

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

**PETITION FOR *INTER PARTES* REVIEW OF
U.S. PATENT NO. 10,699,008
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(b)(1)-(4)	1
A.	Real Parties-In-Interest.....	1
B.	Related Matters.....	1
C.	Counsel	2
D.	Service Information.....	2
III.	STANDING	3
IV.	PAYMENT OF FEES – 37 C.F.R. § 42.103.....	3
V.	TECHNOLOGY BACKGROUND.....	3
VI.	SUMMARY OF THE '008 PATENT	5
A.	Brief Description	5
B.	Priority Date	8
C.	Prosecution History of '008 Patent	8
VII.	IDENTIFICATION OF CHALLENGES UNDER 37 C.F.R. § 42.104(B).....	10
A.	Prior Art.....	10
B.	Challenges	11
VIII.	LEVEL OF ORDINARY SKILL IN THE ART.....	11
IX.	CLAIM CONSTRUCTION	12
A.	“Threat Model Components”	12
B.	“Attack Paths”	12
X.	DETAILED EXPLANATION AND SUPPORTING EVIDENCE.....	13
A.	Overview of the Prior Art.....	13
1.	Jones.....	13
2.	Zheng.....	16
3.	Keenan.....	17

4.	Yu.....	18
5.	Reith.....	19
B.	Ground 1: Jones Anticipates Claims 1 and 3	20
1.	Claim 1	20
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.”	40
C.	Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious.....	41
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.”	42
2.	Claim 4:.....	43
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.”	44

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.” 45
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.....46
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.” 46
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.” 47
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.” 48

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.” 48
10. Claim 12: 48
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.” 50
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.” 50
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.” 50
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.” 50
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.” 51

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.”	51
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.”	52
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.”	54
19.	A POSITA Would Have Been Motivated to Combine Jones, Zheng, and Keenan.	55
D.	Ground 3: The References of Ground 2 and Yu Render Claims 1-20 Obvious	57
E.	Ground 4: The References of Ground 3 and Reith Render Claims 1-20 Obvious.....	60
F.	Ground 5: The References of Ground 4 and the Knowledge of a POSITA Render Claims 5-8 and 13-15.	62
XI.	THIS PETITION IS PROPER UNDER 35 U.S.C. §§ 314(a) AND 325(d).....	63
A.	Stay	63
B.	Trial Date.....	63
C.	Parallel Proceeding.....	63
D.	Issue Overlap.....	64
E.	Same Party.....	64

F.	Other Considerations.....	64
XII.	CONCLUSION.....	65

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

IriusRisk Inc. (“Petitioner”) requests *inter partes* review of claims 1-20 (the “Challenged Claims”) of U.S. Patent No. 10,699,008 (the “’008 patent,” EX-1001), owned by ThreatModeler Software Inc. (“PO”), pursuant to 35 U.S.C. §§ 311-19 and 37 C.F.R. § 42.100.

The ’008 patent relates to a computer application for generating a threat model. During prosecution, the ’008 patent was allowed because the prior art of record did not disclose a relational diagram or threat model chaining. As explained below, those elements, and all other elements of the Challenged Claims, are disclosed in the prior art discussed herein.

II. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(b)(1)-(4)

A. Real Parties-In-Interest

Petitioner, as well as IriusRisk SL, are the real parties-in-interest.

B. Related Matters

PO has asserted the ’008 patent in the following litigation against Petitioner: *ThreatModeler Software Inc v. IriusRisk, Inc.*, C.A. No. 22-912-MN (D. Del.), for which the Complaint was served on July 8, 2022 (the “Litigation”). There, PO asserts the ’008 patent and related U.S. Patent No. 10,713,366 against Petitioner. Petitioner has asserted an IPR against the ’366 patent in IPR2023-00656, filed on March 7, 2023.

C. Counsel

Petitioner designates lead and back-up counsel as noted below. Powers of attorney pursuant to 37 C.F.R. § 42.10(b) accompany this Petition.

Lead Counsel	Backup Counsel
Brent Yamashita Reg. No. 53,808 DLA Piper LLP (US) 2000 University Avenue East Palo Alto, California 94303-2214 Phone: 650.833.2348 Fax: 650.833.2001 Email: brent.yamashita@us.dlapiper.com	Blake Jackson Reg. No. 66,272 DLA Piper LLP (US) 2000 University Avenue East Palo Alto, California 94303-2214 Phone: 650.833.2248 Fax: 650.687.1148 Email: blake.jackson@us.dlapiper.com Matthew Middleton Reg. No. 77,117 DLA Piper LLP (US) 1201 N. Market St., Suite 2100 Wilmington, Delaware 19801-1147 Phone: 302.468.5675 Fax: 302.778.7935 Email: matthew.middleton@us.dlapiper.com

D. Service Information

Please address all correspondence to counsel at the address above. Petitioner consents to electronic service by email at:

brent.yamashita@us.dlapiper.com;

blake.jackson@us.dlapiper.com;

matthew.middleton@us.dlapiper.com.

III. STANDING

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '008 patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting *inter partes* review.

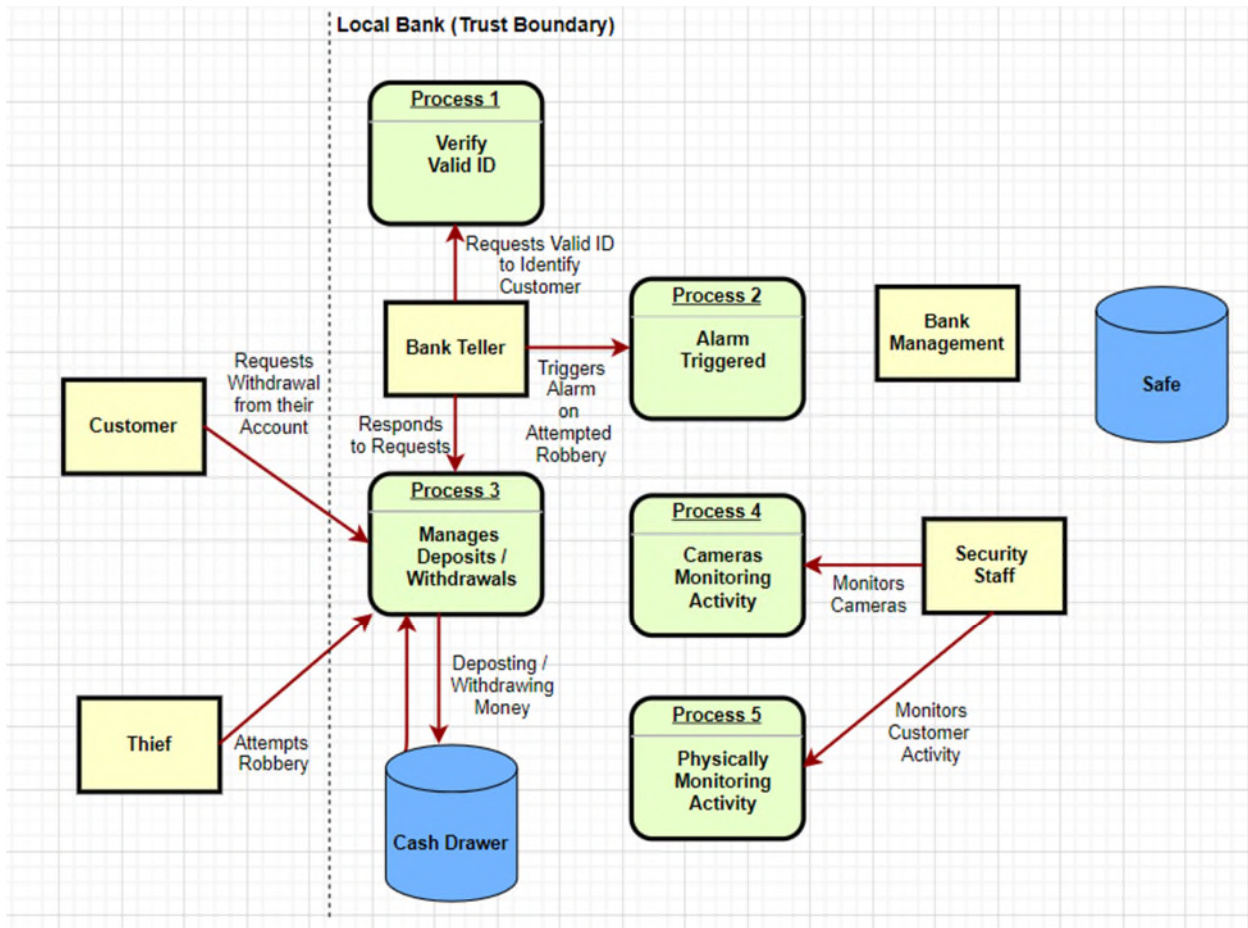
IV. PAYMENT OF FEES – 37 C.F.R. § 42.103

The undersigned authorizes the Director to charge the fee specified by 37 C.F.R. §42.15(a) and any additional fees that might be due in connection with this Petition to Deposit Account No. 50-3266.

V. TECHNOLOGY BACKGROUND

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, *e.g.*, a physical structure, such as an office building or a power plant, or a digital asset, such as financial data or customer information. EX-1003, ¶135.

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 and later could be prepared using computer software applications such as the Microsoft SDL Threat Modeling Tool, which the '008 patent admits is prior art. EX-1003, ¶135; EX-1001, 1:48-54. A simple example of a threat model is the following, which shows potential threats to physical branch of a bank:



EX-1003, ¶35.

This diagram, called a Data Flow Diagram, which is commonly used for Threat Modeling, depicts the following elements:

- **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

The Data Flow Diagram helps identify potential threat actors (Customer, Thief) and various countermeasures to create an initial threat model known in the art before the '008 patent's priority date. EX-1011-1014; EX-1003, ¶¶35-36.

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; EX-1003, ¶¶37-38.

