat model components through the one or more databases.” See Element 1[a]; *see, e.g.*, EX-1004, Fig. 2.



- d. Element 1[c]. “a plurality of compensating controls stored therein, each compensating control associated with at least one of the threats through the one or more databases;”**

74. In my opinion, Jones discloses this element. Jones discloses an “analyzer” that may be configured to identify “one or more” of “a suggested mitigation implementable to reduce the current-risk rating to a lower, measure of residual risk.” EX-1004, 2:37-41, 14:66-15:17; *see also id.*, 2:20-32, 13:9-30

(discussing various alternative security principles used to identify threats), 15:43-49, 16:28-34. Jones further broadly discloses mitigations and security controls of any type. *Id.*, 11:52-57, 14:10-17. Fig. 10B further shows “suggested mitigations” corresponding to “data flow diagram DFD element(s) that the threat applies to:”

1004

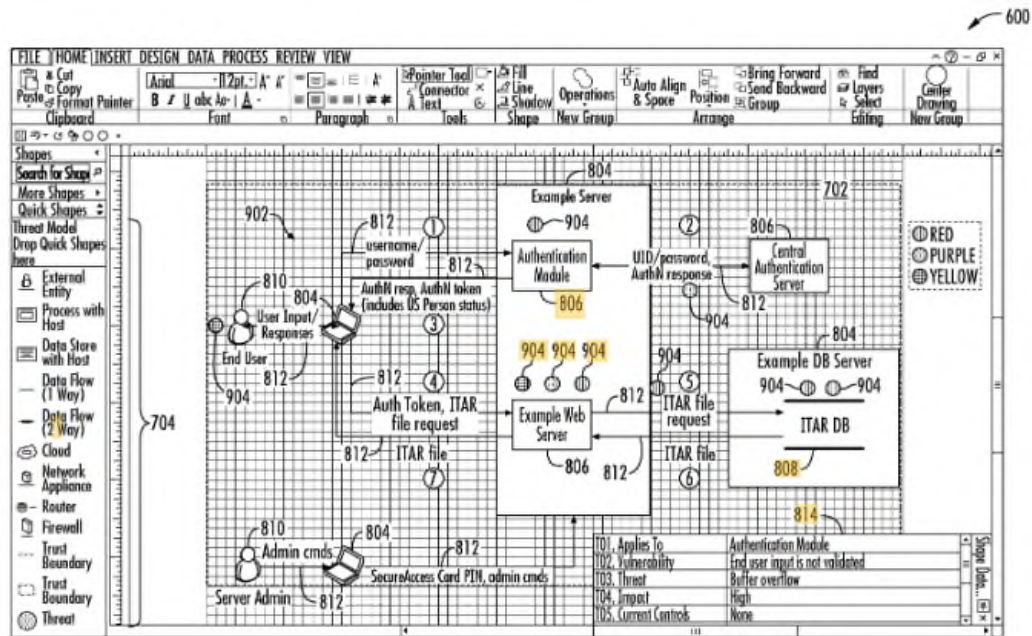
1000

Numbering for this table – this does not correspond to numbering in the Visio diagram.	Security controls that are recommended to bring the Current Risk rating lower.	Risk given that suggested mitigations are implemented.	The data flow diagram (DFD) element(s) that the threat applies to.	Additional clarifying information. If a finding is preliminary, meaning it needs further research indicate “Preliminary” here.	Use to note whether the review process has resulted in acceptance of this threat and associated impact and risk ratings.
REF #	SUGGESTED MITIGATIONS	RESIDUAL RISK	APPLIES TO	REMARKS	REVIEW STATUS
1	Encrypt client-server connections	Medium	Data flows between client app and server.	This is an information disclosure threat that may lead to a follow-on threat of spoofing threat.	Reviewed
2	Protect RPC connections with a protocol that provides integrity-protection (like SSL/TLS)	Medium	Master-to-Backup data flow		Likelihood rating not agreed
3	Fix buffer overflow.	Medium	Login process	CVSS rating of threat indicated high difficulty to reproduce, which is why likelihood is rated Medium	Not Reviewed
4	Use strong two-factor authentication.	Low	Database system	Preliminary: <Describe why finding is preliminary>	Waiting to clear Preliminary status
5	Implement a failover server in the same datacenter as primary server. Implement regional failover server.	Medium	Web server Application server	Preliminary: <Describe why finding is preliminary> Regional failover needed to bring residual risk to Low.	Waiting to clear Preliminary status
6	Background check	Low	Top level sys admins	Not a traditional STRIDE threat. Improper admin designation could result in all STRIDE threats.	Reviewed
7	Log admin success and fail actions.	Low	Application Server		Reviewed
8	Turn on host-based FW	Low	Web server	Type is “Undetermined” as the vulnerability is very general.	Not Reviewed

1002

● YELLOW ● GREEN

FIG. 10B



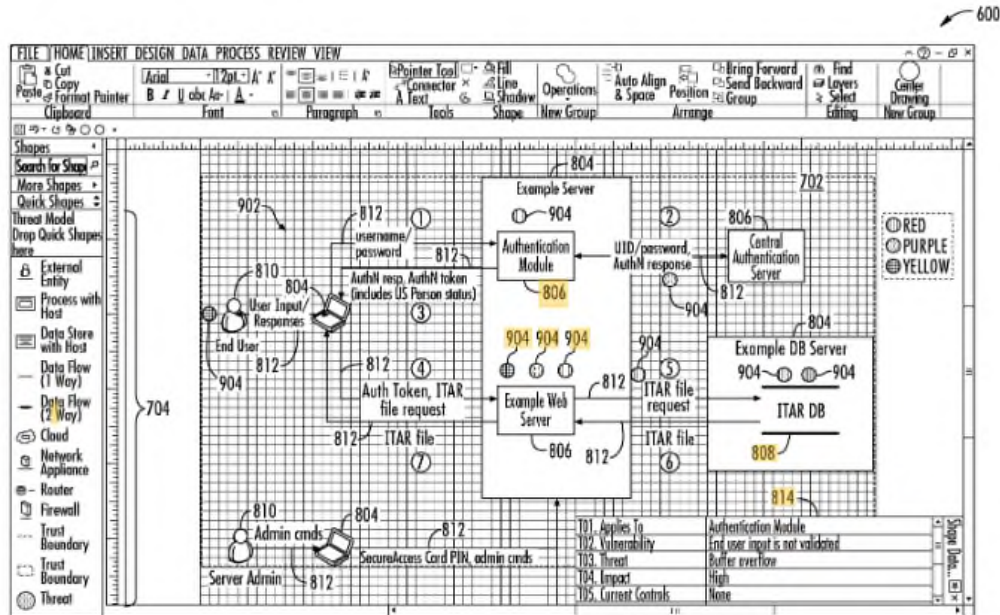
These strategies are intended to mitigate specific threats and are thus associated with the one or more threats as claimed. *See id.*, 2:37-41 (“In some examples, this may include the threat analyzer being configured to identify a measure of current risk of the cybersecurity threat to a particular element, and identify a suggested mitigation implementable to reduce the measure of current risk to a lower, measure of residual risk.”).

75. In my opinion, a POSITA would understand that Jones’ mitigations are compensating controls under the plain and ordinary meaning of the term because compensating controls are mitigations for threats. A POSITA would further understand that Jones’ mitigations may include all well-known mitigation strategies in the art.

76. These compensating controls are further associated with the one or more threats through the one or more databases. *See* Element 1[a].

- e. Element 1[d]. “providing one or more interfaces, including a diagram interface, configured to be displayed on one or more end user computing devices communicatively coupled with the one or more databases;”**

77. In my opinion, Jones discloses this element. Jones discloses “providing one or more interfaces including a diagram interface” because it teaches a graphical user interface (GUI) including data flow diagrams (DFDs). EX-1004, 18:44-57 (“the GUI 700 may include a workspace 702 for composition of a level n DFD from shapes representing its nodes and edges”); *see also id.* at 3:25-28 (“FIG.s 7-9 depict an example graphical user interface in which a DFD, threat-model DFD and their metadata may be composed...”), Figs. 7-9. For example, Fig. 9 illustrates the GUI including these DFDs. *Id.*, 19:10-14.



See also *id.*, 18:30-19:28.

78. Jones further discloses the interface “configured to be displayed on one or more end user computing devices communicatively coupled with the one or more databases” because it teaches a DFD composer including “a general or specific-purpose computing device on which a process,” such as the interface, “may be configured to run.” *Id.*, 8:32-44. Jones further discloses that “[t]he user interfaces may include a display and/or one or more user input interfaces,” which may be “a liquid crystal display (LCD), light-emitting diode display (LED), plasma display panel (PDP) or the like.” *Id.*, 21:4-19. Jones further discloses that its system may be implemented by a computing device—“an apparatus of exemplary implementations of the present disclosure may comprise, include or be embodied in one or more fixed or portable electronic devices. Examples of suitable electronic

devices include a smartphone, tablet computer, laptop computer, desktop computer, workstation computer, server computer or the like.” *Id.*, 20:1-9; *see also* Element 1[a].

- f.* Element 1[e]. “configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model, and;”**

79. In my opinion, Jones discloses this element. Jones discloses “configuring the diagram interface to display a relational diagram of one of a system, an application, and a process” because Jones discloses that the data flow diagram (DFD) “includes shapes for elements including various hosts 804, processes 806, data stores 808 and external entities 810, and data flows 812.” EX-1004, 18:58-62. “The shapes may include a graphic and, in some examples, accompanying text that may be taken from the shape data (e.g., the name of the information system component or type of data flowing in the data flow).” *Id.* at 19:5-9. “For example, the DFD level establishment system may identify a level 2 threat model as appropriate in instances in which the threat model is for any of the following: higher trust level network enclave environments, hybrid access zone, high-trust access zone, Internet facing applications and/or systems...” *Id.* at 5:27-33. A POSITA would understand that this disclosure is similar to the concept of a

multi-process component in a DFD that “is further broken down in a lower-level DFD.” EX-1013, p. 88.

80. Jones further discloses displaying the one of a system, an application, and a process “using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model” because Jones’ discloses an interface that displays a relational diagram (DFDs), the relational diagram defining a threat model. EX-1004, 3:25-28 (“FIG.s 7-9 depict an example graphical user interface in which a DFD, threat-model DFD and their metadata may be composed...”). The interface uses visual representations of its various components using shapes, as shown in Figs. 7-9, and 10B. *Id.*, 18:44-19:28; see also Element 1[d].

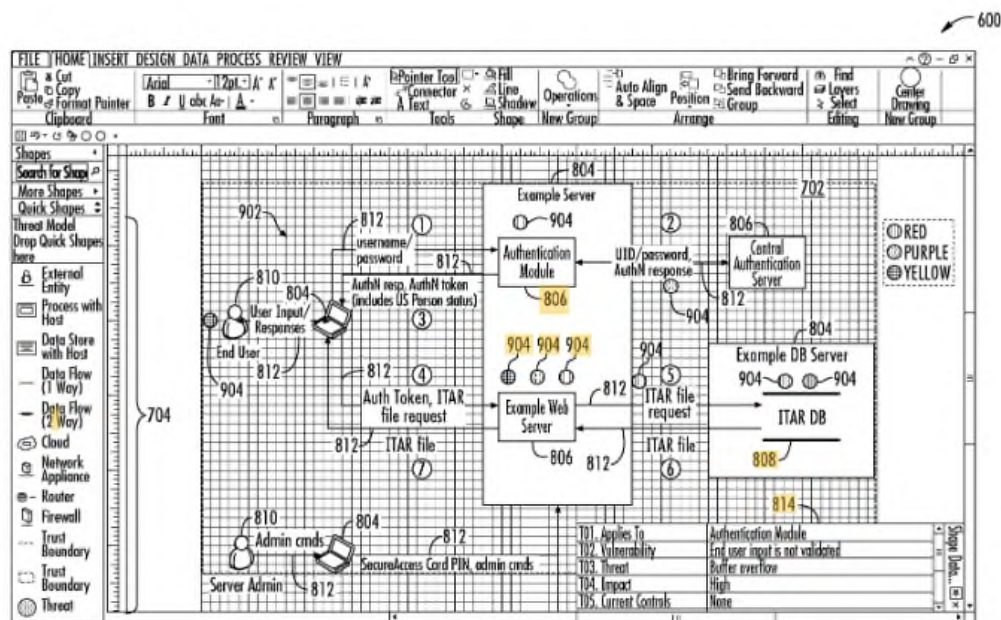


FIG. 9

FIG. 9

1002-

FIG. 10B

- 43-

predefined interrelated group of two or more of the threat model components.”

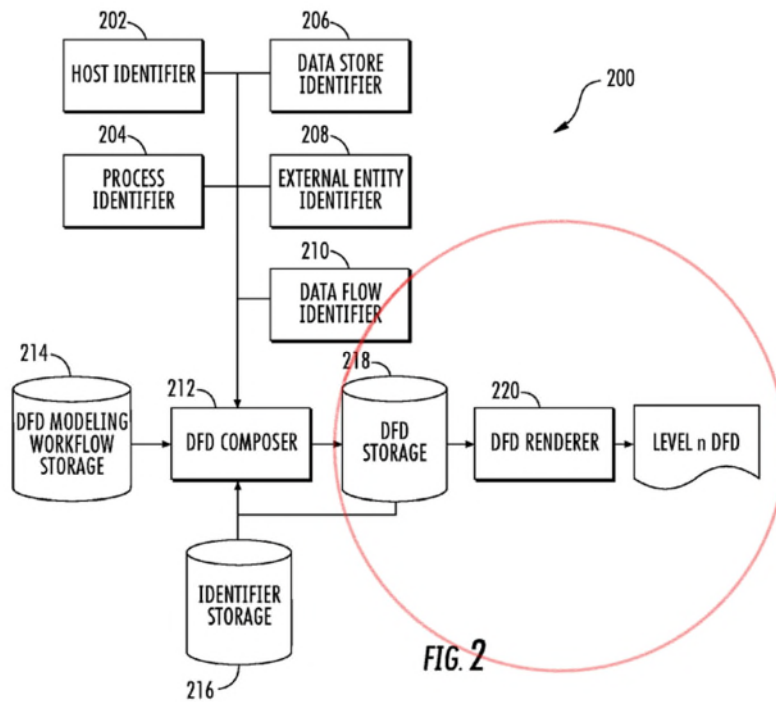
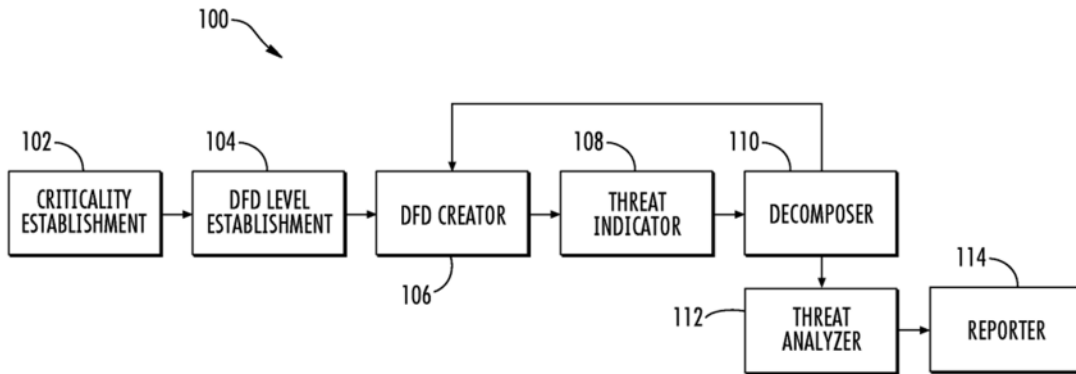
81. In my opinion, Jones discloses this element. See Element 1[p]. Jones discloses that its information system “may include components such as hosts, processes, data stores and/or external entities, and data flows between those components.” EX-1004, 5:4-19. The system then provides a “hierarchical breakdown” of its components at different levels. *Id.* “In this regard, one or more of the information system's components—more often a process, host or data store—may include multiple nested components, one or more of which may include further additional nested components at lower levels of the hierarchy.” *Id.* Jones’ system further may “modify the threat-model DFD for the decomposed components to include their nested components ... thereby producing a level n+1 threat model DFD.” *Id.* at 6:12-34

82. Thus, Jones allows chaining or “nesting” as claimed in Element 1[f] because, in response to user input, the system “add[s] a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group,” creating a level n+1 threat model with one or more nested components, “wherein the component group comprises a predefined interrelated group of two or more of the threat model components.” For example, Figure 9 “illustrates the GUI including a level n threat-model DFD 902 produced from the level n DFD 902 and further including a

See also id. at 4:22-35 (DFD “level establishment system”), 5:10-19 (discussing hierarchal breakdown of components at different levels), 5:20-44, 5:45-53, 5:64-6:11, 7:31-37, 8:23-31, 12:7-21, 12:43-63, 12:64-13:7 (threat model renderer composing a threat model from the components of multiple stored threat models), 15:43-61, 16:37-50, 17:16-31, 17:41-49, 18:44-57, 18:58-60, 19:46-59, Figs. 1-5, 7-9; Element 1[b].