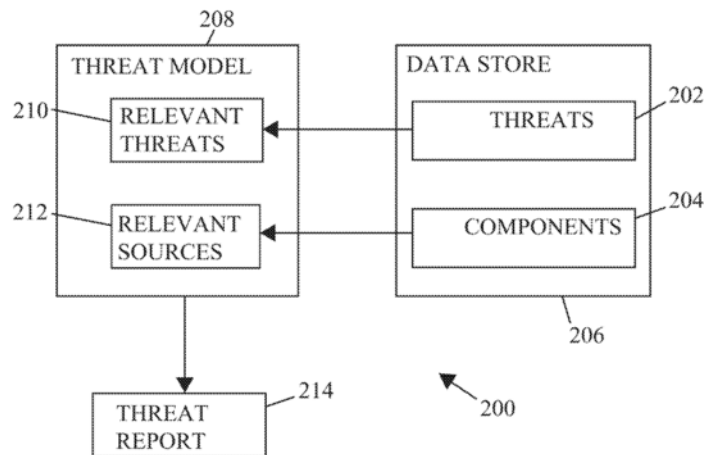
VI. SUMMARY OF THE '008 PATENT

A. Brief Description

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. EX-1003, ¶39.

The '008 patent describes that threat models are created from defined threats and threat model components, which are stored within a database. EX-1001, 9:10-27. This is shown in Figure 2:



Each threat model component “is a potential relevant source for one or more threats.” EX-1001, 9:28-61; EX-1003, ¶¶40-41.

The '008 patent further describes compensating controls stored in the database and associated with the threats that “mitigate different threats emanating from different components.” EX-1001, 25:57-59. FIG. 19 shows the claimed system with six compensating controls (each labeled “CC”):

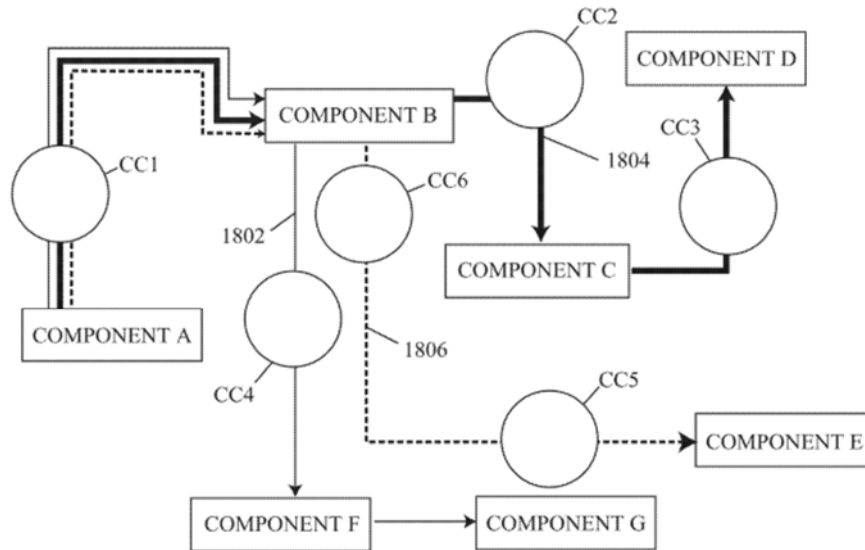


FIG. 19

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; EX-1003, ¶¶42-43.

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. EX-1001, 16:3-14; 23:36-45; EX-1003, ¶44.

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.*; EX-1003, ¶¶45-46.

B. Priority Date

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.

C. Prosecution History of ’008 Patent

The application leading to the ’008 patent was filed on December 20, 2018. See 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.*

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 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; EX-1003, ¶¶48-49.

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.

VII. IDENTIFICATION OF CHALLENGES UNDER 37 C.F.R. § 42.104(B)

A. Prior Art

The challenges in this Petition are based on the knowledge of a person of ordinary skill in the art (a “POSITA”) and the following:

- **Jones (EX-1004):** U.S. Patent No. 9,602,529 (“Jones”) was published on October 8, 2015. Jones is prior art to the ’008 patent under 35 U.S.C. § 102(a)(1).
- **Zheng (EX-1005):** U.S. Patent No. 10,503,907 (“Zheng”) was filed on December 14, 2016, published on June 15, 2017, and claims priority to December 14, 2015. Zheng is prior art to the ’008 patent under 35 U.S.C. § 102(a)(2).
- **Keenan (EX-1006):** U.S. Patent No. 11,200,228 (“Keenan”) was filed on April 19, 2018, and issued on December 14, 2021. Keenan claims priority to April 19, 2017. Keenan is prior art to the ’008 patent under 35 U.S.C. § 102(a)(2).
- **Yu (EX-1007):** U.S. Patent No. 9,948,652 (“Yu”) was filed on May 16, 2016 and published on November 16, 2017. Yu is prior art to the ’008 patent under 35 U.S.C. § 102(a)(2).

- **Reith (EX-1008):** U.S. Patent No. 10,216,938 (“Reith”) was filed on December 3, 2015 and published on June 9, 2016.

Reith is prior art to the ’008 patent under 35 U.S.C. § 102(a)(1).

B. Challenges

Petitioner requests cancellation of claims 1-20 of the ’008 patent based on the following grounds:

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

VIII. LEVEL OF ORDINARY SKILL IN THE ART

A POSITA as of the filing date of the ’008 patent 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 in software development and designing or implementing threat models. Additional work or research experience can substitute for less or different education, and vice-versa. EX-1003, ¶33.

IX. CLAIM CONSTRUCTION

The Challenged Claims are interpreted using the same standard used in federal district court. Petitioner defines two terms below consistent with the '008 patent specification and applies the plain and ordinary meaning that a POSITA would attribute to the remaining terms.

A. “Threat Model Components”

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; EX-1003, ¶51.

B. “Attack Paths”

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, 22:65-68; EX-1003, ¶52.

X. DETAILED EXPLANATION AND SUPPORTING EVIDENCE

A. Overview of the Prior Art

1. Jones

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.

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.

Jones’ process is shown in Figs. 2-5:

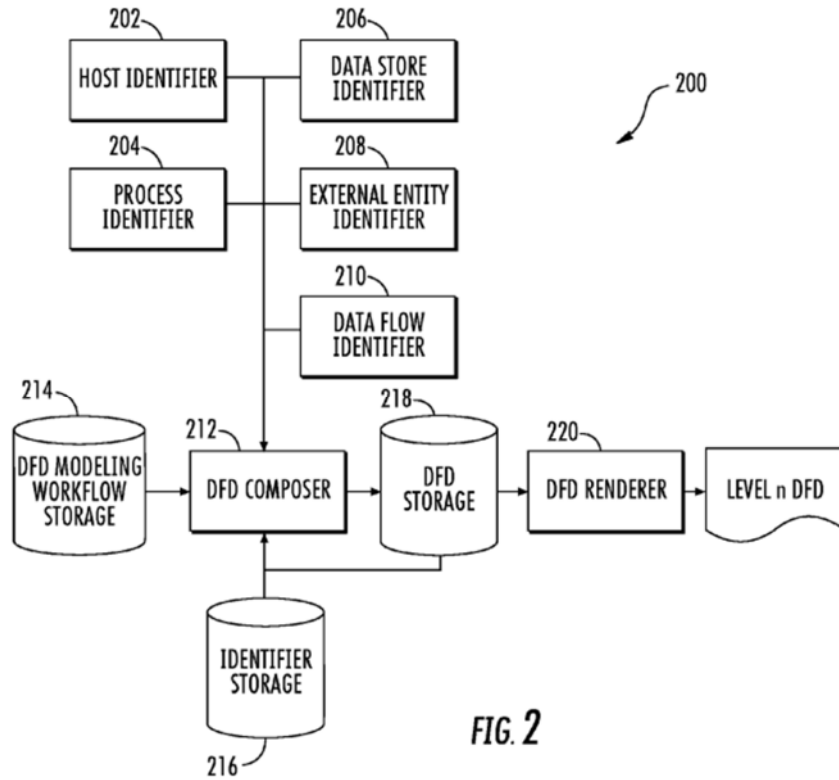


FIG. 2

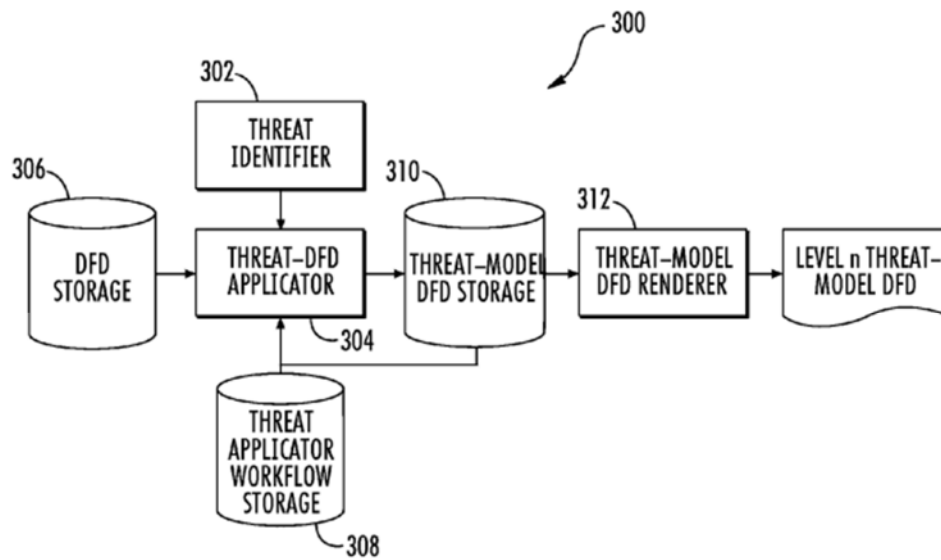


FIG. 3

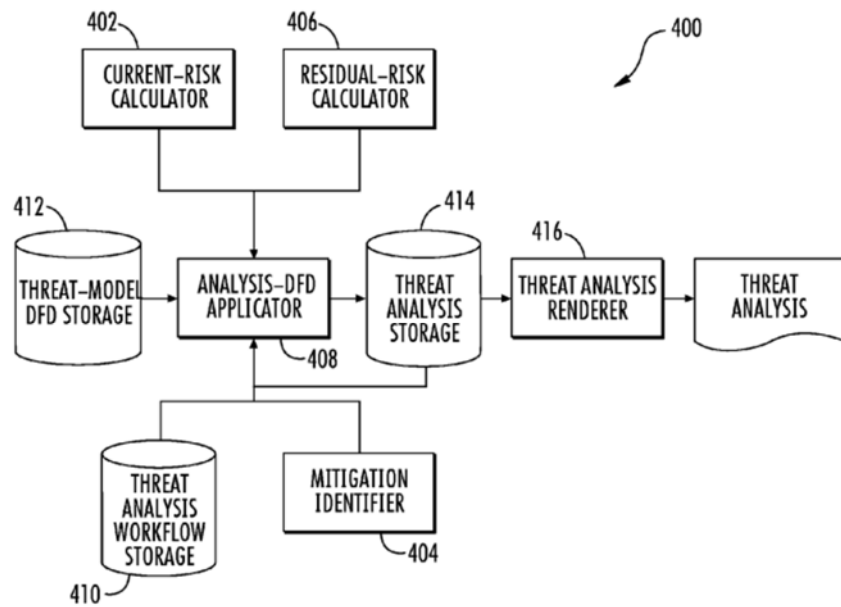


FIG. 4

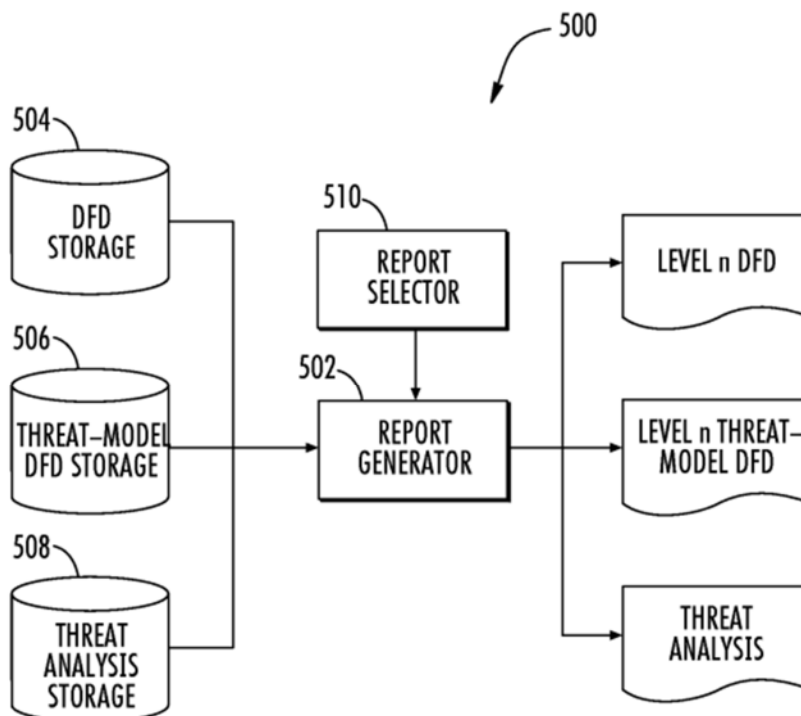


FIG. 5

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:

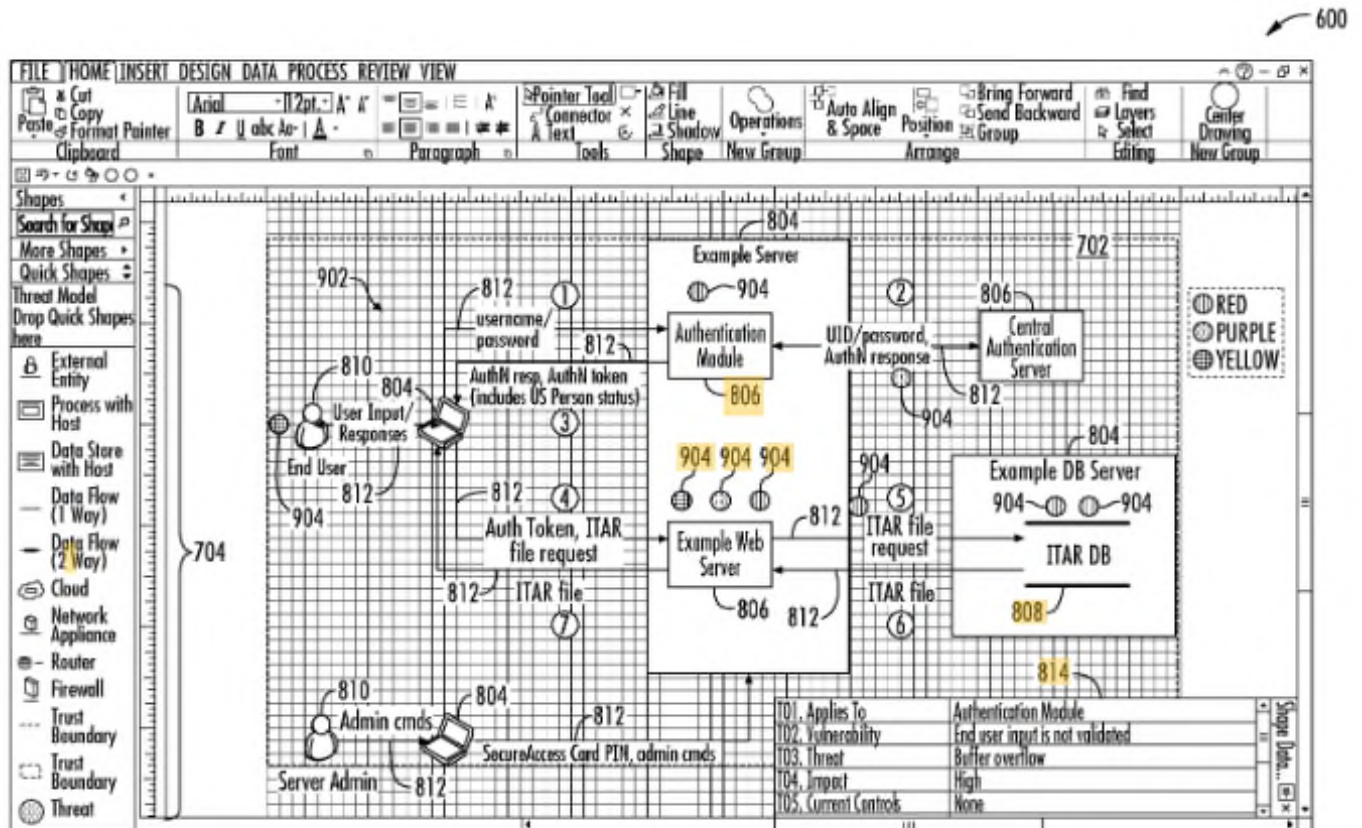


FIG. 9

EX-1003, ¶¶54-57.

2. Zheng

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.*; EX-1003, ¶58.

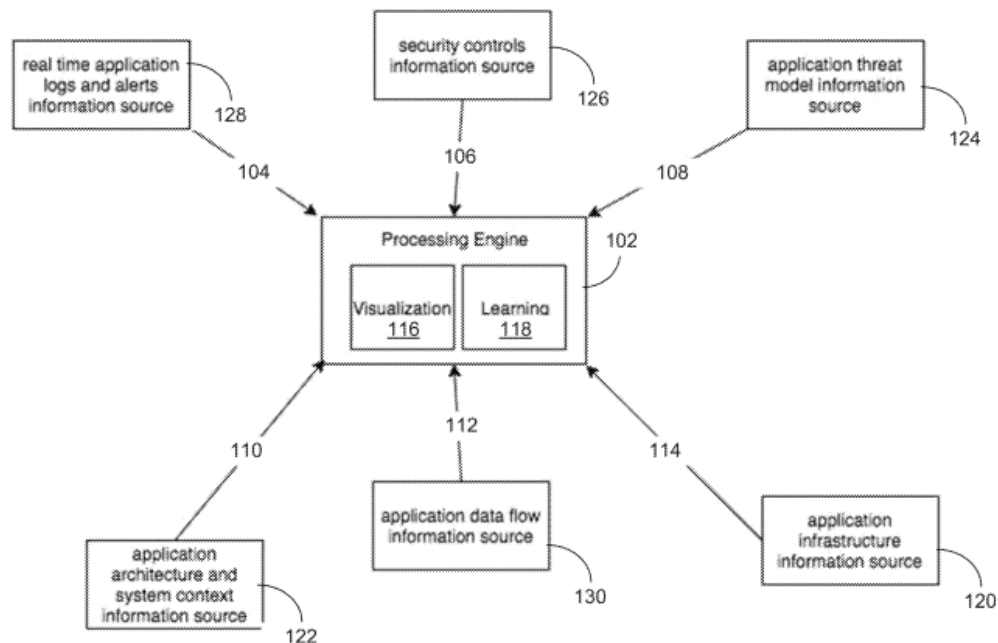


FIG. 1

3. Keenan

Keenan discloses threat modeling and is relied upon in this Petition for its disclosure of toggling. Keenan describes threat modeling systems and methods including a graphical user interface with the ability to “toggle” features on or off. Ex-1006 at 17:19-21; EX-1003, ¶59.

4. Yu

Yu discloses threat modeling and is relied upon in this 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.

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

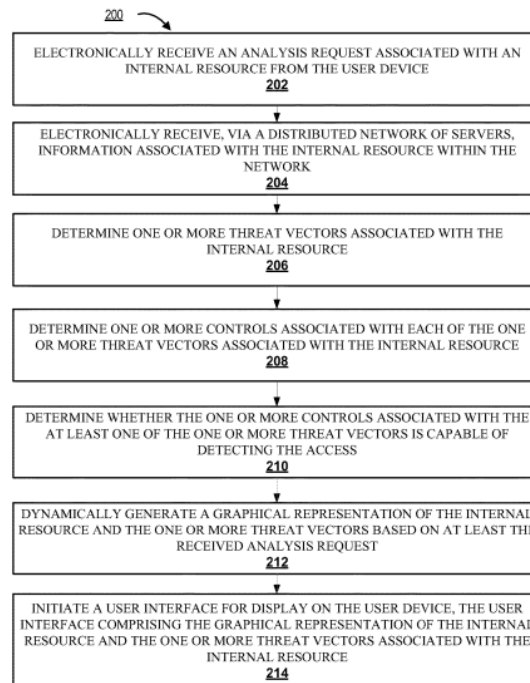


Figure 2

EX-1003, ¶¶60-61.