FIG. 9



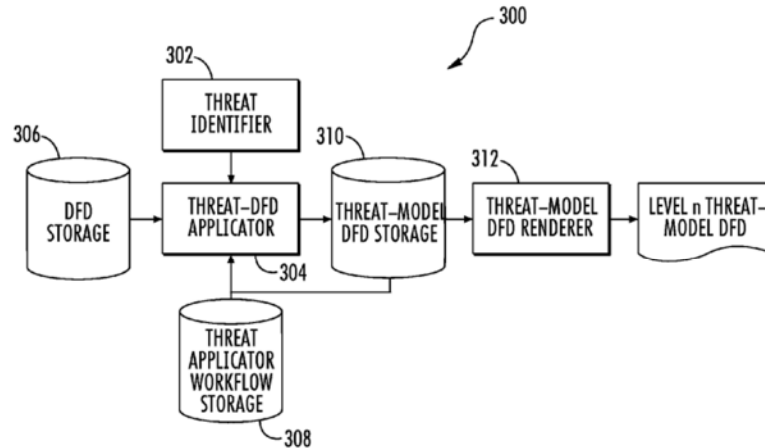


FIG. 3

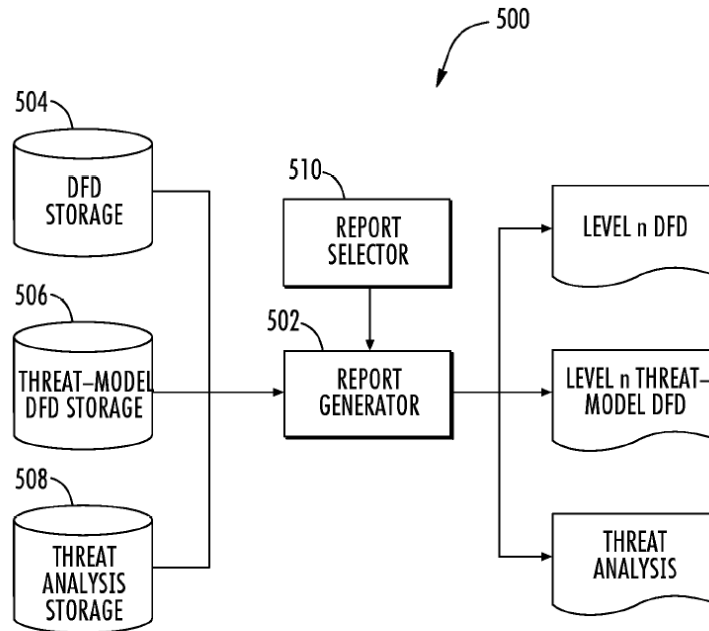


FIG. 5

83. Jones allows for user input through a graphical user interface GUI, as shown in Figure 9. In Jones, the “cybersecurity threats (or rather their shapes) are placed in the workspace 702” within the GUI. *Id.* at 18:44-57 (“the GUI 700 may

include a workspace 702 for composition of a level n DFD from shapes representing its nodes and edges”); *see also id.*, 18:30-43, Figs. 7-9.

84. A POSITA would understand that Jones’ nesting disclosure meets this limitation. *See* Element 1[p]. Indeed, the ’008 patent refers to chaining and nesting as the same concept. EX-1001, 20:23-36 (“When a user adds any of these component groups to a blank or existing diagram/threat model the threat model of the component group is added to (and/or nested within) the threat model of the existing diagram/threat model. . . . This ability is generally termed ‘threat model chaining’ herein.”), 20:46-58 (referring to “nested/chained” threat models), 23:1-13 (“nested or chained threat models”), 24:14-30, 25:18-23, 28:34-41.

2. **Claim 3: “The threat model chaining method of claim 1, further comprising configuring the one or more interfaces to, in response to receiving one or more user inputs, store one or more additional threat model components in the one or more databases, store one or more additional threats in the one or more databases, associate each additional threat with at least one of the additional threat model components through the one or more databases, store one or more additional compensating controls in the one or more databases, and associate each additional compensating control with at least one of the additional threats through the one or more databases.”**

85. In my opinion, Jones discloses this element. *See* Elements 1[p]-1[f]. A POSITA would understand that Jones discloses the steps described in the threat model chaining method of Elements 1[p]-1[f], and that Jones discloses that each of these steps could be performed an additional time. Jones refers consistently to

“one or more” of each of its functions and creating one or more DFDs including the claimed elements. *E.g.*, EX-1004, 4:13-21 (“the system may be configured to perform one or more of its functions or operations under direct operator control.”). Moreover, Figs. 7-9 showing the GUI show multiple threats, threat model components, and compensating controls:

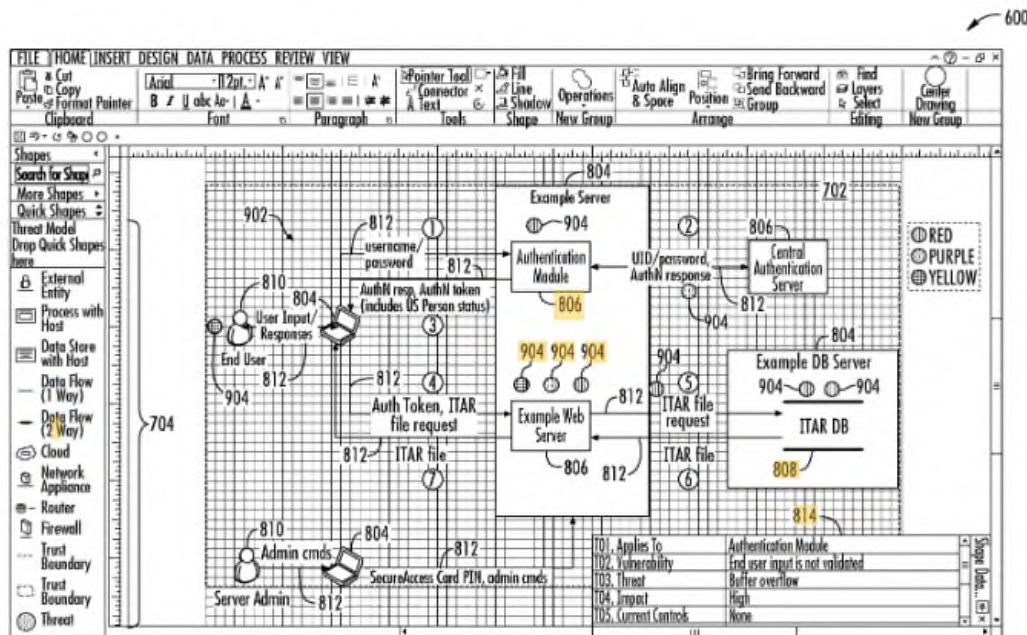


FIG. 9

The exemplary reports in Figs. 10A-10B further show multiple threats, threat model components, and compensating controls in report form. *Id.*, 19:29-45.

C. Ground 2: The Combination of Jones, Zheng, and Keenan Render Claims 1-20 Obvious

86. Ground 1 is incorporated by reference in ground 2. As discussed, Claims 1 and 3 are anticipated by Jones. In my opinion, claims 2 and 4-20 are further rendered obvious by Jones in combination with Zheng and Keenan.

1. **Claim 2: “The threat model chaining method of claim 1, further comprising configuring the diagram interface to, in response to receiving a user selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.”**

87. In my opinion, Zheng discloses this element. Zheng discloses a “threat modeling layer” that visualizes a threat actor and threat target, and a “displayable vector” associating the threat actor and threat target that can “visualize an attack methodology by the threat actor on the threat target.” EX-1005, 2:36-42; *see also id.*, 5:6-24 (“In some embodiments, the visualization module 116 generates and renders the threat modeling layer 204 in a computer display to visualize predicted security objectives, threats and/or vulnerabilities of the application architecture in the base layer 202. The visualization can be rendered in the same application landscape as (e.g., overlays) the base layer 202. Generally, data in the threat modeling layer 204 can be organized into threat agents, vectors, and targets. The threats can also be categorized into different types. Each threat can be visually associated with at least one of (i) a threat actor application, (ii) a threat target application and (iii) a displayable vector connecting the two to represent and visualize a particular attack methodology. For example, a vector connection can be a data flow path between one or more cities or between one or more buildings. A threat can provide one-to-one mapping between a threat actor and a threat target, a

one-to-many mapping, a many-to-one mapping or a many-to-many mapping, depending on the nature of the threat.”), 5:35-47, 7:13-16, 7:17-40, 7:41-48, 9:24-27, 10:10-30, 10:31-60, 10:61-11:3. A POSITA would understand that Zheng’s system may show attack paths of “all” threats because Zheng discloses a system with data related to “know[n] or historical attacks” that can have far-reaching impacts “across the entire ecosystem.” *Id.*, 10:31-60. Moreover, a singular attack path of a threat may comprise “all” threats in a system, and Zheng does not limit itself to identifying less than all threats.

88. A POSITA would have found it obvious to modify Jones’ system to “visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.” *See* Section X.C.19.

2. Claim 4:

a. Element 4[p]. “An attack simulation method, comprising:”

89. In my opinion, Zheng discloses this element. *See* Claim 2 (discussing attack methodologies). “In some embodiments, the security risk analysis tool 100 of the present invention is used to predict future attacks, in addition to detecting current attacks in real time (or near real time). For example, a user can use the data flow module 130 of the system 100 to specify data flows to simulate attacks and/or perform testing to predict future attacks.” EX-1005, 7:17-22. “In some

embodiments, the prediction models and simulations can be used to prepare for zero-day attacks by simulating real potential attacks and behaviors.” *Id.*, 7:34-37.

b. Element 4[a]. “providing one or more databases, the one or more databases comprising:”

90. In my opinion, Jones discloses this element. *See* Element 1[a].

c. Element 4[b]. “a plurality of threat model components stored therein; a plurality of threats stored therein, each threat associated with at least one of the threat model components through the one or more databases; and”

91. In my opinion, Jones discloses this element. *See* Element 1[b].

d. Element 4[c]. “a plurality of compensating controls stored therein, each compensating control associated with at least one of the threats through the one or more databases;”

92. In my opinion, Jones discloses this element. *See* Element 1[c].

e. Element 4[d]. “providing one or more interfaces, including a diagram interface, configured to be displayed on one or more end user computing devices communicatively coupled with the one or more databases;”

93. In my opinion, Jones discloses this element. *See* Element 1[d].

f. Element 4[e]. “configuring the diagram interface to, in response to receiving a user selection of one of the diagrammed threat model components of the first threat model through the one or more interfaces, visually display attack paths of all threats associated with the diagrammed threat model components

which compromise the selected threat model component.”

94. In my opinion, Zheng discloses this element. *See* Claim 2.

- 3. Claim 5: “The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces, visually display one or more attack paths which pass through multiple diagrammed threat model components of the first threat model.”**

95. In my opinion, Zheng discloses this element. Zheng discloses that its “displayable vector” may display one or more attack paths which pass through multiple diagrammed components of the first threat model because Zheng discloses that “a vector connection can be a data flow path between one or more cities or between one or more buildings.” EX-1005, 5:6-24. Moreover, Zheng discloses a “one-to-one mapping between a threat actor and a threat target,” as well as a “one-to-many,” “many-to-one,” and “many-to-many” mapping of threats and threat actors. *Id.*; *see also* Claim 2; Section X.C.19.

96. Moreover, Zheng discloses that “[e]ach vulnerability or attack can have a certain associated impact, such as taking a target application offline, stealing data from the application, etc. Not only does an attack impact directly-targeted applications, it can also have far-reaching impacts across the entire ecosystem.” Ex-1005, 10:43-48.

- 4. Claim 6: “The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response**

to receiving a user toggle of one of the diagrammed compensating controls (hereinafter “first control”) of the first threat model to an on state through the one or more interfaces, toggle all attack paths mitigatable by the first control to a mitigated display state.”

97. In my opinion, Zheng, Jones, and Keenan disclose this element.

Keenan discloses toggling various features on and off. EX-1006 at 12:29-35; 17:19-21. (“The highlighting is preferably accomplished by using the thicker line weighting on the Flow Objects in different color than normally used for lines. Clicking again on the object toggles this feature off. Paths upstream and downstream from up to six objects can be toggled on at the same time. A different highlighting color may be used for each.”). Thus, Keenan discloses a “user toggle” that allows a user to turn a feature on and off.

98. Jones discloses the diagrammed compensating controls and the diagram interface. Elements 1[c]-1[d]. Zheng discloses diagrammed attack paths. Claims 2, 5. A POSITA would have found it obvious to combine these features of Jones and Zheng with the toggling feature of Keenan to “toggle all attack paths mitigatable by the first control to a mitigated display state,” as claimed because, among other reasons, a POSITA would have recognized the utility of using a toggle feature to highlight certain features of the diagrammed threat model as shown in Keenan. Section X.C.19.

5. Claim 7: “The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response

to receiving a user toggle of the first control to an off state through the one or more interfaces, toggle all attack paths mitigatable by the first control to an unmitigated display state.

99. In my opinion, Jones, Zheng, and Keenan disclose this element. See Claim 6 (explaining toggle combination). A POSITA would understand, based on the explanation in claim 6 that attack paths may be toggled on the diagram interface to a mitigated display state, then the attack paths may also be toggled to an unmitigated state. Section X.C.19.

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

100. In my opinion, Jones, Zheng, and Keenan disclose this element. See Claims 6-7. Claims 7 and 8 are substantively identical except for instead of “user toggle” in claim 7, claim 8 uses the term “one or more user inputs through the one or more interfaces to remove the first control from the first threat model.”

However, a POSITA would understand that there is no substantive difference between a “user toggle” in claims 6-7 and “one or more user inputs through one or more interfaces to remove the first control from the first threat model.” In either term, a user inputs into an interface to toggle a control off in the threat model to an unmitigated state. Thus, this element is disclosed. Section X.C.19.

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

101. In my opinion, Jones, Zheng, and Keenan disclose this element. See Claims 6-8. A POSITA would understand that Keenan’s display toggle feature may be incorporated into any element of Jones and Zheng. Therefore, on an interface, a user may toggle off all features except for the attack paths, thus “visually display[ing] only attack paths of all threats associated with a subset of the diagrammed threat model components.” Section X.C.19.

8. **Claim 10: “The attack simulation method of claim 4, further comprising configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces to alter a profile of an attacking component, alter the visually displayed attack paths.”**

102. In my opinion, Zheng and Keenan disclose this element. Zheng discloses displayed attack paths. See Claim 2. Keenan discloses modifying a display. Keenan discloses “a Modify mode, where the user can add, change and delete,” where a user can modify the display. EX-1006, 11:42-56. A POSITA would have found it obvious to combine Keenan’s disclosure of modifying a display with Zheng’s disclosure of displayed attack paths to allow a user through inputs through one or more interfaces to “alter a profile of an attacking component, alter the visually displayed attack paths” as claimed. Section X.C.19; Claims 6-9.

9. **Claim 11: “The attack simulation method of claim 3, further comprising configuring the diagram interface to receive one or more user inputs to add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.”**

103. In my opinion, Jones discloses this element. *See* Claim 1[f].

10. **Claim 12:**

- a. **Element 12[p]. “An attack simulation system, comprising:”**

104. In my opinion, Zheng discloses this element. *See* Element 4[p].

- b. **Element 12[a]. “one or more computing devices communicatively coupled with one or more databases, the one or more computing devices displaying, on one or more displays of the one or more computing devices:”**

105. In my opinion, Jones discloses this element. *See* Element 1[d].

- c. **Element 12[b]. “one or more input interfaces configured to, in response to receiving one or more user inputs, store a plurality of user-defined threat model components in the one or more databases, store a plurality of threats in the one or more databases, associate each of the threats with at least one of the threat model components through the one or more databases, store a plurality of compensating controls in the one or more databases, and associate each compensating control with at least one of the threats through the one or more databases, and;”**

106. In my opinion, Jones discloses this element. *See* Elements 1[a]-1[d].

- d. Element 12[d]. “a diagram interface configured to, in response to receiving one or more user inputs, diagram one of a system, an application, and a process, the diagram including one or more of the threat model components and one or more of the compensating controls, to define a first threat model, the first threat model including all threats associated through the one or more databases with the diagrammed threat model components;”**

107. In my opinion, Jones discloses this element. *See* Elements 1[b]-1[e].

Jones further discloses “the first threat model including all threats associated through the one or more databases with the diagrammed threat model components.” *See* Element 1[a].

- e. Element 12[e]. “wherein the diagram interface is configured to, in response to receiving a selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.”**

108. In my opinion, Zheng discloses this element. *See* Claims 2, 5.

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

109. In my opinion, Zheng and Keenan disclose this element. *See* Claim 6.

- 12. Claim 14: “The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to**

receiving a user input to toggle the first control to an off state, toggle all attack paths mitigatable by the first control to an unmitigated display state.”

110. In my opinion, Zheng and Keenan disclose this element. *See* Claim 7.

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

111. In my opinion, Zheng and Keenan disclose this element. *See* Claim 8.

14. Claim 16: “The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.”

112. In my opinion, Zheng and Keenan disclose this element. *See* Claim 9.

15. Claim 17: “The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, alter a profile of an attacking component, wherein the alteration alters the visually displayed attack paths.”

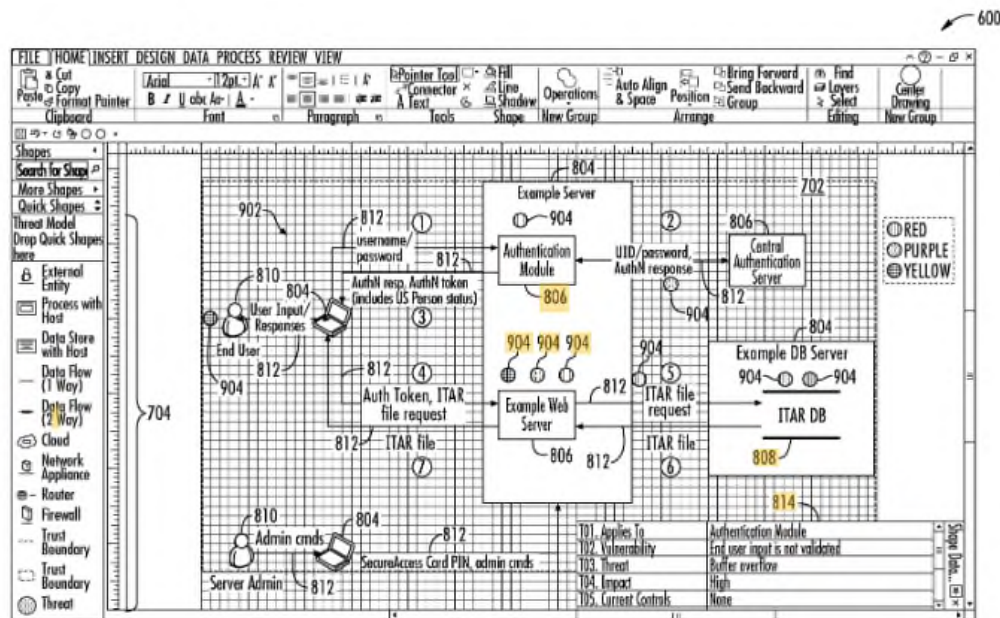
113. In my opinion, Zheng and Keenan disclose this element. *See* Claim

10.

16. Claim 18: “The attack simulation system of claim 12, wherein the one of a system, an application, and a process comprises a computing network.”

114. In my opinion, Jones discloses this element. Jones discloses that
“systems may be networked via standards-based protocols to enable seamless

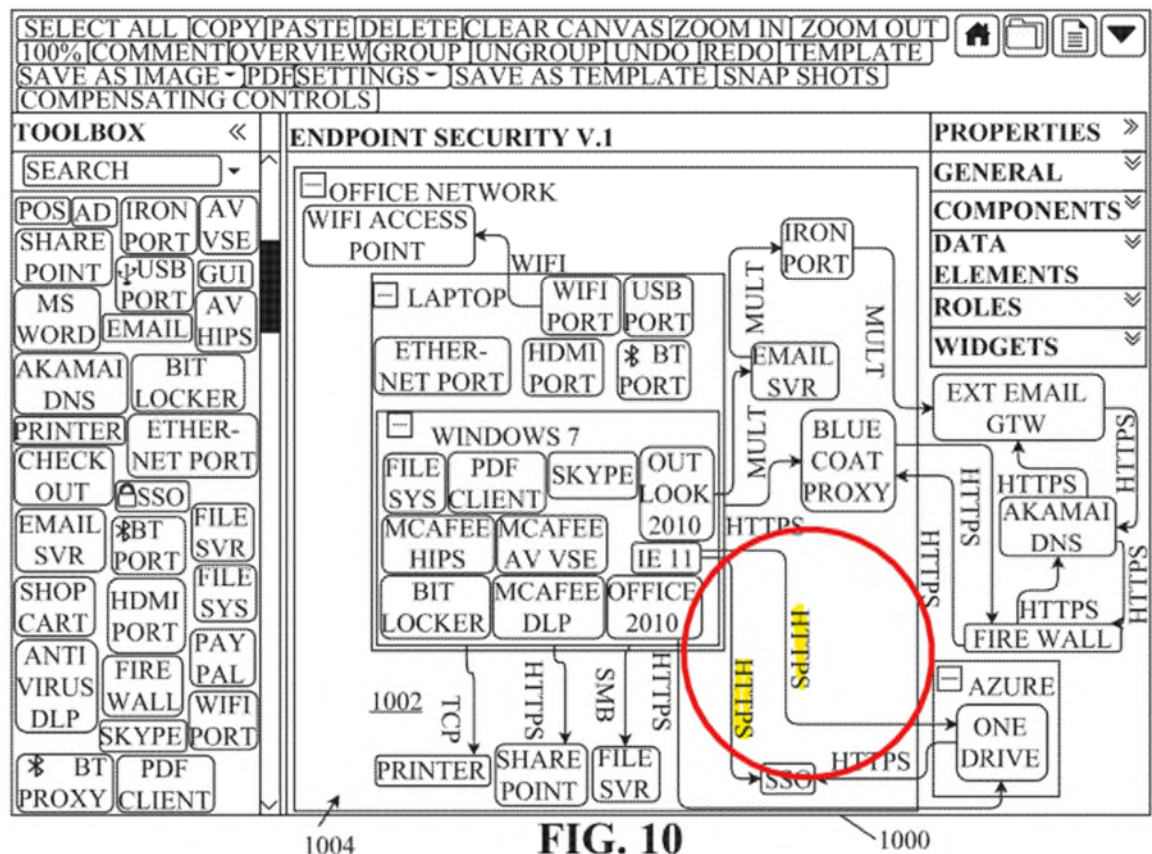
integration of the IT-enabled architecture to implement various information systems.” EX-1004, 1:27-35; *see also id.*, 1:11-26; Element 1[d]. Jones further discloses that its DFDs “may include other relevant components of the complex-system platform configured to implement the information system, such as various network components configured to carry, route, pass, transmit or receive data of the information system.” EX-1004, 7:38-48. “Examples of Suitable network components include a network appliance, firewall, router, cloud computing component and the like.” *Id.*, Figs. 7-9 further show diagrammed network components:



17. **Claim 19:** “The attack simulation system of claim 18, wherein the diagram interface is further configured to, in response to receiving one or more user inputs, diagram a communication protocol between two of the diagrammed threat model

components, the diagrammed communication protocol including an alphanumeric indicator.”

115. In my opinion, Jones discloses this element. The '008 patent explains that “In implementations a communication protocol (protocol) can be defined between components by clicking on a component and dragging the cursor to a second component. This will create an arrow, such as those shown on FIG. 10 between components on the canvas, and will display a default protocol (here the default protocol is HTTPS). ... The alphanumeric descriptions are shown here next to the link arrows,” as shown in Fig. 10:



EX-1001, 16:58-17:11, Fig. 10 (modified). Thus, the diagrammed communication protocol comprising an alphanumeric indicator is as shown in Fig. 10 (e.g., “HTTPS”).

116. Jones discloses this limitation. As shown in Figs. 8-9, Jones’ discloses a diagrammed communication protocol including one or more alphanumeric indicators:

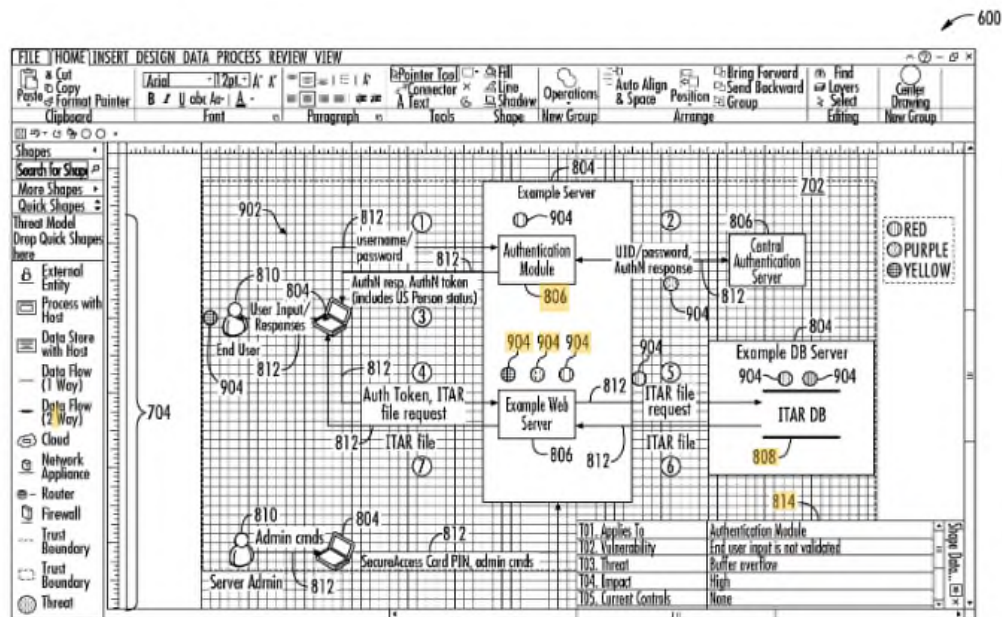


FIG. 9

For example, the communication protocol between the end user 810 and the computing device 804 is “User Input/Responses.” Further, communication protocols between the computing device 804 and the example server(s) 806 include “Auth N token” and “ITAR file request” labels. Thus, Jones discloses this limitation.

18. **Claim 20: “The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.”**

117. In my opinion, Jones discloses this element. See Claim 11.

19. **A POSITA Would Have Been Motivated to Combine Jones, Zheng, and Keenan.**

118. In my opinion, a POSITA would have been motivated to combine Jones, Zheng, and Keenan. First, like the '008 patent, all three references relate to the same general subject matter of generating and displaying threat models on a computer. See EX-1004, Abstract; EX-1005, Abstract; EX-1006, Abstract.

119. Second, Zheng provides express motivation when it discusses the need to minimize the tedious burden on human beings that exists in certain prior art threat modeling software applications:

With the growing complexity of application architecture and application infrastructure, it becomes tedious and often unmanageable to analyze application security across a large portion or an architectural stack. Today's threat modeling applications are often static and require either manual input or antiquated approaches to account for new architecture, code and/or infrastructure....
Accordingly, there is a need for improved systems, methods and apparatuses for a more effective and efficient threat modeling approach in the context of application architecture and infrastructure.

EX-1005, 1:21-34. Adding the teachings of Jones, and Keenan to the system disclosed in Zheng would further Zheng's stated goal of an improved threat modeling system. For example, Zheng recognizes the need to produce threat models faster (in real time or near real time) and using easy-to-understand visualizations. *Id.*, 1:37-45. Most practitioners who create threat models in a manual way look for ways to simplify creating threat models using a computer and understandable visualizations.

120. Third, adding the visual features of Zheng and Keenan described above to the system of Jones would improve the overall user experience. For example, Zheng's disclosure of displaying attack paths would enhance the system of Jones by allowing the user to view attack paths in manner described in Zheng, which would enhance the user's understanding of the potential threats. As another example, Keenan's disclosure of allowing a user to toggle between displaying or hiding certain features in a visual diagram would enhance the system of Jones by providing the user with yet another option for displaying a diagram in the manner best suited for the user's interests at the time. In my opinion, a POSITA would be motivated to include this feature in the system of Jones to allow a user to simplify a diagram by hiding a feature and then displaying that feature again when the user instead wants to view the complete diagram. All human beings sometimes can

better understand a visual presentation when it is simplified, and the ability to toggle a visual feature enables the presentation of a simpler view.

121. Combining the system of Jones with certain features disclosed in Zheng and Keenan would have been within the skillset of a POSITA at the time of the invention and would require no undue experimentation. Displaying and manipulating diagrams on computers was well known at the time and a POSITA would be well versed in such programs. Further, such a combination would have an easily predictable result. Accordingly, in my opinion, a POSITA would have had a reasonable expectation of success. Computer-based threat modeling involves very predictable technologies, and a POSITA would not encounter any insurmountable challenged in implementing this combination.

D. Ground 3: The References of Ground 2 and Yu Render Claims 1-20 Obvious

122. In my opinion, for limitations 1[c], 1[e], 3, 4[c], 4[e], 6, 12[b], 12[c], 13, if it is found that Jones, Zheng, and Keenan do not disclose “compensating controls,” “visual representations of one or more of the compensating controls,” and “the diagram including...one or more of the compensating controls,” then Yu discloses these elements and claims 1-20 are rendered obvious by those references in further combination with Yu.

123. Yu discloses that “resource owners still need to create a threat model to understand their potential exposures and find compensating controls to mitigate

against any damage.” EX-1006, 5:29-32. Yu further discloses, “With a focus on finding ***compensating controls***, this invention provides a resource-centric threat modeling system that allows resource owners to create a threat model while requiring only basic familiarity of the resource’s functions and interactions with other resources. In addition, this invention enables resource owners to match the strength of controls against the frequency of attack and the magnitude of impact from the identified threat vectors to ensure that the controls can sufficiently mitigate the impact in accordance with the resource owner's level of risk tolerance.” *Id.*, 5:54-63. Yu also refers to compensating controls generally as “controls.” *E.g., id.*, 16:11-33. Yu describes how, “[i]n one aspect, the graphical user interface may include one or more categories associated with each of the one or more controls.” *Id.*, 15:9-28; *see also id.*, 16:42-51, 17:55-65.

124. In my opinion, a POSITA would understand that the compensating controls of Yu are the same compensating controls disclosed in the '008 patent because “compensating controls” is a well-understood term in the field of threat modeling. *E.g.*, EX-1015, 1-4.

125. For claim 2, limitation 4[d], claims 5-10, limitation 12[c], and claims 13-17 if it is found that Jones, Zheng, and Keenan do not disclose “attack paths,” then Yu discloses this element. Yu describes a system to show “*attacks* that may be caused along each *threat vector*.” *See* EX-1007, 5:42. Further Yu describes

how to “*dynamically generate a graphical representation of the ... one or more threat vectors...*” See *id.*, Fig. 2.

126. In my opinion, a POSITA would have been motivated to combine the references of ground 2 with Yu. First, like the references of ground 2 and the '008 patent itself, Yu relates to the same general subject matter of generating threat models on a computer. See EX-1007, Abstract.

127. Second, in my opinion, a POSITA would have been motivated specifically to add the “compensating controls” feature and the display of “attack paths” disclosed in Yu to the combined system of Jones, Zheng, and Keenan. Compensating controls were well-known to a POSITA in this timeframe, and a POSITA would naturally wish to be able to display compensating controls in any visual representation of a threat model. *E.g.*, EX-1015, 1-4. To the extent this was not already disclosed in Jones, Zheng, and Keenan, in my opinion, a POSITA would have been motivated to add this feature as taught in Yu because displaying compensating controls would provide a more thorough threat model for the user because the user could then see the mitigation measures that could be taken against various threats. Similarly, a POSITA would have been motivated to display attack paths as taught in Yu in the system of Jones, Zheng, and Keenan.

128. In my opinion, it would have been obvious to combine the references of ground 2 with Yu and a POSITA would have had a reasonable expectation of

success in doing so. Mainly, each reference is of the same field, creation and display of threat modeling, and Jones already acknowledges including mitigation strategies. Thus, a POSITA viewing Jones would be motivated to include in Jones' disclosure all mitigation strategies known in the art for threat modeling, including compensating controls, and a POSTIA would have a reasonable expectation of success in doing so. And because Jones, Zheng, Kennan and Yu describe threat models with display of potential attacks as well as paths of attacks, sometimes described as threat vectors, the combination would be seamless. Computer-based threat modeling involves very predictable technologies, and a POSITA would not encounter any insurmountable challenged in implementing this combination.

E. Ground 4: The References of Ground 3 and Reith Render Claims 1-20 Obvious

129. In my opinion, for limitations 1[e], 11, and 20, if it is found that Jones, Zheng, Keenan, and Yu do not disclose threat model chaining, *i.e.*, redefining a first threat model by including it in a second threat model, Reith discloses these elements, , and claims 1-20 are obvious in view of those references in further combination with Reith. Reith discloses a “Recombinant Threat Models,” as shown in Fig. 4:

400

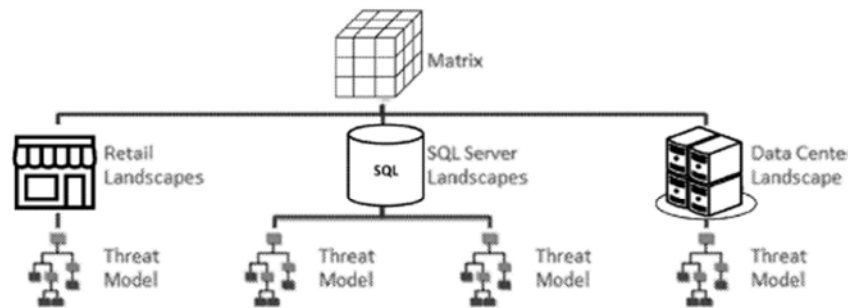


Figure 4

Reith discloses that “[a] Recombinant Threat Model may stand on its own within the threat landscape. Alternatively, multiple Recombinant Threat Models may be interconnected together.” EX-1008, 4:30-44; *see also id.*, 7:37-49, 7:65-8:2, 9:47-56.

130. In my opinion, a POSITA would have been motivated to combine the references of ground 3 with Reith. First, like the references of ground 2 and the '008 patent itself, Reith relates to the same general subject matter of generating threat models on a computer. *See* EX-1008, Abstract.

131. Second, a POSITA would have been motivated to add the threat model chaining feature of Reith to the combined system of Jones, Zheng, Keenan, and Yu. The threat model chaining feature of Reith saves time when the user is building the threat model because it allows the user to incorporate existing threat

models into the new threat model without “recreating the wheel.” A POSITA would have been motivated to create a product that saves time for the user because the user’s time is precious and users have a higher demand for products that save the user time.

132. Combining the combined system of Jones, Zheng, Keenan, and Yu with the threat model chaining feature disclosed in Reith would have been within the skillset of a POSITA at the time of the invention and would require no undue experimentation. Further, such a combination would have an easily predictable result. Accordingly, a POSITA would have had a reasonable expectation of success. Computer-based threat modeling involves very predictable technologies, and a POSITA would not encounter any insurmountable challenged in implementing this combination.