5. Reith

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

400

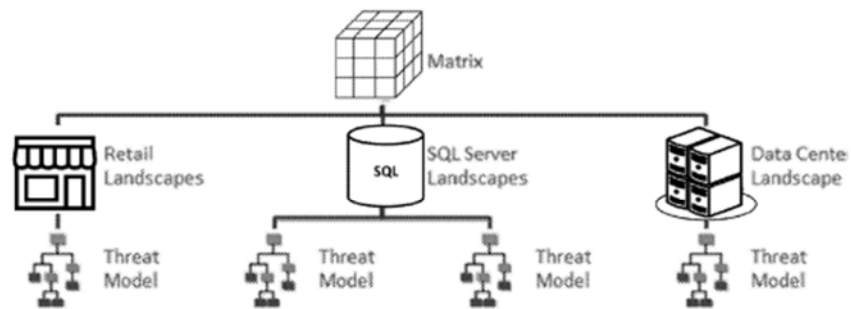


Figure 4

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; EX-1003, ¶¶62-63.

B. Ground 1: Jones Anticipates Claims 1 and 3

1. Claim 1

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

To the extent the preamble is limiting, Jones discloses this element. EX-1003, ¶¶64-66. 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. 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. 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.” 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].

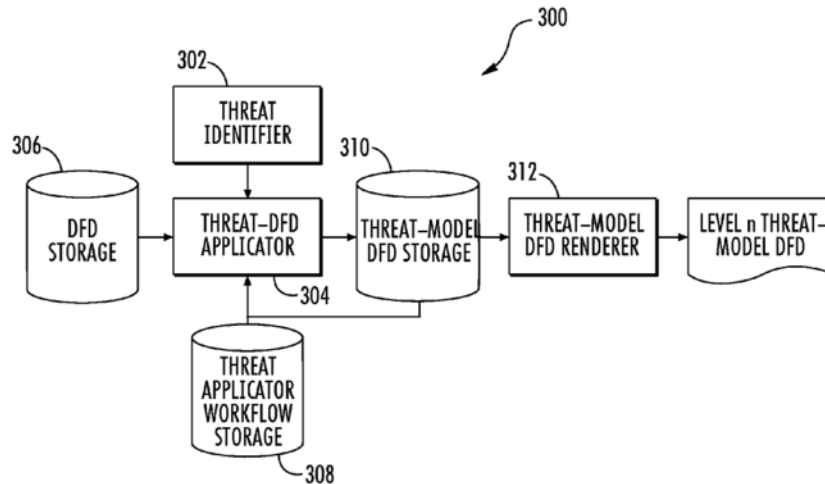


FIG. 3

A POSITA would understand that Jones’ disclosure of “multiple nested components” is threat model chaining as claimed. EX-1003, ¶66. 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:”

Jones discloses this element. EX-1003, ¶67. 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 (DFD Storage), 9.

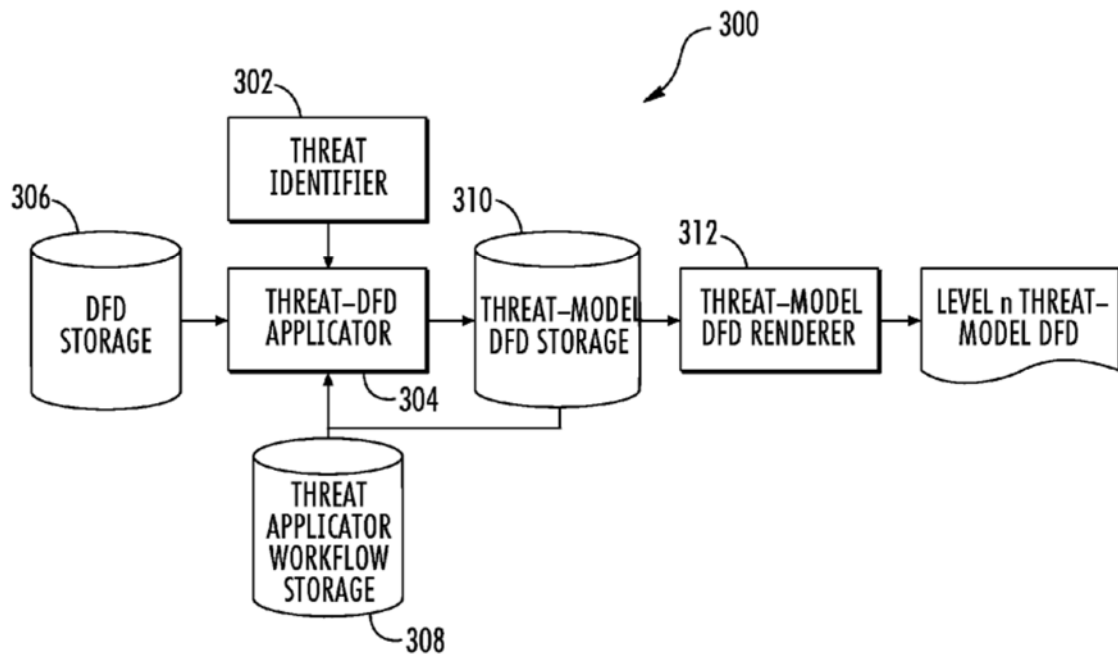
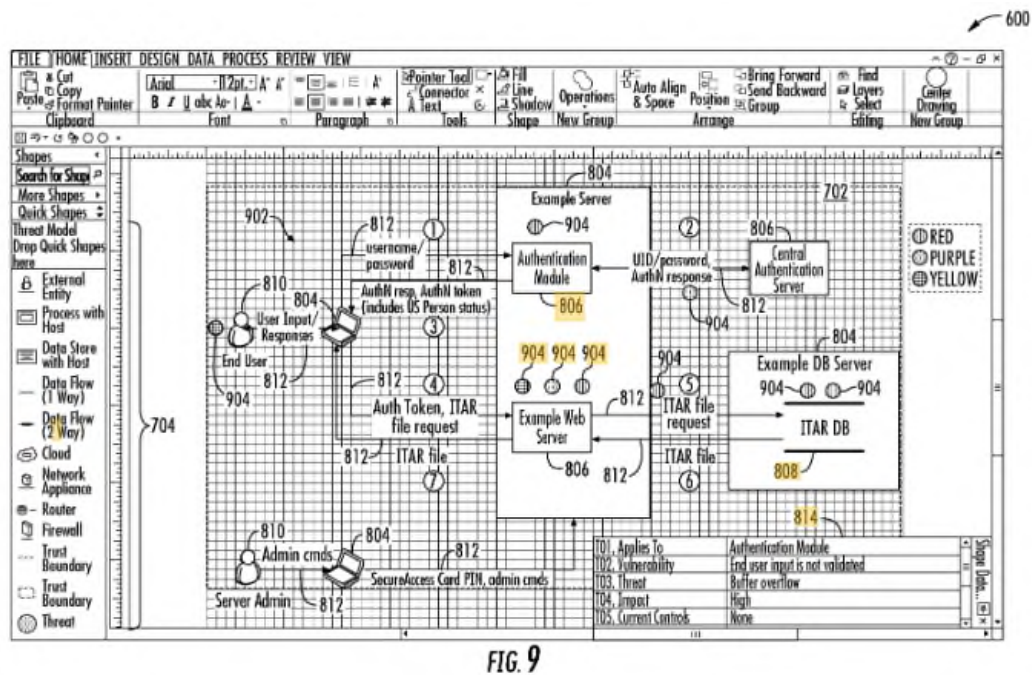
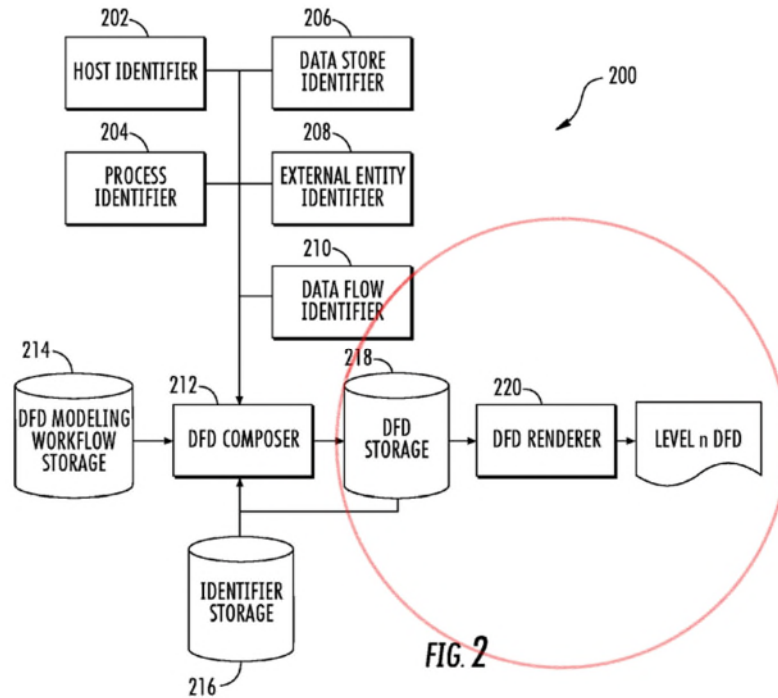


FIG. 3



- 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”

Jones discloses this element. EX-1003, ¶¶68-73. 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.