F. Ground 5: The References of Ground 4 and the Knowledge of a POSITA Render Claims 5-8 and 13-15 Obvious

133. In my opinion, to the extent it is found that the combined system of Jones, Zheng, Keenan, Yu, and Reith do not disclose the toggling limitations of claims 5, 6, 7, 8, 13, 14, 15, that limitation would have been known to a POSITA, and those claims are still rendered obvious by further combining that system with the knowledge of a POSITA. A POSITA would understand that toggling an item displayed in a graphical user interface display was a commonly known technique in user interface design, both within and outside of the threat modeling space. The

ability for a user to toggle an item on display is known to be advantageous because, for example, it allows a user to focus on particular concepts within the display and/or it allows a user to view a less cluttered display. In so applying toggling to the system of Jones, Zheng, Keenan, Yu, and Reith a POSITA would arrive at the toggling limitations 5-8 and 13-15.

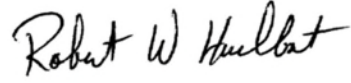
134. It would have been obvious to combine the references of ground 4 with the knowledge of a POSITA regarding toggling, and a POSITA would have had a reasonable expectation of success in doing so. Computer-based threat modeling and graphical user interfaces involve very predictable technologies, and a POSITA would not encounter any insurmountable challenged in implementing this combination.

XI. CONCLUSION

135. Claims 1-20 of the '008 patent are invalid for the reasons discussed above and in the attached Exhibit B.

136. I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct, and that all statements made of my own knowledge are true and that all statements made on information and belief are believed to be true. I understand that willful false statements are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code.

Executed on April 07, 2023 at 5:30 PM ET, Enfield, CT, USA

A handwritten signature in black ink that reads "Robert W. Hurlbut". The signature is written in a cursive style with a horizontal line underneath it.

Robert Hurlbut

EXHIBIT A

ROBERT W. HURLBUT
Principal Application Security Architect / Threat Modeling Lead
Enfield, CT

Phone: 860-515-8459, E-mail: Robert at RobertHurlbut.com

SUMMARY

High performance Principal Application Security Architect and Threat Modeling Lead with outstanding experience as an Application Security Architect / Threat Modeling Architect and Lead / Technical Lead / Developer Trainer & Mentor in diverse arenas, from Fortune 50 organizations to start-ups. Keen eye for detail, with the ability to *concentrate on the big picture while* managing day-to-day operations and *maintaining focus on the company's mission, goals, and revenue*. *Proactive and aggressive in adding value through continuously evaluating and recommending process improvements that streamline operations and processes and lead to significant cost / time reductions.*

- Proven ability in developing concepts and strategies; defining scope, procedures and objectives; managing resources, and interpreting and documenting results.
- Delivering customized training for developers, architects, testers, project managers, and other stakeholders in software / application security topics.
- In-depth understanding of multiple development languages and environments.
- Outstanding ability to drive innovative solutions to complex problems, delivering continuous improvements in performance, cost, quality, and security.
- Strong leader with superior communication skills and the ability to articulate requirements, respond to questions, and convey complex technical information in clear and understandable terms to any audience.
- Calm, flexible, and focused in urgently-paced, demanding, and time-sensitive environments.

PROFESSIONAL COMPETENCIES

- | | | |
|---|-----------------------|------------------------|
| • Security Infrastructures and Patterns | ♦ Secure Coding | ♦ Government |
| • Web, Mobil, and Cloud Security | ♦ Penetration Testing | ♦ Training / Education |
| • Mobile Architecture / Development | ♦ Threat Modeling | ♦ Security Auditing |
| • Object-Oriented Analysis / Design | ♦ DevOps / Agile | ♦ Microservices |
| • Database Architecture and Development | ♦ Project Management | ♦ Problem Resolution |
| • Security / Application Architecture / Development | ♦ DDD / MVC / MVVM | ♦ Microsoft MVP |

PLATFORMS, LANGUAGES & APPLICATIONS

Platforms Windows, Windows Server, Citrix (Terminal Server / Remote Desktop), Linux / UNIX, Mac
Languages C++, C#/.NET, VB, Java, UML, SQL, Python
Databases Microsoft SQL Server, Oracle
Modeling Microsoft Visio, MS Threat Modeling Tool, Threat Modeler, Irius Risk
Security HP Fortify, Checkmarx, Threadfix, SD Elements, Burp Suite, ZAP Proxy, Kali Linux, Gauntlt
Reporting & Project Management Reporting Services for SQL Server, VSView, Microsoft Project

EXPERIENCE

11/21 – Present Aquia, Inc., Enfield, CT

Principal Application Security Architect / Threat Modeling Lead

- Mural, Miro, Lucid Chart, Confluence, Jira
- Leading Threat Modeling Program at Aquia and for various clients including a large Federal Government Agency
- Providing training to many developer teams

9/2017 – 11/2021 Bank of America, Enfield, CT

Senior Vice President, Threat Modeling Senior Architect / Lead

- Microsoft Threat Modeling Tool 2020, Microsoft Visual Studio, Python, C#/.NET.
- Led and further developed Threat Modeling Program at Bank of America which was started in 2016 (see below) as part of GIS CST Architecture (2017- 2021) and then GIS BISO CSW (2021).

- Provided training to 6,000+ associates in In-Person and Virtual sessions. Co-wrote Threat Modeling training that is required in 2021 by 25,000+ developers in the bank.
- Started and led the Threat Modeler in Residence Program from 2019 to 2021. This was a volunteer program of 25+ associates who helped project teams build threat models (essentially a Security Champions Program).
- Worked with project teams to build over 1,000+ threat models over three years as well as empowered others on the GIS CST Architecture Team and other security personnel to work on threat models.

7/2011 – 9/2017 Robert Hurlbut Consulting Services, Enfield, CT
Independent Software Consultant

- Worked on many projects below on a 1099 basis, **each marked with a red plus (+)**.
- Worked on many projects below through **Hurlbut Consulting, Inc.** from 2004 – 2011, **each marked with a red plus (*)**.

+ 07/2011 – 9/2017 Software Consulting Services, Various Clients
Software Security Consultant

- Financial web-based company – secure code reviews, security training (2014-present)
- Finance / Payroll web-based company – secure code reviews, threat modeling (2015 – present)

+ 7/2015 – Current IOActive, Seattle, WA
Software Security Consultant

- Performing threat modeling sessions for client in Silicon Valley, CA.
- Client has mixture of server applications, mobile applications and serves a very large customer base.

***+ 12/2010 – 6/2013, 4/2014 – 9/2015 McKesson Health Solutions, Newton, MA**
Consultant/Team Lead

- Microsoft .NET 4.0 Framework, Windows Presentation Foundation (WPF), Telerik Controls for WPF, SQL Server 2005/2008, Oracle 11g, Windows Communication Foundation (WCF), NHibernate 3.2, FluentNHibernate, Behavior Driven Design (BDD), Test Driven Development (TDD), White, WiX
- Worked within the SCRUM and Agile methodologies as established for the team. Served as a User Interface (UI) Lead Developer on a team using SCRUM (daily stand up meetings, 3 week sprints, stories, etc.).
- Worked on leading a development team using WPF 4.0 for a WPF/XBAP browser application for a care management application. The project was to rewrite an existing older client-server application into a WPF/XBAP application using WPF Web Services.
- Worked with team and management in getting fundamental software practices in place such as Continuous Integration (using TeamCity), BDD and TDD (using StoryQ), and White for white-box testing.
- Worked on strategies for deployment of the WPF/XBAP application and WCF Web Services using Click Once and standard installation practices.
- Worked on improving WCF Web Services performance and NHibernate mapping and performance on the back-end services.
- Worked on back-end integration of health care software products using EDI and Web Services/REST. Created a windows service to manage the integrations for multiple customers.
- Worked with WiX to create install programs for deployment to customers.
- Worked on a WPF project for a customer using XAML, NHibernate.

9/2013 – 9/2014 RSA Security, Inc., Bedford, MA
Software Architect/Consultant

- Microsoft .NET 4.5 Framework, Visual Studio 2013, ASP.NET MVC 4.5, Windows Communication Foundation (WCF) 4.5, Team Foundation Server (TFS) 2013, Test Driven Development (TDD), WiX.
- Provided architecture assistance and mentoring for several projects, including developing a new SDLC process as a way to introduce iterative and agile methodologies for new projects.
- Primary architect and developer on an existing internal/external MVC Web project that used WCF Web Services to interface with an SAP system.
- Provided security code review and improvements to several projects.
- Wrote several data integration tools used for migrating from an older system to a new system.

- Worked to create an updated build, testing, and continuous integration system using TFS 2013.
- Worked to introduce WiX to create install programs for automatic deployments.
- Made improvements to existing secure certificate architecture for existing WCF projects.
- Helped with installation and deployment of secure certificates for several products.

10/2004-6/2011 Hurlbut Consulting, Inc., Agawam, MA

President/Owner/Software Architect/Consultant

- Worked on many projects below on a Corp-to-Corp basis or 1099 basis, **each marked with a red star (*)**.

*** 6/2013 – 9/2013 Mobiquity, Inc., Waltham, MA**

Software Architect/Developer/ Consultant

- Microsoft .NET 4.5 Framework, ASP.NET MVC 4.5, WebAPI 4.5, Visual Studio 2012, Javascript, Mobile tools, Amazon Web Services (AWS) EC2 server.
- Worked on creating a mobile web application using ASP.NET MVC 4.5 and WebAPI 4.5.
- Provided architecture and other assistance to the team.
- Provided security code reviews and improvements for the team.

*** 2/2010 – 11/2010 Cengage Learning, Inc., Boston, MA**

Software Architect/Consultant

- Microsoft .NET 4.0 Framework, SQL Server 2005/2008, SOA using Windows Communication Foundation (WCF), ASP.NET 4.0, Ajax, jQuery, Windows Presentation Foundation (WPF), Microsoft Office 2010, Office OpenXML Toolkit
- Worked within the SCRUM and Agile methodologies as established by the company. Served as a developer on several teams using SCRUM (daily stand up meetings, 3 week sprints, stories, etc.).
- Worked on an Microsoft Office project grading engine using WCF Services, MVC services, and Office OpenXML Toolkit (used automation for Microsoft Access) to grade Microsoft Office student projects and WPF for an instruction builder application that creates the test criteria for grading the projects.

12/2009-4/2010 Verizon Business, Inc., Ashburn, VA

Application Security Consultant

- Microsoft .NET 2.0, 3.5, Java, Ounce Labs - Security Analyst
- Performed security code and PCI reviews for major client (large nationwide retailer)

***+ 10/2009-5/2013 GoGreen EBilling, Inc., Denver, CO**

Software Architect/Developer/Consultant

- Microsoft .NET 3.5 SP1, 4.0, **ASP.NET 4.0**, SQL Server 2005/2008, MVC Pattern, JQuery, JavaScript, AJAX, HTML/CSS, NHibernate / FluentNHibernate / NHibernate.Linq, SOA using Windows Communication Foundation (WCF), Subversion, Cruise Control
- Maintained and enhanced a financial payment web site.
- Introduced Subversion, Cruise Control, Test Driven Development (TDD), and other modern software practices to improve development and maintenance.
- Added ability for political campaigns, non-profit organizations, and other entities to accept financial contributions through the web site.
- Designed and developed highly transactional WCF Services for payment gateway transactions.

*** 11/2008 - 10/2009 Specialized Technology Resources (STR), Inc., Enfield, CT**

Software Architect/Consultant

- Microsoft .NET 3.5 SP1, SQL Server 2005, SOA using Windows Communication Foundation (WCF), Windows Workflow, NHibernate / FluentNHibernate / NHibernate.Linq, ASP.NET 3.5, Ajax, jQuery, ComponentArt ASP.NET Controls, AutoMapper
- Led a programming team as a software architect under a project manager for a new worldwide master file data system.
- Utilized Microsoft MSF, full SDLC, and Agile Methodologies

- Introduced Agile Estimation, Test Driven Development (TDD) and Domain Driven Design (DDD) to the team to efficiently design the new application and begin development. Facilitated stand-up meetings, 2-week iterations, and other Agile techniques for managing the team and code deliverables.

*** 10/2008 Intuit, Inc., Cleveland, OH**

NHibernate and Security Consultant

- Microsoft .NET 2.0, 3.5, SQL Server 2005, SOA using Windows Communication Foundation (WCF), Windows Presentation Foundation (WPF), NHibernate
- Was called in as an NHibernate and software security expert to troubleshoot performance and security issues with an existing software product

*** 11/2007-10/2008 VCI Solutions, Inc., Springfield, MA**

Software Architect/Consultant

- Microsoft .NET 2.0, 3.5, SQL Server 2005, SOA using Windows Communication Foundation (WCF), ASP.NET 2.0/3.5, Telerik ASP.NET Controls, Windows Presentation Foundation (WPF), NHibernate
- Was software architect/programming lead for a new product re-write. The product, Innovation, is a comprehensive media revenue software suite that provides dynamic sales, traffic, and accounting functionality and helps television stations manage the core functions of broadcast and cable operations.
- Introduced Agile Estimation, Test Driven Development (TDD) and Domain Driven Design (DDD) to the team to efficiently design the new application and begin development

*** 08/2007-10/2007 Thomson Financial, Boston, MA**

Consultant

- Microsoft .NET 2.0, SQL Server 2005, ASP.NET 2.0, Web Services, C++
- Added web services support to existing web application to retrieve data

*** 07/2006-07/2007 National Evaluation Systems, Inc., Hadley, MA**

Software Architect/Consultant

- Microsoft .NET 2.0, 3.0, SQL Server 2005, SOA using Windows Communication Foundation (WCF), ASP.NET 2.0
- Taught a two-day class in May, 2006 on “Microsoft .NET and Object Oriented Programming”
- Brought on staff to make software architecture recommendations – introduced Test Driven Development (TDD), Domain Driven Design (DDD), secure programming techniques, and ways to protect sensitive data in SQL Server 2005

*** 11/2006 Gerson Lehrman Group, Inc., New York, NY**

Security Consultant

- Microsoft .NET 2.0, SQL Server 2005, ASP.NET 2.0, Authorization Manager (AzMan)
- Taught 2-day class “Security for the .NET Developer” which covered threat modeling, secure code review, ASP.NET security, database security, Code Access Security, Authorization Manager (AzMan) security, etc.

*** 9/2006 PetEdge, Inc., Peabody, MA**

Security Consultant

- SQL Server 2000, SQL Server 2005
- Performed extensive database security audit of the company’s databases (all SQL Server based)

*** 04/2006-07/2006 Investment Technology Group, Inc., Boston, MA**

Software Architect/Consultant

- Microsoft .NET 1.1, SQL Server 2000
- Performed updates to existing custom code for a CMS application

*** 04/2006 Nexus Energy Software, Inc., Wellesley, MA**

Database Consultant

- Microsoft .NET 1.1, SQL Server 2000

- Analyzed SQL Server 2000 for performance issues, security issues, and other bottlenecks.

*** 03/2006 Algorithmics, Inc., Mount Laurel, NJ**

Security and Database Consultant

- Microsoft .NET 2.0, WinFX 3.0 Beta, WCF, SQL Server 2005, Oracle 10g R2, CodeSmith
- Performed security code audit of the client's smart client application using ClickOnce, WCF services, and SQL Server 2005

*** 12/2005 Telligent Systems, Inc., Dallas, TX**

Security Consultant

- Microsoft .NET 1.1, SQL Server 2000, CodeSmith
- Performed security code audit and penetration testing for one of the client's web sites
- Documented security bugs and provided recommendations for the client

*** 11/2005 – 12/2005 Allscripts, LLC, Chicago, IL**

Security Consultant

- Microsoft .NET 1.1, MESA syslog tools, OpenSSL, SSL
- Developed samples and provided direction for creating secure web services using SSL and other tools
- Developed a syslog .NET client and library to be used for creating medical-based audit messages

*** 12/2004 – 3/2008 iGlobal Technologies, LLC, Cranston, RI**

Computer Consultant/Architect

- Microsoft .NET 1.1/2.0, Visual C++ 7.1, SQL Server 2000, C#/.NET, IIS 6.0, Security, Java 1.5, Tomcat 5.5, Oracle 9i, Macromedia Flash MX 2004, Macromedia Director MX 2004
- Working as Senior Architect/Developer and Project Manager for three sets of teams in developing high volume client/server
- Designed security infrastructure as well as overall physical and software architecture for applications

*** 6/2005 – 10/2007 Salvage Software, Inc., Tucson, AZ and Chicago, IL**

Computer Consultant/Security Consultant

- VS.NET 2003/2005, .NET Framework 1.1/2.0, C#, Installation tools, Access/MSDE/SQL Server 2005 Express, Vista OS development and installation
- Updated original VB 6 and Access application to fix bugs, etc.
- Client contracted my company, Hurlbut Consulting, Inc., to rewrite application in C#/.NET 1.1 using a two-tier client server application approach (i.e. Windows Forms application, central server with a database). Hired another consultant to do most of the development.

*** 7/2003 – 9/2005 Boston Communications Group, Inc., Bedford, MA**

Computer Consultant

- VS.NET 2003, .NET Framework 1.1, ASP.NET, C#, IIS 5/6, Oracle 9i/10g, VB 6.0, COM+, Enterprise Services, .NET Remoting, Web Services, WSE 1.0/2.0, VS.NET Setup and Deployment
- Worked as Senior Developer on project developing a Web-based management system for mobile phones. Phase 1 was written in VB 6.0, COM+, and Oracle 9i. Phase 2 was the previous project re-written as C#, COM+/EnterpriseServices, .NET Remoting, and Oracle 9i.
- Served as Architect for the VB 6.0 version of the above project, and co-Architect for the .NET version of the above project.
- Led **Security Best Practices** seminars for the company to train users/developers on how best to use and develop secure applications within the company.