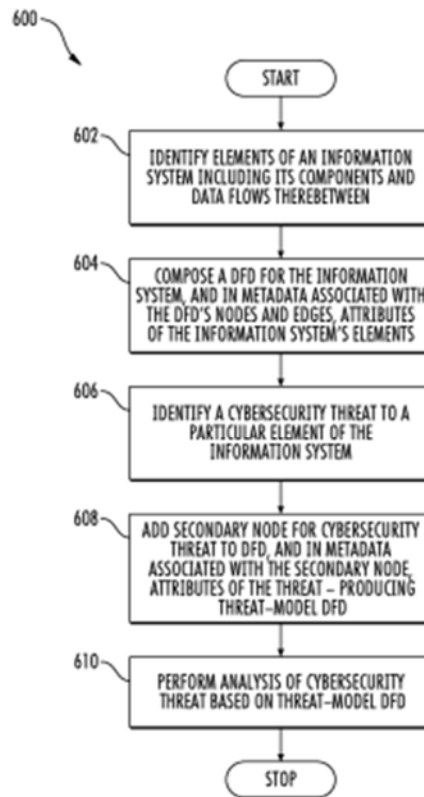


FIG. 6

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.

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; EX-1003, ¶70. 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, 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

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

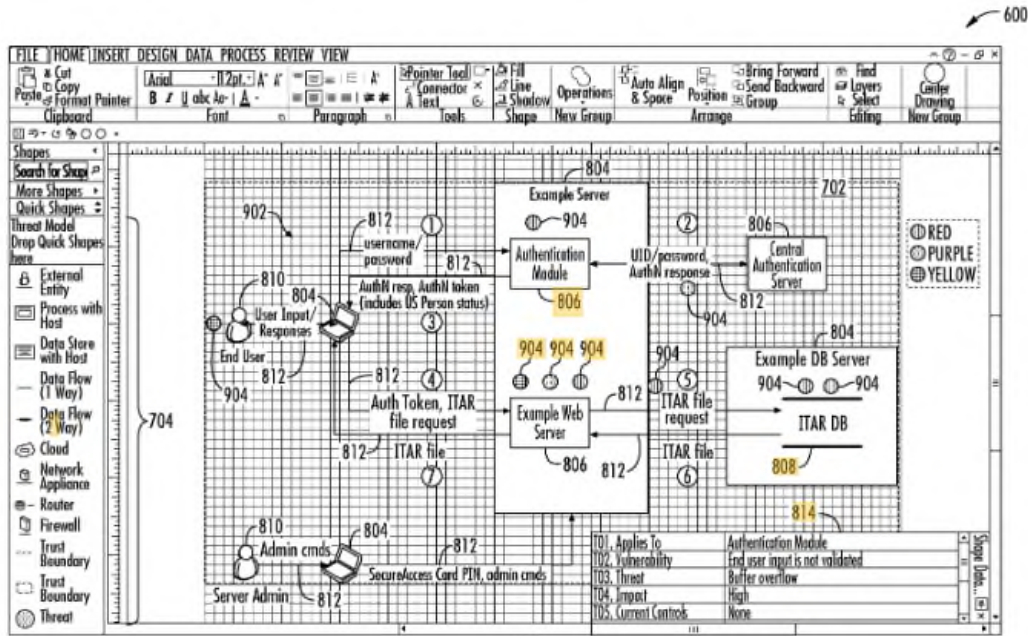


FIG. 9

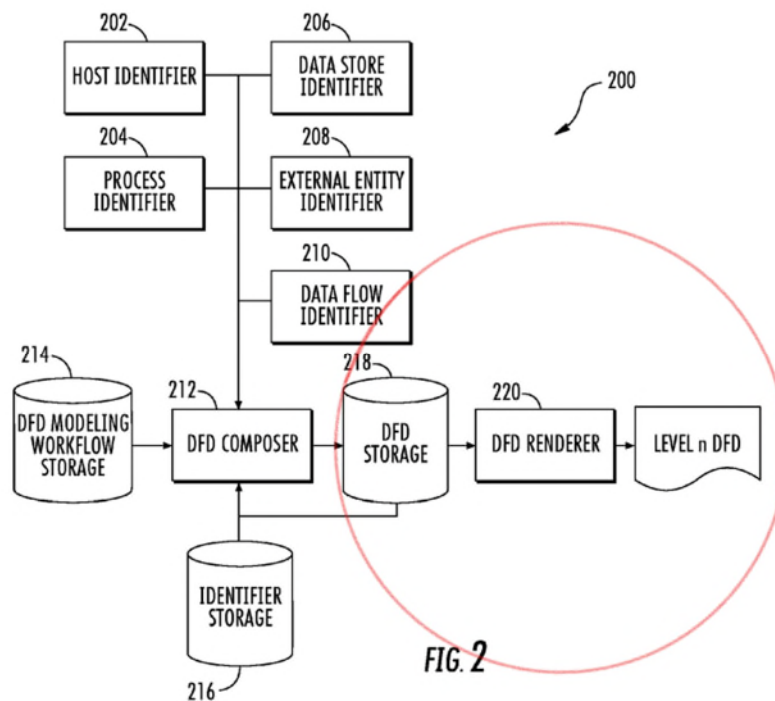
	T01. Applies To	Authentication Module
	T02. Vulnerability	End user input is not validated
	T03. Threat	Buffer overflow
	T04. Impact	High
	T05. Current Controls	None

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.

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). EX-1003, ¶72.

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;”**

Jones discloses this element. EX-1003, ¶¶74-76. 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:”

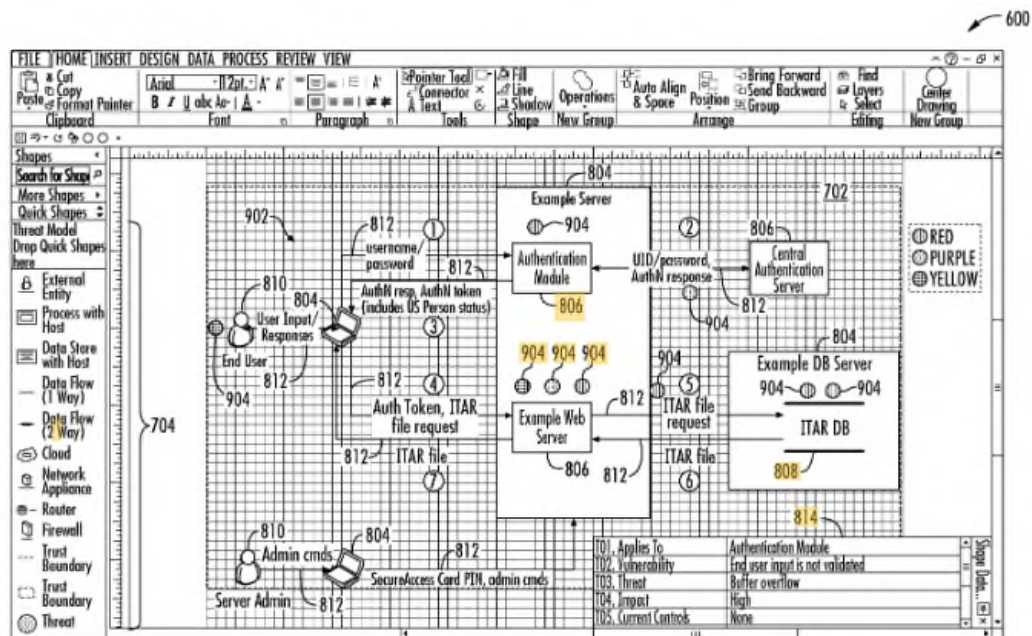
1004

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

● 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.

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. EX-1003, ¶75. A POSITA would further understand that Jones’ mitigations may include all well-known mitigation strategies in the art. *Id.*

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;”**

Jones discloses this element. EX-1003, ¶¶77-78. 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.

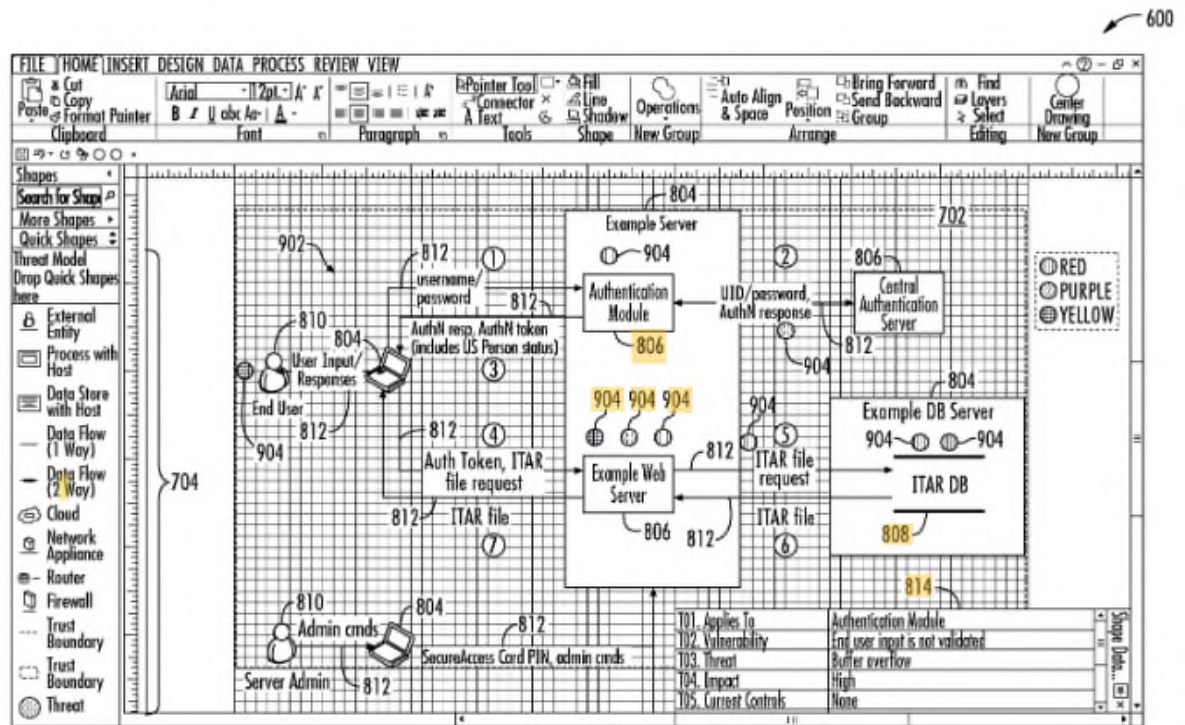


FIG. 9

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

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;”**

Jones discloses this element. EX-1003, ¶¶79-80. 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 at 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. This 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; EX-1003, ¶79.