*** 8/2003 – 11/2005 eDatamate, Inc., Braintree, MA**

Computer/Security Consultant

- Working as Senior Developer/Architect on projects developing Access and Web-based applications. Most applications involved porting older Access applications to SQL Server 2000.

*** 4/2003 – 6/2003 Tier 1 Performance Solutions, Inc., Wilmington, NC**

Computer Consultant

- VS.NET 2003, .NET Framework 1.1, ASP.NET, C#, VB.NET, IIS 5.0, JavaScript, SQL Server 2000, XML, SourceGear Vault
- Working as Developer on a training content management system using C#/VB.NET and ASP.NET. The system is compliant with SCORM training protocols to allow easy integration with other commercial programs.

3/2003 – 12/2003 IT Systems, Inc., Cranston, RI

Computer Consultant/Architect

- VS.NET 2002, .NET Framework 1.0, ASP.NET, VB.NET, IIS 5.0, JavaScript, SQL Server 2000, XML, Visio 2002, Excel
- Working as Senior Architect/Developer on an ASP.NET website for one of the company's clients. The website is a reconfiguration of an old HTML website into the new .NET Framework. The site manages an online catalog of products.

*** 10/2000, 10/2002 – 1/2004 Global Internet Technologies, Cranston, RI**

Computer Consultant/Architect

- Visual Basic 6.0, C#/.NET, IIS 5.0, ASP 2.5, VBScript, JavaScript, ODBC, Access 2000/SQL Server 7.0, SourceSafe 6.0, XML, XSLT, DCOM, Security
- Working as Senior Architect/Developer in a team of two people on the client's site as well as a client of this company.
- Provided security analysis of network and current component systems. Found several areas for improvement, made recommendations, and made changes to improve security across all components and systems.

7/2001 – 10/2002 Geonetics, Inc., Boston, MA

Director of Application Development/Senior Architect

- Visual Interdev 6.0, Visual C++ 6.0, Visual Basic 6.0, Java 1.3, J2EE 1.3, JSP, Java Servlets, ESRI ArcSDE, IIS 5.0, ASP 2.5, VBScript, JavaScript, ADO 2.5, Oracle 8i, SQL Server 2000, SourceSafe 6.0, XML, XSLT, C#, .NET
- Manage/lead/mentor a staff of five developers and two project manager/developers for multiple projects (seven) that are new and/or ongoing at Geonetics.
- Architect/Design/Develop projects for these clients: Massachusetts Highway Department and Central Artery.
- Completed two major projects for Massachusetts Highway involving porting data from old systems to new fiscal management systems. Both projects were completed under budget and on time.

11/2000 - 06/2001 Sprockets.com, Inc., Boston, MA

Computer Consultant

- Visual Interdev 6.0, Visual C++ 6.0, Visual J++ 6.0, IIS 5.0, ASP 2.5, VBScript, JavaScript, ADO 2.5, Oracle 8i, Oracle Objects for OLE, SourceSafe 6.0, XML
- Participated with other C++ and Java developers in a revamping of the main engine for Sprockets.com. The company sells a web collaboration tool for the marketing industry.

4/2000 - 10/2000 Foodline.com, Inc., Boston, MA

Architect/Senior Technical Lead/Computer Consultant

- Visual Interdev 6.0, Visual C++ 6.0, IIS 4.0, ASP 2.0, VBScript, JavaScript, ADO 2.5, SQL Server 7.0, SourceSafe 6.0, XML
- Developer on a small development team (4 people) designing a co-branded sites for the main site. Foodline.com allows customers to make restaurant reservations online.

1/2000 - 3/2000 Centra Software, Inc., Lexington, MA

Computer Consultant

- Visual J++ 6.0, Visual Interdev 6.0, IIS 4.0, MTS 2.0, ASP 2.0, VBScript, JavaScript, ADO 2.1, Site Server 3.0 (Commerce), SQL Server 7.0, ClearCase
- Developer on a small development team (6 people) designing an interface for e-collaboration software marketed by the company. Use of ASP for the front-end work and Java components for the middle/business tiers.

7/1999 - 12/1999 Bain & Company, Inc., Boston, MA

Architect/Computer Consultant

- Visual Basic 6.0, Visual Interdev 6.0, IIS 4.0, MTS 2.0, ASP 2.0, VBScript, JavaScript, ADO 2.1, SQL Server 6.5/7.0
- Project lead/mentor/architect of a small development team designing an information retrieval system for the company Intranet that allows marketing consultants to obtain documents from the company database and from the Internet in one web interface. The Intranet site services 28 offices worldwide.

2/1999 - 6/2001 The Naughton Company, Hingham, MA

Architect/Computer Consultant

- Visual Basic 6.0, Visual C++ 6.0/ATL/COM, Visual Interdev 6.0, IIS 4.0, MTS 2.0, ASP 2.0, VBScript, JavaScript, ADO 2.0, SQL Server 6.5/7.0
- Developing web applications for one of the company's Real Estate sites.

1/1999 - 6/1999 Fidelity Investments, Smithfield, RI

Computer Consultant

- Visual Basic 6.0, Visual C++ 6.0, Oracle 7.3/8.0, InstallShield 5.5, Crystal Reports 6.0
- Designer/developer of COM business objects using MFC/ATL/C++ for retirement fund applications. Prototype user interfaces in Visual Basic.
- Wrote technical and functional specifications for enhancements of retirement applications.

9/1998 - 12/1998 Staples (E-Commerce group) , Westborough, MA

Computer Consultant / Technical Lead

- Visual Basic 5.0, Microsoft Access 97, SQL Server 6.5, NetSoft (AS/400 Interface), InstallShield 5.5, Crystal Reports 4.5/5.0, Active Server Pages, IIS 4.0, Crystal Reports, InstallShield
- Developed/updated applications for order processing through telephone and online connections. Extensive DBA work with SQL Server for projects.

3/1997 - 8/1997, 3/1998 - 9/1998 Medtronic, Inc. , Danvers, MA

Computer Consultant

- Visual Basic 4.0/5.0, Microsoft Access 2.0/97, Visual FoxPro, IBM Client Access (AS/400 Interface), Crystal Reports 4.5/5.0
- Developed interface to AS/400 database servers in Japan to poll inventory data.

9/1997 - 2/1998 Registry of Motor Vehicles, Boston, MA

Computer Consultant

- Visual Basic 5.0, Oracle 7.3, PL/SQL, VS View 2.0
- Technical lead/developer of five-member development team.
- Three-tier client/server application for tracking dealer registration license plates.

9/1996 - 3/1997 Mass Save, Inc., Marlborough, MA

Computer Consultant

- Visual Basic 4.0, Microsoft Access 2.0, SQL Server 6.5, Crystal Reports 4.0
- Completed multi-user applications for updating company database

9/1995 - 9/1996 Boston Voice, Inc., Boston, MA

Computer Programmer

- C/C++ (Borland), Microsoft Access 2.0, Clipper
- Completed projects that enabled automated processing of jobs and reports and to synchronize contact manager databases.

5/1994 - 8/1995 Intelesis, Inc., Columbus, IN

Computer Systems Specialist/Programmer

- Visual Basic 3.0, Microsoft Access 2.0
- Completed software projects that enabled the company to track telecommunications data.

5/1991 - 9/1993 DAC Services, Tulsa, OK

Software Engineer/ Programmer

- C, Paradox
- Completed software projects that enabled voice mail screening.

6/1986 - 5/1991 Southwestern Power Administration, U.S. Department of Energy, Tulsa, OK

Engineering Technician (Student Trainee)

- C, FORTRAN, dBase III+, PRIME mainframe
- Developed engineering applications.

INDEPENDENT RESEARCH, SPEAKING ENGAGEMENTS, & WRITING

- Co-wrote Threat Modeling Manifesto with 14 other industry experts on Threat Modeling in 2020 (<https://threatmodelingmanifesto.org>)
- Wrote series of articles on *Security Best Practices* for code and database development for .NET community.
- Wrote article on *SQL Injection for .NET Developers Journal*.
- Frequently wrote technical content on web blog (<https://roberthurlbut.com/blog>).
- Speaker at user groups and national / international conferences on security (Application Security / Threat Modeling), .NET, and developer topics.
- Wrote courses for NHibernate training, ASP.NET MVC 2.0 training, OWASP security courses for LearnNowOnline.
- Manage two local user groups, one on architecture (since 2004), and one on security (since 2016).
- Co-hosted application security podcast.

EDUCATION

Master of Science, Cyber Security, Southern New Hampshire University, Manchester, NH, 2020

Bachelor of Science, Mathematics, Oklahoma State University, Stillwater, OK, 1990

CERTIFICATION

(ISC)2 Certified Secure Software Lifecycle Professional (CSSLP), 2014 - 2023

MANAGEMENT & MENTORING COMPETENCIES

Lead Developer / Architect / Mentor / Project Manager / Director

- Communication & organizational skills
- Mentoring & encouraging best work from team members
- Creating work schedules & weekly staff meetings
- Ongoing consultation
- Understanding business challenges
- Applying technical experience to develop team-based solutions

EXHIBIT B

US 10,699,008 Threat Model Chaining and Attack Simulation Systems and Related Methods	US 9,602,529 (“Jones”)
1[p]. A threat model chaining method, comprising:	The Jones reference discloses this claim element. For example, Jones discloses: “The present disclosure relates generally to cybersecurity and, in particular, to modeling and analysis of cybersecurity threats in complex-system (e.g., aviation) platforms.” Jones at 1:5-7. “The threat indicator may be configured to identify a cybersecurity threat to a particular element of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat model DFD for the information system. Similar to the DFD creator, the threat indicator may provide structured information including attributes of the cybersecurity threat, and may do so in metadata associated with the secondary node of the threat-model DFD. This structured information may include, for example, a description of the cybersecurity threat and a Vulnerability giving rise thereto, a description of any current security controls designed to mitigate the cyber security threat or the like.” Jones at 2:20-32 “Example implementations of the present disclosure are generally directed to modeling and analysis of cybersecurity threats in a complex-system platform such as that of an aircraft. A complex-system (e.g., aviation) platform may refer to a hardware architecture including one or more systems of a complex-system, and software framework including one or more application frameworks, that enable software such as particularly application software to operate the complex system or one or more of its systems.” Jones at 3:52-60 “The system 100 may include one or more of each of a number of different subsystems (each an individual system) coupled to one another for performing one or more functions or operations. As shown in FIG. 1, for example, the system may include a criticality establishment system 102, data flow diagram (DFD) level establishment system 104, DFD creator 106, threat indicator 108, decomposer 110, threat analyzer 112 and/or reporter 114. Although shown as part of the modeling and analysis system, one or more of the criticality establishment system, DFD level establishment system, DFD creator, threat indicator, decomposer, threat

	analyzer and/or reporter may instead be separate from but in communication with the modeling and analysis system.” Jones at 4:22-35 “In some examples, the information system may be describable in terms of a hierarchical breakdown (hereinafter referred to as a “hierarchy”) of its components (interconnected by appropriate data flows) at different levels. In this regard, one or more of the information system's components—more often a process, host or data store—may include multiple nested components, one or more of which may include further additional nested components at lower levels of the hierarchy. The DFD level establishment system 104 may be configured to assess various criteria of the information system to identify an appropriate level of threat model—threat-model data flow diagram (DFD)—to produce for the information system. In some examples, various criteria of the information system may be associated with various levels, and the appropriate level may identified by matching criteria to a level. For example, the DFD level establishment system may identify a level 2 threat model as appropriate in instances in which the threat model is for any of the following: higher trust level network enclave environments, hybrid access Zone, high-trust access Zone, Internet facing applications and/or systems with transitive access, perimeter-related systems. In instances in which the threat model is not for any of the aforementioned, a level 2 threat model may still be appropriate in instances in which it is based on data classification that application or system stores and/or processes for any of the following: sensitive or highly-sensitive personally identifiable information (PII), own or third-party proprietary, critical technical information (CTI), export controlled EAR, ITAR, material non-public or national security information, trade secret or the like. And in instances in which none of the foregoing are met, the DFD level establishment system may identify a level 1 threat model as appropriate. The DFD creator 106 may be configured to identify elements of the information system, and compose a DFD for the information system from those elements and in accordance with the threat-model level identified by the DFD level establishment system 104. The DFD may include nodes representing the components and edges representing the data flows. The DFD represent the information system at some level n of the hierarchy, and may at times be referred to as a level in DFD (e.g., level 2 DFD).” Jones at 5:10-53 “The threat indicator 108 may be configured to identify a cybersecurity threat to a particular element of the elements of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system— this threat-model DFD at times referred to as a level in threat-model DFD (e.g., level 2 threat-model DFD). Similar to the DFD creator, the threat indicator may provide structured information including attributes of the
--	--

	cybersecurity threat, and may do so in metadata associated with the secondary node of the threat-model DFD. This structured information may include, for example, a description of the cybersecurity threat and a Vulnerability giving rise thereto, a description of any current security controls designed to mitigate the cybersecurity threat or the like.” Jones at 5:64-6:11 “In some examples it may be desirable to look deeper into one or more components of the information system, Such as to provide a more thorough analysis of those components or their cybersecurity threats. In these examples, the decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows therebetween. The decomposer may then provide feedback of its decomposition to the DFD creator 106, which may modify the threat-model DFD for the decomposed components to include their nested components and data flows (and appropriate metadata), thereby producing a level n+1 threat-model DFD. And again, the threat indicator 108 may be applied to identify any cybersecurity threats to elements (nested components and data flows) of the decomposed components, and add appropriate secondary nodes (and appropriate metadata) representing those threats. Or instead of modifying the existing threat-model DFD, in some examples, the DFD creator and threat indicator may begin again to compose a new DFD and threat-model DFD for this level of the hierarchy. This decomposition and follow-on modeling of the information system's components and threats may continue until a desired level of the information system is achieved.” Jones at 6:12-34. “The identifiers 202-210 may be coupled to a DFD composer 212 configured to communicate with the identifiers to receive the identification of or identify components and data flows and their attributes, compose a level in DFD representing components and data flows and including metadata with structured information including attributes of the components and data flows.” Jones at 7:31-37 “In some examples, the DFD composer 212 may compose the metadata attributes of the components and data flows of the information system without itself composing the DFD. In these examples, the DFD composer may communicate to the DFD storage, the metadata attributes of the information system for a level in DFD. In these examples, the stored metadata attributes may be accessed by a separate DFD renderer 220 configured to compose the level in DFD from the metadata attributes.” Jones at 8:23-31 “The threat-DFD applicator 304 configured to receive the identification of or identify cybersecurity threats (and their attributes) to components and
--	---

	data flows of the information system. The threat-DFD applicator may also be configured to receive a level in DFD for an information system—or in Some examples the metadata attributes of the information system for a level in DFD, such as from a DFD storage 306 (e.g., file storage, database storage, cloud storage). The DFD storage may be resident with the threat indicator 300, or may be separate from and in communication with the threat indicator, and in Some examples may correspond to DFD storage 218. And again, the DFD and its metadata may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types.” Jones at 12:7-21 “The threat-DFD applicator 304 may be configured to apply secondary nodes representing the cybersecurity threats to the DFD, and include metadata with structured information including attributes of the cybersecurity threats. The threat-DFD applicator may thereby produce a level in threat-model DFD for the information system. The threat DFD applicator may be configured to communicate the threat-model DFD (including the metadata attributes for elements of the information system and cybersecurity threats thereto), such as to a threat-model DFD storage 310 (e.g., file storage, database storage, cloud storage) for later retrieval. Similar to the DFD storage 306, the threat-model DFD storage may be resident with the threat indicator 300, or may be separate from and in communication with the threat indicator. Also, similar to the DFD, the threat-model DFD and its metadata may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types. And in some examples, a previously-stored threat-model DFD may be retrieved from the threat-model DFD storage by the threat DFD applicator to produce a new threat-model DFD.” Jones at 12:43-63 “In some examples, the threat-DFD applicator 304 may compose the metadata attributes of cybersecurity threats to the components and data flows of the information system without itself composing the threat-model DFD. In these examples, the threat-DFD applicator may communicate to the threat-model DFD storage, the metadata attributes of the information system and cybersecurity threats for a level in threat-model DFD. In these examples, the stored metadata attributes may be accessed by a separate threat-model renderer 312 configured to compose the level in threat-model DFD from the metadata attributes.” Jones at 12:64-13:7 “The analysis-DFD applicator 408 may be configured to receive the current-risk rating, Suggested mitigation and residual-risk rating from the current-risk calculator 402. mitigation identifier 404 and residual-risk calculator 406, the threat analyzer 400, or communicate with those components to calculate or identify the current-risk rating, Suggested
--	---