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].

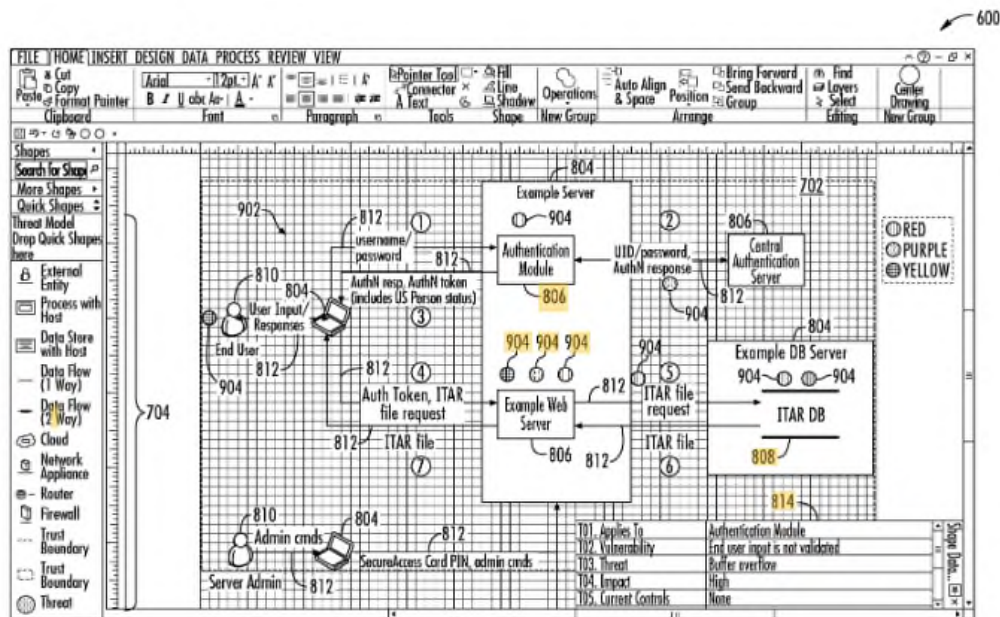


FIG. 9

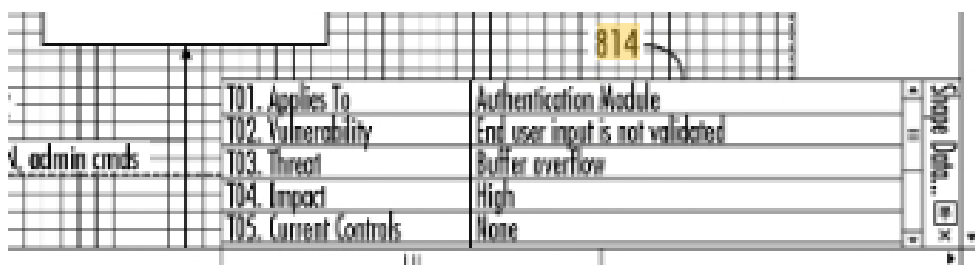


FIG. 9

Detail Fig. 9, 814.

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	RESTDUAL 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

- g. **Element 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 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.”**

Jones discloses this element. EX-1003, ¶¶81-84; *see also* 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

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 number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD.” *Id.* at 19:10-28. A POSITA would understand that the interrelated group of two or more threat model components in Jones may be predefined because Jones discloses identifying elements of the information system, which would be dependent on a predefined system when Jones’ system is applied. EX-1003, ¶82.

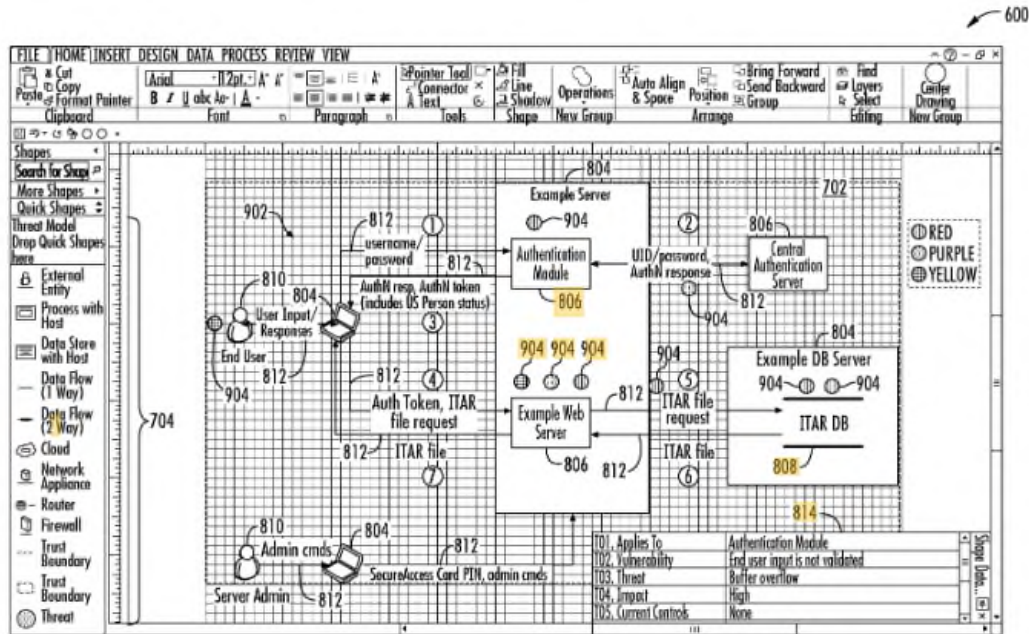


FIG. 9

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].