	mitigation and residual-risk rating. The threat-DFD applicator may also be configured to receive a level in threat model DFD for the information system—or in some examples the metadata attributes of the information system and cybersecurity threats for a level in threat-model DFD, such as from a threat-model DFD storage 412 (e.g., file storage, database storage, cloud storage). The threat-model DFD storage may be resident with the threat analyzer, or may be separate from and in communication with the threat analyzer, and in some examples may correspond to threat model DFD storage 310—the threat-model DFD and its metadata again being formatted and stored in any of a number of different manners.” Jones at 15:43-61 “By the above, the analysis-DFD applicator 408 may produce a threat analysis that includes at least the level in threat-model DFD (together with or simply including meta data for the information system's elements and cybersecurity threats), with metadata including further attributes of the cybersecurity threat. The analysis-DFD applicator may be configured to communicate the threat analysis, Such as to a threat analysis storage 414 (e.g., file storage, database storage, cloud storage) for later retrieval. The threat analysis storage may be resident with the threat analyzer 400, or may be separate from and in communication with the threat analyzer. In some examples, a previously-stored threat analysis may be retrieved from the threat analysis storage by the threat analyzer to produce a new threat analysis.” Jones at 16:37-50 “The report generator 502 may be configured to retrieve any of a number of different pieces of information or data regarding an information system, its components and data flows, and/or cybersecurity threats, from one or more of the storage 504, 506, 508. For example, the report generator may retrieve from the DFD storage, a level in DFD for an information system (or simply the metadata attributes of the information system). Additionally or alternatively, the report generator may retrieve from the threat-model DFD storage, a level in threat-model DFD for the information system (or simply the metadata attributes of the information system and cybersecurity threats). And further additionally or alternatively, the report generator may retrieve a threat analysis for the information system (or simply the metadata attributes and further attributes of the information system and cyber security threats).” Jones at 17:16-31 “Graphically, the report generator may generate drawings of one or more of a level in DFD, level in threat-model DFD and/or threat analysis. Through the report selector, the operator may in some examples select the level (select n) of the DFD or threat-model DFD, a number of dependencies between information systems or components of information
--	---

	systems for which to generate reports (e.g., system. A depends on system B, which depends on system C).” Jones at 17:41-49 “As shown in FIG. 7, in some examples, the GUI 700 may include a workspace 702 for composition of a level in DFD from shapes representing its nodes and edges. In some examples, as shown, the GUI may provide a stencil 704 with a collection of shapes for respective types of components (e.g., host, process, data store, external entity) and data flows of an information system, cybersecurity threats, and perhaps also various relevant components of the complex-system platform configured to implement the information system. And in Some examples, these shapes may be configured to accept shape data, which may be specifically configured for types of attributes of the information systems components (e.g., host, process, data store, external entity) and data flows, as well as the cybersecurity threats.” Jones at 18:44-57 “FIG. 8 illustrates the GUI 700 including various shapes placed in the workspace 702 and arranged to compose a level in DFD 802 for an information system.” Jones at 18:58-60 “FIG. 9 illustrates the GUI including a level in threat-model DFD902 produced from the level in DFD902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD. Similar to elements of the information system, as or after the cybersecurity threats (or rather their shapes) are placed in the workspace 702, attributes and even further attributes of the cybersecurity threats may be entered for their shapes. Also similar to before, in Some examples, the window 814 may be recalled for each of the shapes, in which data for a shape and thus attributes of a cybersecurity threat may be entered, and thereby included as structured information in metadata associated with the shape (and thus secondary node). FIG. 9 illustrates an example in which the window presents fields for receiving or otherwise presenting attributes of the cybersecurity threat “Buffer overflow.” Again, the shapes for the cybersecurity threats may include a graphic and, in some examples, the graphic may be color coded to various shape data Such as the current-risk rating.” Jones at 19:10-28 “According to example implementations of the present disclosure, the system 100 for modeling and analysis of cybersecurity threats and its Subsystems including the criticality establishment system 102, DFD level establishment system 104, DFD creator 106, threat indicator 108, decomposer 110, threat analyzer 112 and reporter 114 may be implemented by various means. Similarly, the examples of a DFD creator 200, threat indicator 300, threat analyzer 400 and reporter 500, including each of their respective elements, may be implemented by various means according to
--	--

	example implementations. Means for implementing the systems, Subsystems and their respective elements may include hardware, alone or under direction of one or more computer programs from a computer-readable storage medium.” Jones at 19:46-59 Figs. 1-5, 7-9
1[a]. providing one or more databases, the one or more databases comprising:	The Jones reference discloses this claim element. For example, Jones discloses: “As described herein, information and other data may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types. Examples of suitable types of storage as described herein include file storage, database storage, cloud storage or the like.” Jones at 8:4-9. “The DFD composer 212 may be configured to communicate the DFD (including the metadata attributes), such as to a DFD storage 218 for later retrieval. The DFD storage may be resident with the DFD creator 200, or may be separate from and in communication with the DFD creator. The DFD and its metadata may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types (e.g., file storage, database storage, cloud storage). In some examples, a previously-stored DFD may be retrieved from the DFD storage by the DFD composer to compose a new DFD. In some examples, the DFD composer 212 may compose the metadata attributes of the components and data flows of the information system without itself composing the DFD. In these examples, the DFD composer may communicate to the DFD storage, the metadata attributes of the information system for a level in DFD. In these examples, the stored metadata attributes may be accessed by a separate DFD renderer 220 configured to compose the level in DFD from the metadata attributes.” Jones at 8:10-31. “A data store identified by the DFD composer 212 in communication with the data store identifier 206 may include, for example, a database Such as a relational data base (Oracle or SQL Server database, MySQL database), a directory (e.g., active directory, lightweight directory access protocol—LDAP directory), flat file or the like, that may be run or otherwise maintained or accessed by a host.” Jones at 10:26-34 “The threat-DFD applicator 304 configured to receive the identification of or identify cybersecurity threats (and their attributes) to components and data flows of the information system. The threat-DFD applicator may also be configured to receive a level in DFD for an information system—or in

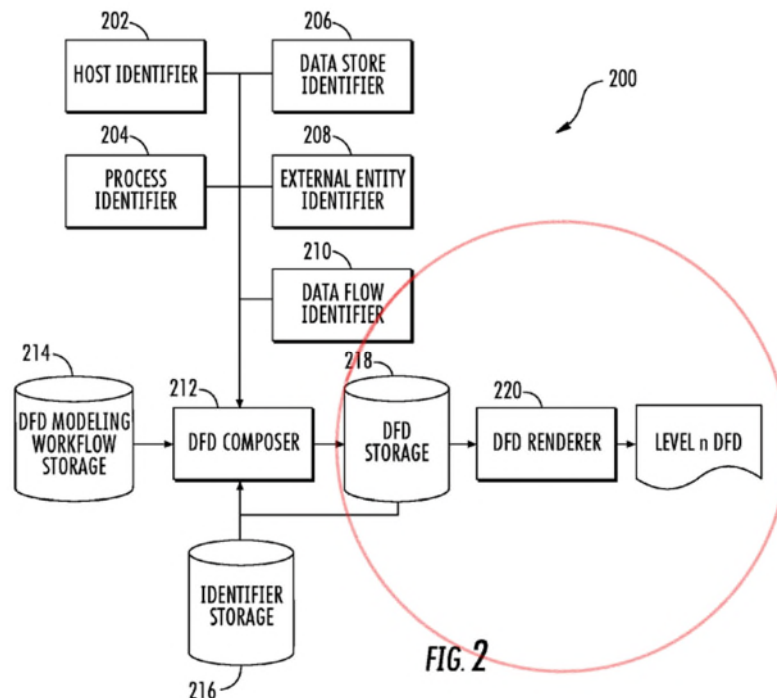
	Some examples the metadata attributes of the information system for a level in DFD, such as from a DFD storage 306 (e.g., file storage, database storage, cloud storage). The DFD storage may be resident with the threat indicator 300, or may be separate from and in communication with the threat indicator, and in Some examples may correspond to DFD storage 218. And again, the DFD and its metadata may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types.” Jones at 12:7-21 “The threat DFD applicator may be configured to communicate the threat-model DFD (including the metadata attributes for elements of the information system and cybersecurity threats thereto), such as to a threat-model DFD storage 310 (e.g., file storage, database storage, cloud storage) for later retrieval. Similar to the DFD storage 306, the threat-model DFD storage may be resident with the threat indicator 300, or may be separate from and in communication with the threat indicator. Also, similar to the DFD, the threat-model DFD and its metadata may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types. And in some examples, a previously-stored threat-model DFD may be retrieved from the threat-model DFD storage by the threat DFD applicator to produce a new threat-model DFD.” Jones at 12:49-63 “In some examples, the threat-DFD applicator 304 may compose the metadata attributes of cybersecurity threats to the components and data flows of the information system without itself composing the threat-model DFD. In these examples, the threat-DFD applicator may communicate to the threat-model DFD storage, the metadata attributes of the information system and cybersecurity threats for a level in threat-model DFD. In these examples, the stored metadata attributes may be accessed by a separate threat-model renderer 312 configured to compose the level in threat-model DFD from the metadata attributes.” Jones at 12:67-13:7 “In examples involving the collection of information, the analysis-DFD applicator 408 may be coupled to a threat analysis workflow storage 410 (e.g., file storage, database storage, cloud storage) resident with or separate from but in communication with the threat analyzer 400.” Jones at 15:18-22. “The threat-DFD applicator may also be configured to receive a level in threat model DFD for the information system—or in some examples the metadata attributes of the information system and cybersecurity threats for a level in threat-model DFD, such as from a threat-model DFD storage 412 (e.g., file storage, database storage, cloud storage). The threat-model DFD storage may be resident with the threat analyzer, or may be separate from
--	--

and in communication with the threat analyzer, and in some examples may correspond to threat model DFD storage 310)—the threat-model DFD and its metadata again being formatted and stored in any of a number of different manners.” Jones at 15:49-61

“As shown, the reporter 500 may include a report generator 502 coupled to one or more storage such as a DFD storage 504, threat-model DFD storage 506 and/or threat analysis storage 508. This storage may be resident with the reporter, or may be separate from and in communication with the reporter, or some storage may be resident while other storage may be separate. In some examples, the DFD storage 504, threat-model DFD storage 506 and threat analysis storage 508 may correspond to DFD storage 218, 306 threat-model DFD storage 310, 412 and threat analysis storage 414, respectively.” Jones at 17:1-15

“For example, the report generator may retrieve from the DFD storage, a level in DFD for an information system (or simply the metadata attributes of the information system). Additionally or alternatively, the report generator may retrieve from the threat-model DFD storage, a level in threat-model DFD for the information system (or simply the metadata attributes of the information system and cybersecurity threats).” Jones at 17:20-27

Figs. 2-3, 9



Jones at Fig. 2 emphasis added

1[b]. a plurality of threat model components stored therein; a plurality of threats stored therein, each threat associated with at least one of the threat model components through the one or more databases; and	The Jones reference discloses this claim element. For example, Jones discloses: “A system is provided for modeling and analysis of cyber security threats may include a data flow diagram (DFD) creator, threat indicator and threat analyzer. The DFD creator may identify elements of an information system, and compose a DFD including nodes and edges representing components and data flows of the information system. The threat indicator may identify a cybersecurity threat to a particular element of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system. In metadata associated with the nodes, edges and secondary node, the DFD creator and threat indicator may provide structured information including attributes of the components, data flows and cybersecurity threat. And the threat analyzer may perform an analysis of the cybersecurity threat based on the threat-model DFD and metadata associated with the nodes, edges and secondary node thereof.” Jones at Abstract “The DFD creator may be configured to identify elements of an information system configured for implementation by a complex-system platform, and compose a DFD for the information system from those elements. The elements of the information system may include components such as hosts, processes, data stores and/or external entities, and data flows between components. The DFD, then, may include nodes representing the components and edges representing the data flows.” Jones at 2:1-9 “The threat indicator may be configured to identify a cybersecurity threat to a particular element of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat model DFD for the information system. Similar to the DFD creator, the threat indicator may provide structured information including attributes of the cybersecurity threat, and may do so in metadata associated with the secondary node of the threat-model DFD. This structured information may include, for example, a description of the cybersecurity threat and a Vulnerability giving rise thereto, a description of any current security controls designed to mitigate the cyber security threat or the like.” Jones at 2:20-32 “The threat analyzer may be configured to perform an analysis of the cybersecurity threat based on the threat model DFD and metadata associated with the nodes, edges and secondary node thereof. In some examples, this may include the threat analyzer being configured to identify
---	--

	a measure of current risk of the cybersecurity threat to a particular element, and identify a Suggested mitigation implementable to reduce the measure of current risk to a lower, measure of residual risk. The threat analyzer may also provide in the metadata associated with the secondary node, further structured information including the measure of current risk, Suggested mitigation and measure of residual risk. A cybersecurity threat may refer to a circumstance or event with a likelihood to have an adverse impact on the information system or a particular element of the information system. In some examples, then, the measure of current risk may be a function of measures of the likelihood and adverse impact. And the further structured information provided in the metadata associated with the secondary node may also include the measures of likelihood and impact.” Jones at 2:33-53 “A cyber security threat may refer to a circumstance or event with a likelihood to have an adverse impact on an asset. Such as the information system or elements of the information, or in some examples, the complex-system platform or one or more of its components (e.g., systems) configured to implement the information system, through unauthorized access, destruction, disclosure, modification of data and/or denial of service.” Jones 3:64-4:5 “The DFD creator 106 may be configured to identify elements of the information system, and compose a DFD for the information system from those elements and in accordance with the threat-model level identified by the DFD level establishment system 104. The DFD may include nodes representing the components and edges representing the data flows. The DFD represent the information system at some level n of the hierarchy, and may at times be referred to as a level in DFD (e.g., level 2 DFD).” Jones at 5:45-53 “The threat indicator 108 may be configured to identify a cybersecurity threat to a particular element of the elements of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system—this threat-model DFD at times referred to as a level n threat-model DFD (e.g., level 2 threat-model DFD).” Jones at 5:64-6:11. “The decomposer may then provide feedback of its decomposition to the DFD creator 106, which may modify the threat-model DFD for the decomposed components to include their nested components and data flows (and appropriate metadata), thereby producing a level n+1 threat-model DFD. And again, the threat indicator 108 may be applied to identify any cybersecurity threats to elements (nested components and data flows) of the decomposed components, and add appropriate secondary nodes (and appropriate metadata) representing those threats.” Jones at 6:18-27
--	--

	“The threat analyzer 112 may be configured to perform an analysis of the cybersecurity threat based on the threat model DFD and metadata associated with the nodes, edges and secondary node thereof. In some examples, this may include the threat analyzer being configured to identify a measure of current risk of the cybersecurity threat to a particular element, sometimes be referred to as a current-risk rating, and identify a Suggested mitigation implementable to reduce the current-risk rating to a lower, measure of residual risk, which may sometimes be referred to as a residual-risk rating.” Jones at 6:35-45 “The threat analyzer 112 may also provide in the metadata associated with the secondary node, further structured information including the current-risk rating, suggested mitigation and residual-risk rating. As explained above, a cyber security threat may refer to a circumstance or event with a likelihood to have an adverse impact on the information system or a particular element of the information system. In Some examples, then, the current-risk rating may be a function of measures of the likelihood and adverse impact, which may sometimes be referred to as likelihood and impact ratings. And the further structured information provided in the metadata associated with the secondary node may also include the likelihood and impact ratings.” Jones at 6:46-58 “FIG. 2 illustrates a DFD creator 200, which in some example implementations of the present disclosure may correspond to the DFD creator 106 of FIG. 1. As indicated above and explained in greater detail below, the DFD creator may be more generally configured to identify elements of the information system, and compose a DFD for the information system from those elements. As shown, the DFD creator may include an identifier for each of a number of different types of elements of an information system, including those for components such as hosts 202, processes 204. data stores 206 and/or external entities 208, and data flows 210 between those components. These identifiers may be configured to identify the components and data flows of the information system, as well as their attributes.” Jones at 7:17-30 “FIG. 3 illustrates a threat indicator 300, which in some example implementations of the present disclosure may correspond to the threat indicator 108 of FIG.1. As indicated above and explained in greater detail below, the threat indicator may be more generally configured to identify a (one or more) cybersecurity threat to a particular element (component or data flow) of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system. As shown, the threat indicator may include a threat identifier 302 coupled to and in
--	--

	communication with a threat-DFD applicator 304 configured to identify cyber security threats to respective particular components and/or data flows of the information system, as well as their attributes.” Jones at 11:59-12:6 “The threat-DFD applicator 304 may be configured to apply secondary nodes representing the cybersecurity threats to the DFD, and include metadata with structured information including attributes of the cybersecurity threats. The threat-DFD applicator may thereby produce a level in threat-model DFD for the information system. The threat DFD applicator may be configured to communicate the threat-model DFD (including the metadata attributes for elements of the information system and cybersecurity threats thereto), such as to a threat-model DFD storage 310 (e.g., file storage, database storage, cloud storage) for later retrieval.” Jones at 12:43-54 “A cybersecurity threat may refer to a circumstance or event with a likelihood to have an adverse impact on an asset, such as the information system or elements of the information, or in some examples, the complex-system platform or one or more of its components (e.g., systems) configured to implement the information system, through unauthorized access, destruction, disclosure, modification of data and/or denial of service.” Jones at 13:10-17. “The current-risk calculator 402 may be configured to identify or more particularly in some examples calculate a current-risk rating of the cybersecurity threat to a particular element of the information system. In some examples, the current-risk rating may be on a scale of increasing risk: low, medium, high or critical. In some more particular examples, the current-risk rating may be a function of likelihood and impact ratings. In some of these examples, likelihood may be on a scale of increasing likelihood: low, medium, high or very high; and likewise, impact may be on a scale of increasing impact: low, medium, high or critical. The current-risk calculator 402 may therefore be configured to calculate the current-risk rating from likelihood and impact ratings.” Jones at 14:33-48 “The threat-model DFD may include a DFD of an information system and include a (one or more) secondary node representing a cybersecurity threat to an element of the information system.” Jones at 15:62-65 “By the above, the analysis-DFD applicator 408 may produce a threat analysis that includes at least the level in threat-model DFD (together with or simply including meta data for the information system's elements and cybersecurity threats), with metadata including further attributes of the cybersecurity threat.” Jones at 16:37-42
--	---

“In some examples, the report generator 502 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. In Some examples, the attributes may be organized in a table including a row for each of one or more cybersecurity threats, and a column for each of one or more attributes of the threat and/or element(s) of the information system to which the threat is applicable. In some examples, the report may include for each of one or more cybersecurity threats, a description of the cybersecurity threat and a vulnerability giving rise thereto, impact rating (e.g., independent of current security controls or Suggested mitigation), any current security controls, likelihood rating, current-risk rating, Suggested mitigation, residual-risk rating, element(s) of the information system to which the cybersecurity threat is applicable, and the like.” Jones at 17:50-67

“As shown at block 606, the method also includes identifying a cybersecurity threat to a particular element of the elements of the information system. The method includes adding to the DFD, a secondary node representing the cybersecurity threat, and metadata associated with the secondary node and providing structured information including attributes of the cybersecurity threat, as shown in block 608. This may thereby produce a threat-model DFD for the information system. And the method may include performing an analysis of the cybersecurity threat based on the threat-model DFD and metadata associated with the nodes, edges and secondary node thereof, as shown at block 610.” Jones at 18:18-29

“FIG. 8 illustrates the GUI 700 including various shapes placed in the workspace 702 and arranged to compose a level in DFD 802 for an information system. As shown, the DFD includes shapes for elements including various hosts 804, processes 806, data stores 808 and external entities 810, and data flows 812. As or after these elements (or rather their shapes) are placed in the workspace, attributes of the elements may be entered for their shapes.” Jones at 18:58-65

“FIG. 9 illustrates the GUI including a level in threat-model DFD902 produced from the level in DFD902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD. Similar to elements of the information system, as or after the cybersecurity threats (or rather their shapes) are placed in the workspace 702, attributes and even further attributes of the cybersecurity threats may be entered for their shapes. Also similar to before, in Some examples, the window 814 may be recalled for each of the

	shapes, in which data for a shape and thus attributes of a cybersecurity threat may be entered, and thereby included as structured information in metadata associated with the shape (and thus secondary node). FIG. 9 illustrates an example in which the window presents fields for receiving or otherwise presenting attributes of the cybersecurity threat “Buffer overflow.” Again, the shapes for the cybersecurity threats may include a graphic and, in some examples, the graphic may be color coded to various shape data Such as the current-risk rating.” Jones 19:10-28 “FIGS. 10A and 10B depict an example report 1000 that may be generated according to example implementations. As shown, for example, the report may include attributes (including further attributes) of at least some of the components, data flows or cybersecurity threat, organized in a table including rows 1002 for respective cybersecurity threats, and columns 1004 for respective attributes of the threat and/or element(s) of the information system to which the threat is applicable.” Jones at 19:29-37 Figs. 2-3, 6, 8-9, 10A-B.
1[c]. a plurality of compensating controls stored therein, each compensating control associated with at least one of the threats through the one or more databases;	The Jones reference discloses this claim element. For example, Jones discloses: “Similar to the DFD creator, the threat indicator may provide structured information including attributes of the cybersecurity threat, and may do so in metadata associated with the secondary node of the threat-model DFD. This structured information may include, for example, a description of the cybersecurity threat and a vulnerability giving rise thereto, a description of any current security controls designed to mitigate the cybersecurity threat or the like.” Jones at 2:20-32. “In some examples, this may include the threat analyzer being configured to identify a measure of current risk of the cybersecurity threat to a particular element, sometimes be referred to as a current-risk rating, and identify a suggested mitigation implementable to reduce the current-risk rating to a lower, measure of residual risk, which may sometimes be referred to as a residual-risk rating.” Jones at 2:37-41. “Security Controls - Indicates security controls (mechanisms) that are implemented for the data flow, and protect data on the flow. In some examples, this may be closely related to connection type (e.g., HTTPS has security controls encryption and integrity).” Jones at 11:52-57. “Current Controls Security controls, or factors, that are already implemented in the information system, or its component or data flow. Examples of suitable controls include technical controls (e.g., “encrypted

connection”), administrative controls (e.g., “requires manager approval”), operational controls (e.g., “server is in an access-controlled data center”) or the like.” Jones at 14:10-17.

“The mitigation identifier 404 may be configured to identify a (one or more) suggested mitigation implementable to reduce the current-risk rating to a lower, residual-risk rating. This suggested mitigation may be identified in any of a number of manners. In one example, the suggested mitigation may be identified from or using an analysis similar to that for which the cybersecurity threat is identified. This may be the case, for example, in the case of application of the STRIDE threat model, which may provide a number of security controls or mitigations for a number of known security threats.

In some examples, the suggested mitigations of cybersecurity threats to components and data flows of the information system may be identified through the collection of information from the operator. This information may be collected or retrieved by the analysis-DFD applicator 408, and with logic provided by the mitigation identifier 404, suggested mitigations of cybersecurity threats may be identified.” Jones at 14:66-15:17

“The analysis-DFD applicator 408 may be configured to receive the current-risk rating, suggested mitigation and residual-risk rating from the current-risk calculator 402, mitigation identifier 404 and residual-risk calculator 406, the threat analyzer 400, or communicate with those components to calculate or identify the current-risk rating, suggested mitigation and residual-risk rating.” Jones at 15:43-49.

“Suggested Mitigations - Suggested mitigations that may lower the measure of current risk to a lower, measure of residual risk.” Jones at 16:28-34.

1004

1000

REF #	SUGGESTED MITIGATIONS	RESIDUAL RISK	APPLIES TO	REMARKS	REVIEW STATUS
1	Encrypt client-server connections	Medium	Data flows between client app and server.	This is an information disclosure threat that may lead to a follow-on threat of spoofing threat.	Reviewed
2	Protect RPC connections with a protocol that provides integrity protection (like SSL/TLS)	Medium	Master-to-Backup data flow		Likelihood rating not agreed
3	Fix buffer overflow.	Medium	Login process	CVSS rating of threat indicated high difficulty to reproduce, which is why likelihood is rated Medium	Not Reviewed
4	Use strong two-factor authentication.	Low	Database system	Preliminary: <Describe why finding is preliminary>	Waiting to clear Preliminary status
5	Implement a failover server in the same datacenter as primary server. Implement regional failover server.	Medium	Web server Application server	Preliminary: <Describe why finding is preliminary> Regional failover needed to bring residual risk to Low.	Waiting to clear Preliminary status
6	Background check	Low	Top level sys admins	Not a traditional STRIDE threat. Improper admin designation could result in all STRIDE threats.	Reviewed
7	Log admin success and fail actions.	Low	Application Server		Reviewed
8	Turn on host-based FW	Low	Web server	Type is "Undetermined" as the vulnerability is very general.	Not Reviewed

1002

● YELLOW ● GREEN

FIG. 10B

	“mitigations” Jones at Fig. 10B
1[d]. providing one or more interfaces, including a diagram interface, configured to be displayed on one or more end user computing devices communicatively coupled with the one or more databases;	The Jones reference discloses this claim element. For example, Jones discloses: “FIGS. 7-9 depict an example graphical user interface in 25 which a DFD, threat-model DFD and their metadata may be composed or produced according to some example implementations of the present disclosure; and” Jones at 3:25-28 “As explained above, a DFD may include nodes and edges representing hosts, processes, data stores and/or external entities, and data flows of the information system, as well as metadata with structured information including attributes of those elements. A host identified by the DFD composer 212 in communication with the host identifier 202 may include, for example, a general or specific-purpose computing device on which a process may be configured to run. Similarly, for example, a host may include a general or specific-purpose computing device on which a data store is configured to run.” Jones at 8:32-44 “To further illustrate example embodiments of the present invention, reference will now be made to FIGS. 7-9, which depict example graphical user interface (GUI) 700 in which a DFD, threat-model DFD and their metadata may be composed or produced according to some example implementations of the present disclosure.” Jones at 18:30-43. “As shown in FIG. 7, in some examples, the GUI 700 may include a workspace 702 for composition of a level n DFD from shapes representing its nodes and edges. In some examples, as shown, the GUI may provide a stencil 704 with a collection of shapes for respective types of components (e.g., host, process, data store, external entity) and data flows of an information system, cybersecurity threats, and perhaps also various relevant components of the complex-system platform configured to implement the information system. And in some examples, these shapes may be configured to accept shape data, which may be specifically configured for types of attributes of the information systems' components (e.g., host, process, data store, external entity) and data flows, as well as the cybersecurity threats.” Jones at 18:44-57. “FIG. 9 illustrates the GUI including a level in threat-model DFD902 produced from the level in DFD902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD.” Jones at 19:10-14 Figs. 7-9

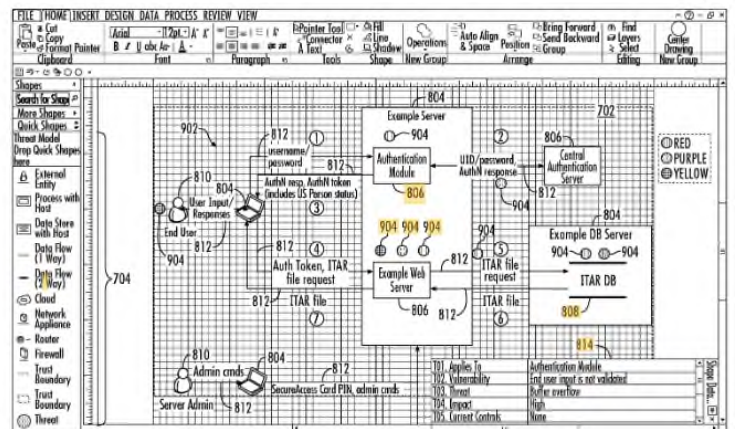


FIG. 9

Jones at Fig. 9

“Examples of Suitable communication interfaces include a network interface controller (NIC), wireless NIC (WNIC) or the like. The user interfaces may include a display and/or one or more user input interfaces (e.g., input/output unit). The display may be configured to present or otherwise display information to a user, Suitable examples of which include a liquid crystal display (LCD), light-emitting diode display (LED), plasma display panel (PDP) or the like. The user input interfaces may be wired or wireless, and may be configured to receive information from a user into the apparatus, such as for processing, storage and/or display. Suitable examples of user input interfaces include a micro phone, image or video capture device, keyboard or keypad, joystick, touch-sensitive surface (separate from or integrated into a touchscreen), biometric sensor or the like. The user interfaces may further include one or more interfaces for communicating with peripherals such as printers, Scanners or the like.”
Jones at 21:1-19

1[e]. configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and

The Jones reference discloses this claim element. For example, Jones discloses:

“FIGS. 7-9 depict an example graphical user interface in 25 which a DFD, threat-model DFD and their metadata may be composed or produced according to some example implementations of the present disclosure; and” Jones at 3:25-28

“For example, the DFD level establishment system may identify a level 2 threat model as appropriate in instances in which the threat model is for any of the following: higher trust level network enclave environments, hybrid access Zone, high-trust access Zone, Internet facing applications and/or systems with transitive access, perimeter-related systems.” Jones at 5:27-33

visual representations of one or more of the compensating controls, the relational diagram defining a first threat model, and;	“As shown in FIG. 7, in some examples, the GUI 700 may include a workspace 702 for composition of a level in DFD from shapes representing its nodes and edges. In some examples, as shown, the GUI may provide a stencil 704 with a collection of shapes for respective types of components (e.g., host, process, data store, external entity) and data flows of an information system, cybersecurity threats, and perhaps also various relevant components of the complex-system platform configured to implement the information system. And in Some examples, these shapes may be configured to accept shape data, which may be specifically configured for types of attributes of the information systems components (e.g., host, process, data store, external entity) and data flows, as well as the cybersecurity threats. FIG. 8 illustrates the GUI 700 including various shapes placed in the workspace 702 and arranged to compose a level in DFD 802 for an information system. As shown, the DFD includes shapes for elements including various hosts 804, processes 806, data stores 808 and external entities 810, and data flows 812. As or after these elements (or rather their shapes) are placed in the workspace, attributes of the elements may be entered for their shapes. In some examples, a window 814 may be recalled for each of the shapes. And in this window, data for a shape and thus attributes of an element may be entered, and thereby included as structured information in metadata associated with the shape (and thus node or edge of the DFD). FIG. 8 illustrates an example in which the window presents fields for receiving or otherwise presenting attributes of the external entity “End User.” The shapes may include a graphic and, in some examples, accompanying text that may be taken from the shape data (e.g., the name of the information system component or type of data flowing in the data flow). FIG. 9 illustrates the GUI including a level in threat-model DFD902 produced from the level in DFD902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD. Similar to elements of the information system, as or after the cybersecurity threats (or rather their shapes) are placed in the workspace 702, attributes and even further attributes of the cybersecurity threats may be entered for their shapes. Also similar to before, in Some examples, the window 814 may be recalled for each of the shapes, in which data for a shape and thus attributes of a cybersecurity threat may be entered, and thereby included as structured information in metadata associated with the shape (and thus secondary node). FIG. 9 illustrates an example in which the window presents fields for receiving or otherwise presenting attributes of the cybersecurity threat “Buffer overflow.” Again, the shapes for the cybersecurity threats may include a graphic and, in some examples, the graphic may be color coded to various shape data Such as the current-risk rating.” Jones at 18:44-19:28 Figs. 7-9, and 10B
---	--

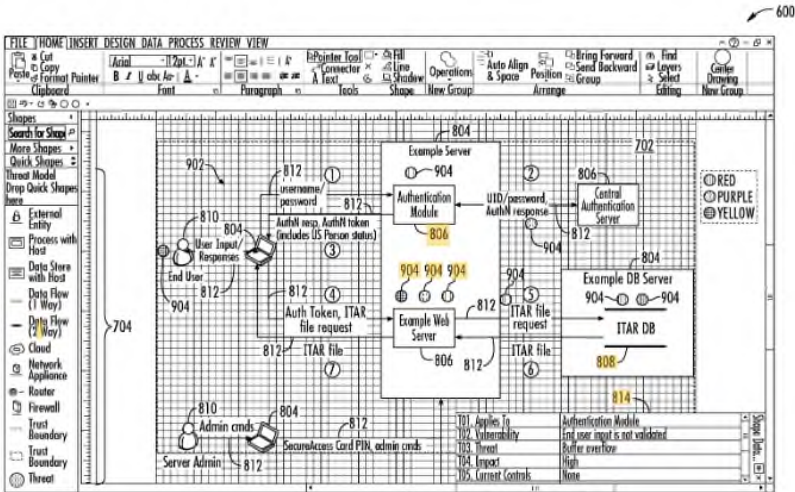


FIG. 9

Jones at Fig. 9

1004					
1000					
Numbering for this table - this does not correspond to numbering in the Visio diagram.	Security controls that are recommended to bring the Current Risk rating lower.	Risk given that suggested mitigations are implemented.	The data flow diagram (DFD) element(s) that the threat applies to.	Additional clarifying information. If a finding is preliminary, meaning it needs further research indicate "Preliminary" here.	Use to note whether the review process has resulted in acceptance of this threat and associated impact and risk ratings.
REF #	SUGGESTED MITIGATIONS	RESIDUAL RISK	APPLIES TO	REMARKS	REVIEW STATUS
1	Encrypt client-server connections	Medium	Data flows between client app and server.	This is an information disclosure threat that may lead to a follow-on threat of spoofing threat.	Reviewed
2	Protect RPC connections with a protocol that provides integrity-protection (like SSL/TLS)	Medium	Master-to-Backup data flow		Likelihood rating not agreed
3	Fix buffer overflow.	Medium	Login process	CVSS rating of threat indicated high difficulty to reproduce, which is why likelihood is rated Medium	Not Reviewed
4	Use strong two-factor authentication.	Low	Database system	Preliminary: <Describe why finding is preliminary>	Waiting to clear Preliminary status
5	Implement a failover server in the same datacenter as primary server. Implement regional failover server.	Medium	Web server Application server	Preliminary: <Describe why finding is preliminary> Regional failover needed to bring residual risk to Low.	Waiting to clear Preliminary status
6	Background check	Low	Top level sys admins	Not a traditional STRIDE threat. Improper admin designation could result in all STRIDE threats.	Reviewed
7	Log admin success and fail actions.	Low	Application Server		Reviewed
8	Turn on host-based FW	Low	Web server	Type is "Undetermined" as the vulnerability is very general.	Not Reviewed

FIG. 10B

Jones at Fig. 10B.