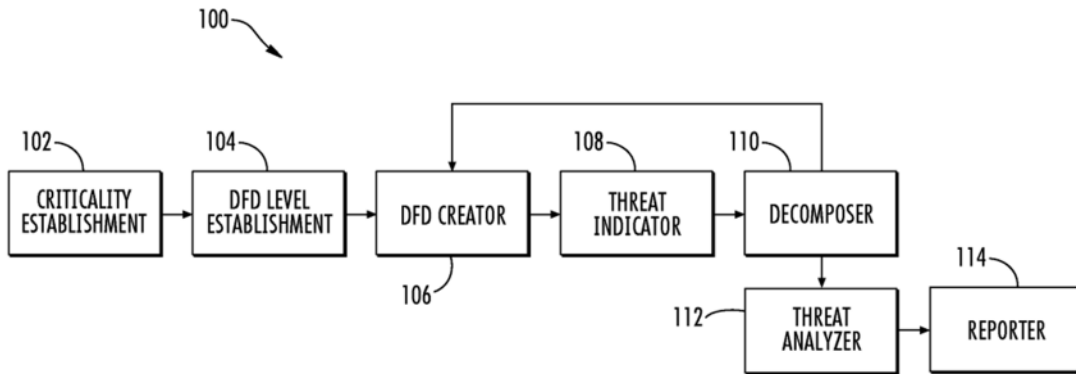


FIG. 1

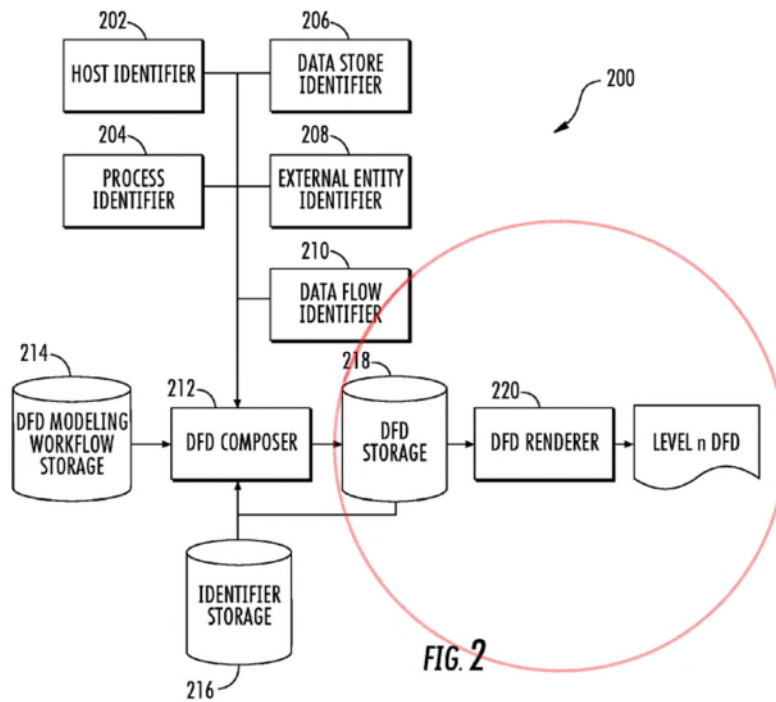


FIG. 2

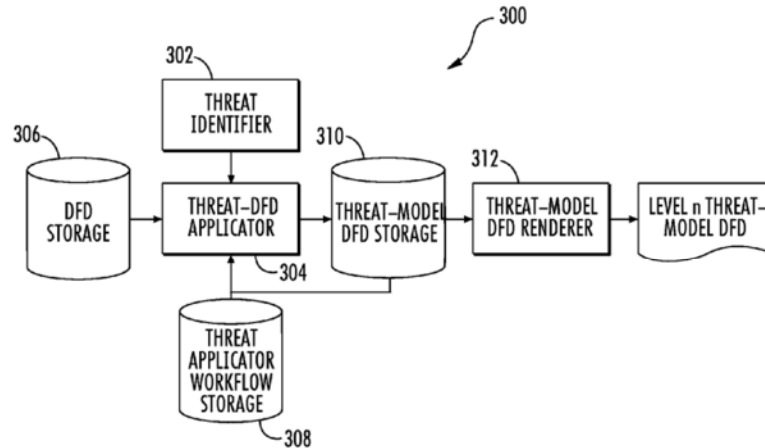


FIG. 3

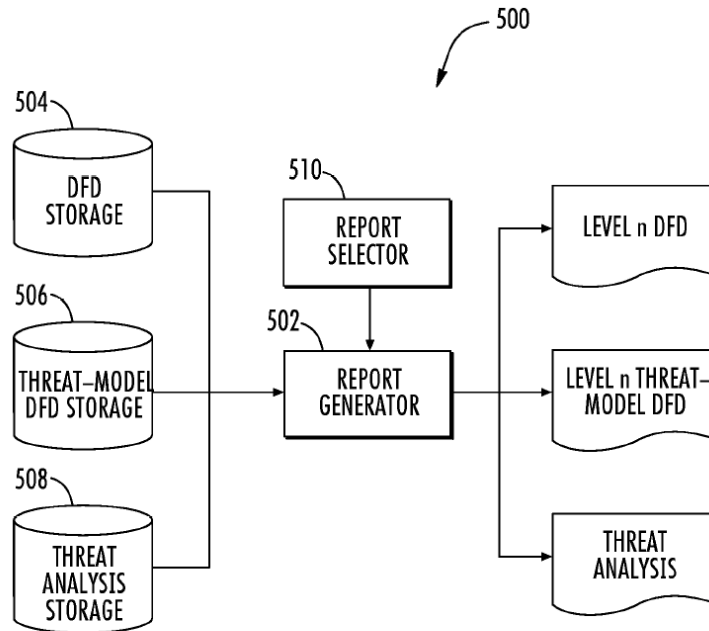


FIG. 5

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***

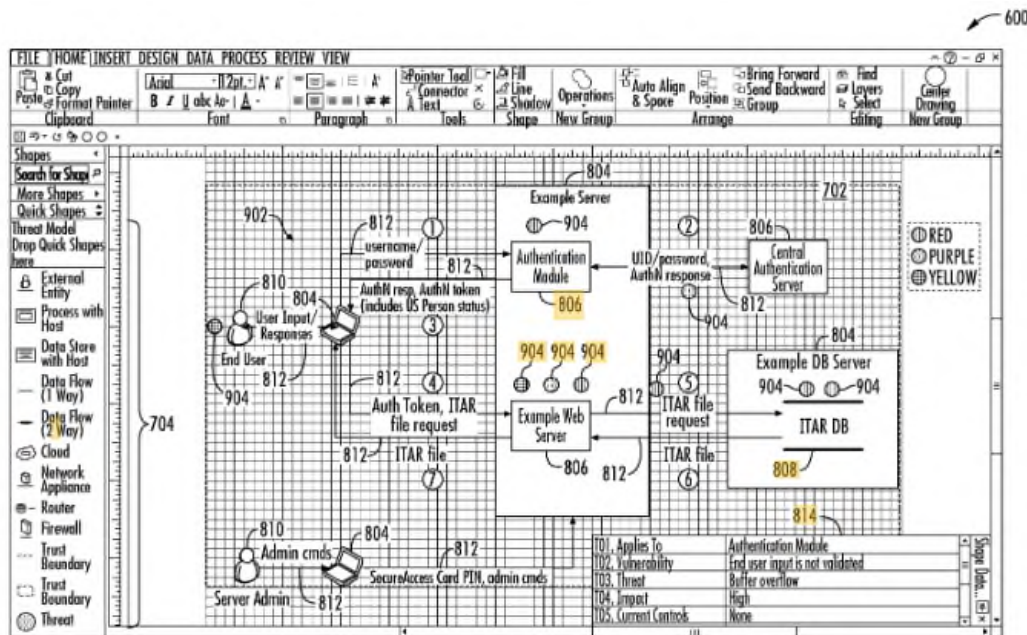
a workspace 702 for composition of a level n *DFD from shapes representing its nodes and edges*”); see also *id.* at 30-43, Figs. 7-9.

A POSITA would understand that Jones’ nesting disclosure meets this limitation. EX-1003, ¶84; 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.”**

Jones discloses this element. See Elements 1[p]-1[f]; EX-1003, ¶85. 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.”); EX-1003, ¶85. Moreover, Figs. 7-9 showing the GUI show multiple threats, threat model components, and compensating controls:



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: Jones, Zheng, and Keenan Render Claims 1-20 Obvious

Ground 1 is incorporated by reference in ground 2. Claims 1 and 3 are anticipated by Jones. Claims 2 and 4-20 are further rendered obvious by Jones in combination with Zheng and Keenan. EX-1003, ¶86.

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.”**

Zheng discloses this element. EX-1003, ¶¶87-88. 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, 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; EX-1003, ¶87. 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. EX-1003, ¶87.

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; EX-1003, ¶88.

2. **Claim 4:**

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

Zheng discloses this element. See Claim 2 (discussing attack methodologies); EX-1003, ¶89. “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:”**

Jones discloses this element. See Element 1[a]; EX-1003, ¶90.

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”**

Jones discloses this element. See Element 1[b]; EX-1003, ¶91.

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;”

Jones discloses this element. *See* Element 1[c]; EX-1003, ¶92.

- 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;”**

Jones discloses this element. *See* Element 1[d]; EX-1003, ¶93.

- 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.”**

Zheng discloses this element. *See* Claim 2; EX-1003, ¶94.

- 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.”**

Zheng discloses this element. EX-1003, ¶¶95-96. 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 as example 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; EX-1003, ¶95.

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.”**

Zheng, Jones, and Keenan disclose this element. EX-1003, ¶¶97-98.

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.

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; EX-1003, ¶98.

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.**

Jones, Zheng, and Keenan disclose this element. See Claim 6 (explaining toggle combination); EX-1003, ¶99. 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; EX-1003, ¶99.

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.”

Jones, Zheng, and Keenan disclose this element. See Claims 6-7; EX-1003, ¶100. 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; EX-1003, ¶100.

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.”

Jones, Zheng, and Keenan disclose this element. See Claims 6-8; EX-1003, ¶101. 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; EX-1003, ¶101.

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.”**

Zheng and Keenan disclose this element. EX-1003, ¶102. 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, at 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; EX-1003, ¶102; 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.”**

Jones discloses this element. *See* Claim 1[f]; EX-1003, ¶103.

10. **Claim 12:**

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

Zheng discloses this element. *See* Element 4[p]; EX-1003, ¶104.

- 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:”**

Jones discloses this element. *See* Element 1[d]; EX-1003, ¶105.

- 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;”**

Jones discloses this element. *See* Elements 1[a]-1[d]; EX-1003, ¶106.

- 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;”**

Jones discloses this element. *See* Elements 1[b]-1[e]; EX-1003, ¶107. 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.”**

Zheng discloses this element. *See* Claims 2, 5; EX-1003, ¶108.

- 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.”**

Zheng and Keenan disclose this element. *See* Claim 6; EX-1003, ¶109.

- 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.”**

Zheng and Keenan disclose this element. *See* Claim 7; EX-1003, ¶110.

- 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.”**

Zheng and Keenan disclose this element. *See* Claim 8; EX-1003, ¶111.

- 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.”

Zheng and Keenan disclose this element. See Claim 9; EX-1003, ¶112.

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.”**

Zheng and Keenan disclose this element. See Claim 10; EX-1003, ¶113.

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.”**

Jones discloses this element. EX-1003, ¶114. 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:

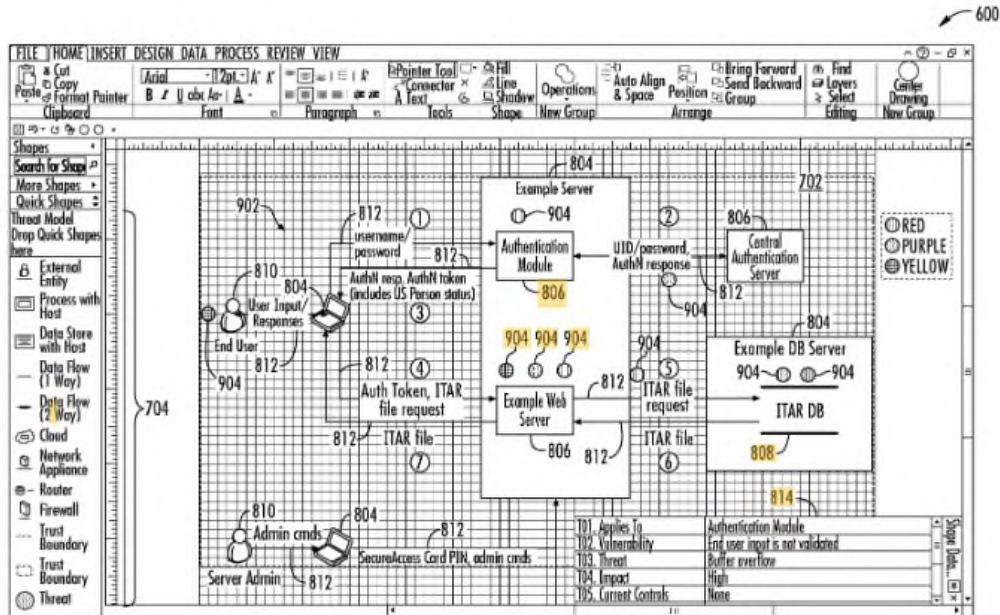
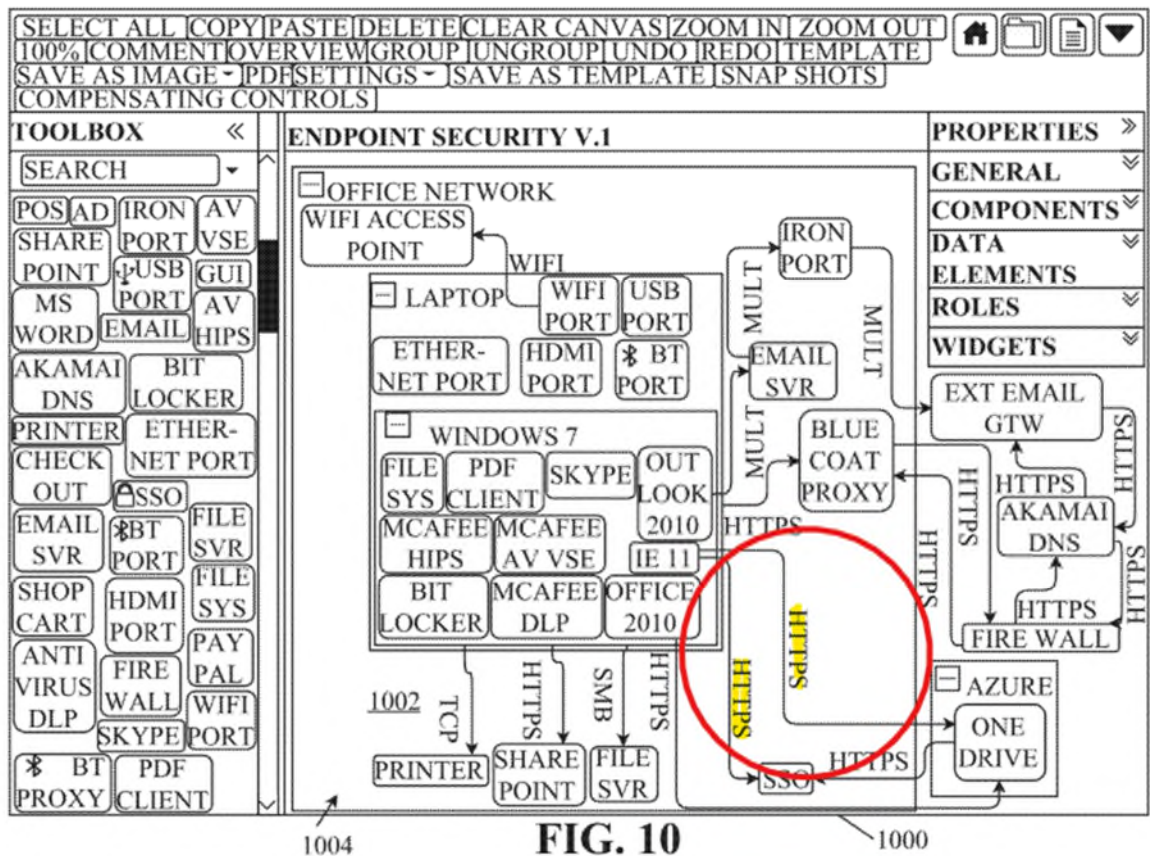