1[f]. configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a

The Jones reference discloses this claim element. For example, Jones discloses:

“The system 100 may include one or more of each of a number of different subsystems (each an individual system) coupled to one another for performing one or more functions or operations. As shown in FIG. 1, for example, the system may include a criticality establishment system 102, data flow diagram (DFD) level establishment system 104, DFD creator 106, threat indicator 108, decomposer 110, threat analyzer 112 and/or reporter 114. Although shown as part of the modeling and analysis system, one or more of the criticality establishment system, DFD level establishment system, DFD creator, threat indicator, decomposer, threat

second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.	analyzer and/or reporter may instead be separate from but in communication with the modeling and analysis system.” Jones at 4:22-35 “The information system may include components such as hosts, processes, data stores and/or external entities, and data flows between those components. In some examples, a process may be identified along with the host on which the process is configured to run; and similarly, in some examples, a data store may be identified along with the host on which the data store is configured to run. In some examples, the information system may be describable in terms of a hierarchical breakdown (hereinafter referred to as a “hierarchy”) of its components (interconnected by appropriate data flows) at different levels. In this regard, one or more of the information system's components—more often a process, host or data store—may include multiple nested components, one or more of which may include further additional nested components at lower levels of the hierarchy.” Jones at 5:4-19. “The DFD level establishment system 104 may be configured to assess various criteria of the information system to identify an appropriate level of threat model—threat-model data flow diagram (DFD)—to produce for the information system. In some examples, various criteria of the information system may be associated with various levels, and the appropriate level may identified by matching criteria to a level. For example, the DFD level establishment system may identify a level 2 threat model as appropriate in instances in which the threat model is for any of the following: higher trust level network enclave environments, hybrid access Zone, high-trust access Zone, Internet facing applications and/or systems with transitive access, perimeter-related systems. In instances in which the threat model is not for any of the aforementioned, a level 2 threat model may still be appropriate in instances in which it is based on data classification that application or system stores and/or processes for any of the following: sensitive or highly-sensitive personally identifiable information (PII), own or third-party proprietary, critical technical information (CTI), export controlled EAR, ITAR, material non-public or national security information, trade secret or the like. And in instances in which none of the foregoing are met, the DFD level establishment system may identify a level 1 threat model as appropriate.” Jones at 5:20-44 “The DFD creator 106 may be configured to identify elements of the information system, and compose a DFD for the information system from those elements and in accordance with the threat-model level identified by the DFD level establishment system 104. The DFD may include nodes representing the components and edges representing the data flows. The DFD represent the information system at some level n of the hierarchy, and
--	--

	may at times be referred to as a level in DFD (e.g., level 2 DFD).” Jones at 5:45-53 “The threat indicator 108 may be configured to identify a cybersecurity threat to a particular element of the elements of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system— this threat-model DFD at times referred to as a level in threat-model DFD (e.g., level 2 threat-model DFD). Similar to the DFD creator, the threat indicator may provide structured information including attributes of the cybersecurity threat, and may do so in metadata associated with the secondary node of the threat-model DFD. This structured information may include, for example, a description of the cybersecurity threat and a Vulnerability giving rise thereto, a description of any current security controls designed to mitigate the cybersecurity threat or the like.” Jones at 5:64-6:11 “In some examples it may be desirable to look deeper into one or more components of the information system, such as to provide a more thorough analysis of those components or their cybersecurity threats. In these examples, the decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows therebetween. The decomposer may then provide feedback of its decomposition to the DFD creator 106, which may modify the threat-model DFD for the decomposed components to include their nested components and data flows (and appropriate metadata), thereby producing a level n+1 threat-model DFD. And again, the threat indicator 108 may be applied to identify any cybersecurity threats to elements (nested components and data flows) of the decomposed components, and add appropriate secondary nodes (and appropriate metadata) representing those threats. Or instead of modifying the existing threat-model DFD, in some examples, the DFD creator and threat indicator may begin again to compose a new DFD and threat-model DFD for this level of the hierarchy. This decomposition and follow-on modeling of the information system's components and threats may continue until a desired level of the information system is achieved.” Jones at 6:12-34. “The identifiers 202-210 may be coupled to a DFD composer 212 configured to communicate with the identifiers to receive the identification of or identify components and data flows and their attributes, compose a level in DFD representing components and data flows and including metadata with structured information including attributes of the components and data flows.” Jones at 7:31-37
--	--

	“In some examples, the DFD composer 212 may compose the metadata attributes of the components and data flows of the information system without itself composing the DFD. In these examples, the DFD composer may communicate to the DFD storage, the metadata attributes of the information system for a level in DFD. In these examples, the stored metadata attributes may be accessed by a separate DFD renderer 220 configured to compose the level in DFD from the metadata attributes.” Jones at 8:23-31 “The threat-DFD applicator 304 configured to receive the identification of or identify cybersecurity threats (and their attributes) to components and data flows of the information system. The threat-DFD applicator may also be configured to receive a level in DFD for an information system—or in Some examples the metadata attributes of the information system for a level in DFD, such as from a DFD storage 306 (e.g., file storage, database storage, cloud storage). The DFD storage may be resident with the threat indicator 300, or may be separate from and in communication with the threat indicator, and in Some examples may correspond to DFD storage 218. And again, the DFD and its metadata may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types.” Jones at 12:7-21 “The threat-DFD applicator 304 may be configured to apply secondary nodes representing the cybersecurity threats to the DFD, and include metadata with structured information including attributes of the cybersecurity threats. The threat-DFD applicator may thereby produce a level in threat-model DFD for the information system. The threat DFD applicator may be configured to communicate the threat-model DFD (including the metadata attributes for elements of the information system and cybersecurity threats thereto), such as to a threat-model DFD storage 310 (e.g., file storage, database storage, cloud storage) for later retrieval. Similar to the DFD storage 306, the threat-model DFD storage may be resident with the threat indicator 300, or may be separate from and in communication with the threat indicator. Also, similar to the DFD, the threat-model DFD and its metadata may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types. And in some examples, a previously-stored threat-model DFD may be retrieved from the threat-model DFD storage by the threat DFD applicator to produce a new threat-model DFD.” Jones at 12:43-63 “In some examples, the threat-DFD applicator 304 may compose the metadata attributes of cybersecurity threats to the components and data flows of the information system without itself composing the threat-model DFD. In these examples, the threat-DFD applicator may communicate to
--	---

	the threat-model DFD storage, the metadata attributes of the information system and cybersecurity threats for a level in threat-model DFD. In these examples, the stored metadata attributes may be accessed by a separate threat-model renderer 312 configured to compose the level in threat-model DFD from the metadata attributes.” Jones at 12:64-13:7 “The analysis-DFD applicator 408 may be configured to receive the current-risk rating, Suggested mitigation and residual-risk rating from the current-risk calculator 402, mitigation identifier 404 and residual-risk calculator 406, the threat analyzer 400, or communicate with those components to calculate or identify the current-risk rating, Suggested mitigation and residual-risk rating. The threat-DFD applicator may also be configured to receive a level in threat model DFD for the information system—or in some examples the metadata attributes of the information system and cybersecurity threats for a level in threat-model DFD, such as from a threat-model DFD storage 412 (e.g., file storage, database storage, cloud storage). The threat-model DFD storage may be resident with the threat analyzer, or may be separate from and in communication with the threat analyzer, and in some examples may correspond to threat model DFD storage 310)—the threat-model DFD and its metadata again being format” Jones at 15:43-61 “By the above, the analysis-DFD applicator 408 may produce a threat analysis that includes at least the level in threat-model DFD (together with or simply including meta data for the information system's elements and cybersecurity threats), with metadata including further attributes of the cybersecurity threat. The analysis-DFD applicator may be configured to communicate the threat analysis, Such as to a threat analysis storage 414 (e.g., file storage, database storage, cloud storage) for later retrieval. The threat analysis storage may be resident with the threat analyzer 400, or may be separate from and in communication with the threat analyzer. In some examples, a previously-stored threat analysis may be retrieved from the threat analysis storage by the threat analyzer to produce a new threat analysis.” Jones at 16:37-50 “The report generator 502 may be configured to retrieve any of a number of different pieces of information or data regarding an information system, its components and data flows, and/or cybersecurity threats, from one or more of the storage 504, 506, 508. For example, the report generator may retrieve from the DFD storage, a level in DFD for an information system (or simply the metadata attributes of the information system). Additionally or alternatively, the report generator may retrieve from the threat-model DFD storage, a level in threat-model DFD for the information system (or simply the metadata attributes of the information system and cybersecurity threats). And further additionally or alternatively, the report generator may
--	--

	retrieve a threat analysis for the information system (or simply the metadata attributes and further attributes of the information system and cyber security threats).” Jones at 17:16-31 “Graphically, the report generator may generate drawings of one or more of a level in DFD, level in threat-model DFD and/or threat analysis. Through the report selector, the operator may in some examples select the level (select n) of the DFD or threat-model DFD, a number of dependencies between information systems or components of information systems for which to generate reports (e.g., system. A depends on system B, which depends on system C).” Jones at 17:41-49 “As shown in FIG. 7, in some examples, the GUI 700 may include a workspace 702 for composition of a level in DFD from shapes representing its nodes and edges. In some examples, as shown, the GUI may provide a stencil 704 with a collection of shapes for respective types of components (e.g., host, process, data store, external entity) and data flows of an information system, cybersecurity threats, and perhaps also various relevant components of the complex-system platform configured to implement the information system. And in Some examples, these shapes may be configured to accept shape data, which may be specifically configured for types of attributes of the information systems components (e.g., host, process, data store, external entity) and data flows, as well as the cybersecurity threats.” Jones at 18:44-57 “FIG. 8 illustrates the GUI 700 including various shapes placed in the workspace 702 and arranged to compose a level in DFD 802 for an information system.” Jones at 18:58-60 “FIG. 9 illustrates the GUI including a level in threat-model DFD902 produced from the level in DFD902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD. Similar to elements of the information system, as or after the cybersecurity threats (or rather their shapes) are placed in the workspace 702, attributes and even further attributes of the cybersecurity threats may be entered for their shapes. Also similar to before, in Some examples, the window 814 may be recalled for each of the shapes, in which data for a shape and thus attributes of a cybersecurity threat may be entered, and thereby included as structured information in metadata associated with the shape (and thus secondary node). FIG. 9 illustrates an example in which the window presents fields for receiving or otherwise presenting attributes of the cybersecurity threat “Buffer overflow.” Again, the shapes for the cybersecurity threats may include a graphic and, in some examples, the graphic may be color coded to various shape data Such as the current-risk rating.” Jones at 19:10-28
--	---

“According to example implementations of the present disclosure, the system 100 for modeling and analysis of cybersecurity threats and its Subsystems including the criticality establishment system 102, DFD level establishment system 104, DFD creator 106, threat indicator 108, decomposer 110, threat analyzer 112 and reporter 114 may be implemented by various means. Similarly, the examples of a DFD creator 200, threat indicator 300, threat analyzer 400 and reporter 500, including each of their respective elements, may be implemented by various means according to example implementations. Means for implementing the systems, Subsystems and their respective elements may include hardware, alone or under direction of one or more computer programs from a computer-readable storage medium.” Jones at 19:46-59

Figs. 1-5, 7-9

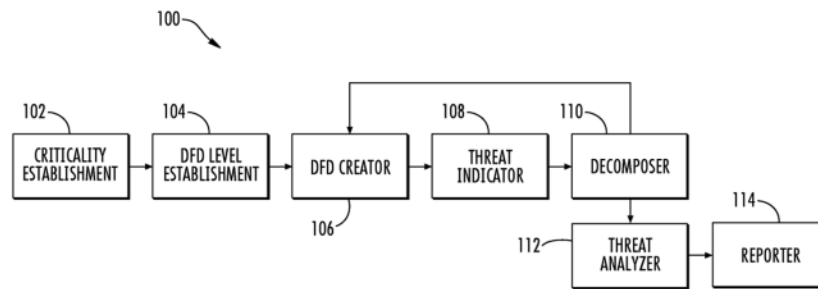
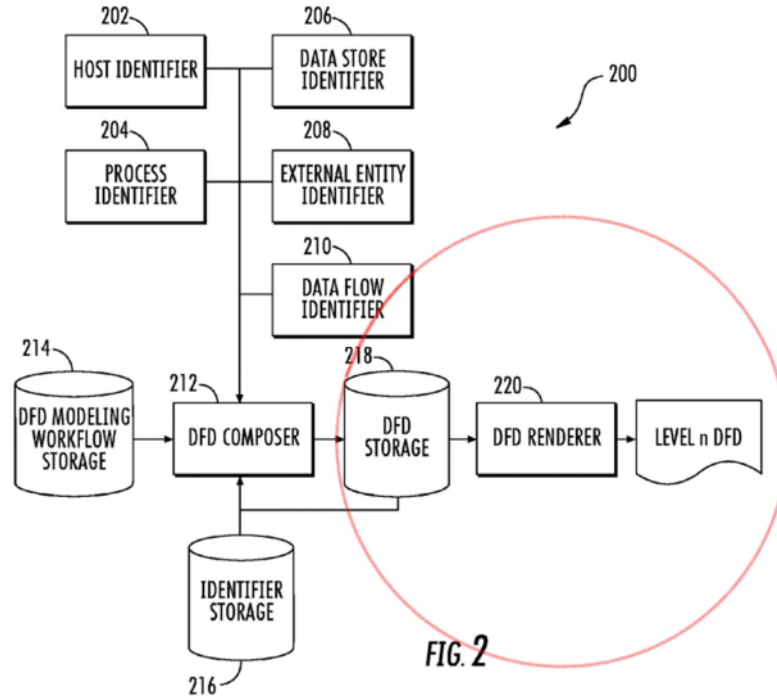
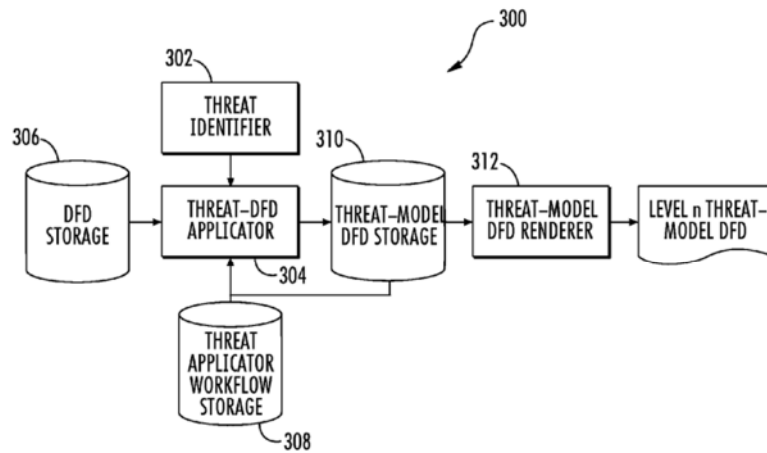


FIG. 1

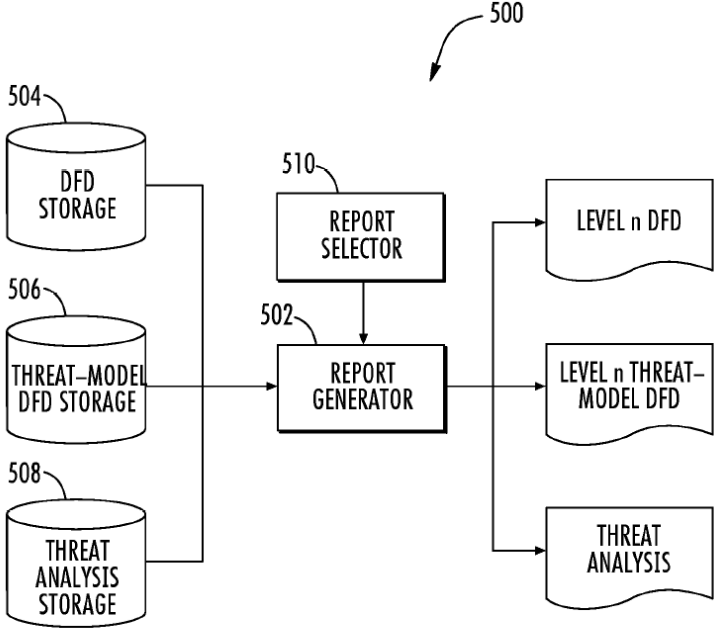
Jones at Fig. 1



Jones at Fig. 2 emphasis added.



Jones at Fig. 3

	 FIG. 5 Jones at Fig. 5
3. The threat model chaining method of claim 1, further comprising configuring the one or more interfaces to, in response to receiving one or more user inputs, store one or more additional threat model components in the one or more databases, store one or more additional threats in the one or more databases, associate each additional threat with at least one	The Jones reference discloses this claim element. For example, Jones discloses: “In this regard, the system may be configured to perform one or more of its functions or operations automatically, that is, without being directly controlled by an operator Such as a security architect that may be assigned to model and analyze cybersecurity threats in the complex-system platform. Additionally or alternatively, the system may be configured to perform one or more of its functions or operations under direct operator control.” Jones at 4:13-21 “FIG. 8 illustrates the GUI 700 including various shapes placed in the workspace 702 and arranged to compose a level in DFD 802 for an information system. As shown, the DFD includes shapes for elements including various hosts 804, processes 806, data stores 808 and external entities 810, and data flows 812. As or after these elements (or rather their shapes) are placed in the workspace, attributes of the elements may be entered for their shapes. In some examples, a window 814 may be recalled for each of the shapes. And in this window, data for a shape and thus attributes of an element may be entered, and thereby included as structured information in metadata associated with the shape (and thus node or edge of the DFD). FIG. 8 illustrates an example in which the window presents fields for receiving or otherwise presenting attributes of the external entity

of the additional threat model components through the one or more databases, store one or more additional compensating controls in the one or more databases, and associate each additional compensating control with at least one of the additional threats through the one or more databases.	“End User.” The shapes may include a graphic and, in some examples, accompanying text that may be taken from the shape data (e.g., the name of the information system component or type of data flowing in the data flow).” Jones at 18:58-68; 19:1-9 “FIGS. 10A and 10B depict an example report 1000 that may be generated according to example implementations. As shown, for example, the report may include attributes (including further attributes) of at least some of the components, data flows or cybersecurity threat, organized in a table including rows 1002 for respective cybersecurity threats, and columns 1004 for respective attributes of the threat and/or element(s) of the information system to which the threat is applicable. In some examples, the report may include for each of one or more cybersecurity threats, a description of the cybersecurity threat and a vulnerability giving rise thereto, impact rating (e.g., independent of current security controls or Suggested mitigation), any current security controls, likelihood rating, current-risk rating, Suggested mitigation, residual-risk rating, element(s) of the information system to which the cybersecurity threat is applicable, and the like.” Jones at 19:29-45. Figs. 1-9, 10A-10B
---	---