FIG. 9

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.”

Jones discloses this element. EX-1003, ¶¶115-16. 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”).

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

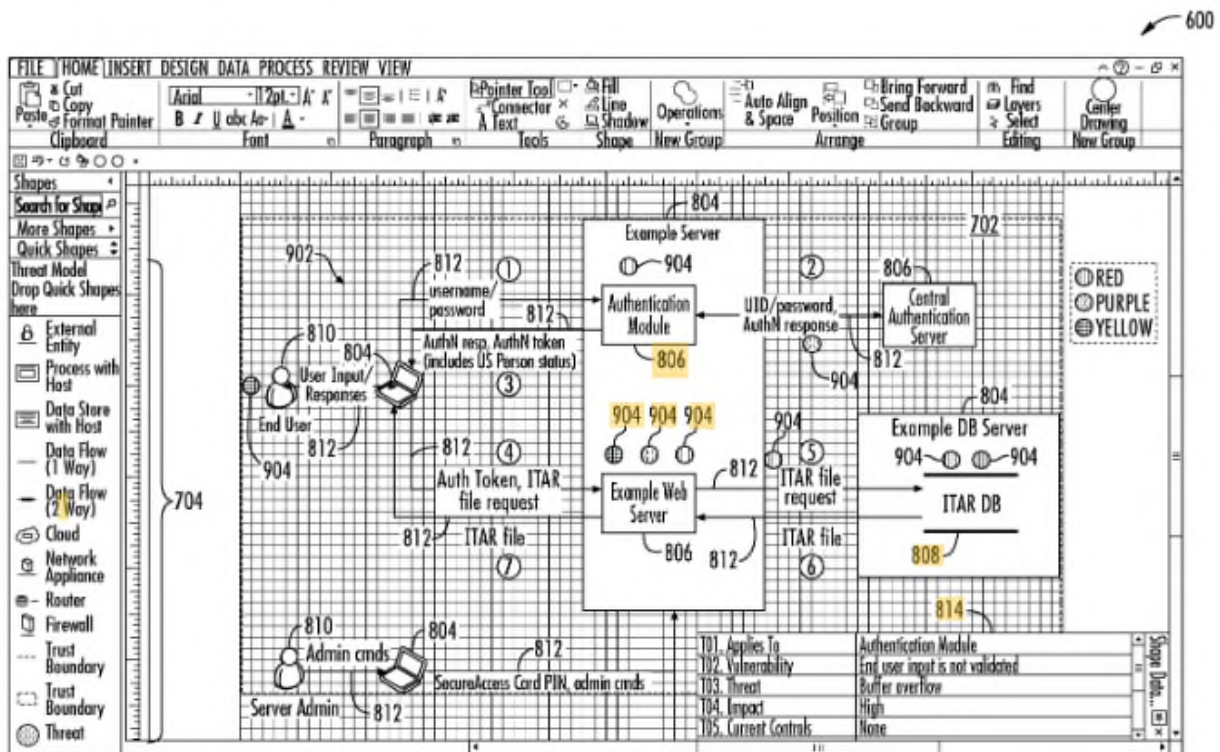


FIG. 9

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.”

Jones discloses this element. See Claim 11; EX-1003, ¶117.

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

A POSITA would have been motivated to combine Jones, Zheng, 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; EX-1003, ¶118.

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-1003, 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; EX-1003, ¶119. As explained by Petitioner's expert, "[m]ost practitioners who create threat models in a manual way look for ways to

simplify creating threat models using a computer and understandable visualizations.” EX-1003, ¶119.

Third, adding the visual features of Zheng and Keenan described above to the system of Jones would improve the overall user experience. EX-1003, ¶120. 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. 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. EX-1003, ¶120. 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. *Id.*

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. *Id.*, ¶121. Displaying and manipulating diagrams on computers was well known at the time and a POSITA

would be well versed in such programs. *Id.* 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. *Id.*

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

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. EX-1003, ¶122.

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* 16:42-51, 17:55-65; EX-1003, ¶123.

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. EX-1015, 1-4; EX-1003, ¶124.

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; EX-1003, ¶125.

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; EX-1003, ¶126.

Second, a POSITA would have been motivated specifically to add the “compensating controls” feature and the display of “attach 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; EX-1003, ¶127. To the extent this was not already disclosed in Jones, Zheng, and Keenan, 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. EX-1003, ¶127.

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 challenge in implementing this combination. EX-1003, ¶128.

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

For limitations 1[e], 11, and 20, if it is found that Jones, Zheng, and Keenan 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. EX-1003, ¶129.

Reith discloses a “Recombinant Threat Models,” as shown in Fig. 4:

400

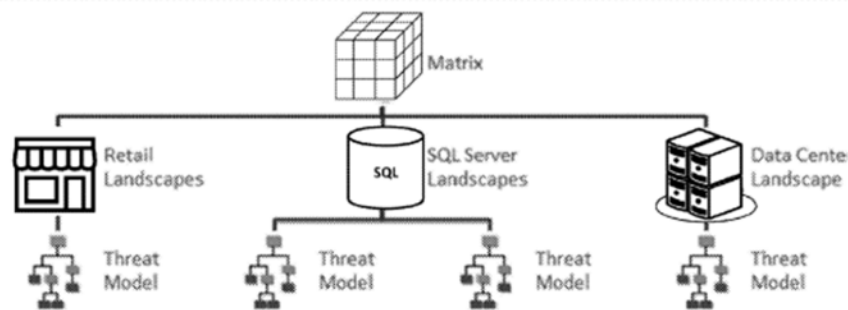


Figure 4

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; EX-1003, ¶129.

A POSITA would have been motivated to combine the references of ground 3 with Reith. First, like the references of ground 3 and the ’008 patent itself, Reith relates to the same general subject matter of generating threat models on a computer. *See* EX-1008, Abstract; EX-1003, ¶130.

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. EX-1003, ¶131.

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. EX-1003, ¶132.

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

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, and 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, and Yu, a POSITA would arrive at the toggling limitations 5-8 and 13-15. EX-1003, ¶133.

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. EX-1003, ¶134.

XI. THIS PETITION IS PROPER UNDER 35 U.S.C. §§ 314(a) AND 325(d)

The *Fintiv* factors weigh against discretionary denial. *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020) (precedential).

A. Stay

Petitioner intends to promptly seek a stay of the Litigation if the Board institutes this proceeding. This factor weights against discretionary denial, or at worst, is neutral.

B. Trial Date

The deadline for a Final Written Decision will be around October 2024. In the Litigation, the Court has set a *Markman* hearing for June 21, 2024, and a trial date of April 7, 2025, six months after the Final Written Decision would be issued in this IPR. EX-1009, pp. 9, 13. This factor weighs against a discretionary denial.

C. Parallel Proceeding

In *Sand Revolution*, the parties had already exchanged infringement and invalidity contentions, and the court had issued a *Markman* Order. *Sand Revolution II, LLC v. Continental Intermodal Grp. - Trucking LLC*, IPR2019-01393, Paper 24 (June 16, 2020) (informative). Despite these facts, the Board found that the third *Fintiv* factor “weighs only marginally, if at all, in favor of exercising discretion to

deny institution.” *Id.* Here, the Litigation is at a drastically earlier phase.

Infringement contentions will be served on May 19, 2023, invalidity contentions will be served on June 16, 2023, and the *Markman* hearing will be held on June 21, 2024. EX-1009, pp. 3, 9. This factor weighs against discretionary denial.

D. Issue Overlap

Petitioner has stipulated that, to the extent the Board institutes this IPR Petition, Petitioner will not pursue in the Litigation the grounds raised in this Petition. EX-1010. Moreover, the prior art in the Litigation will include a substantial number of references not at issue in this IPR. This factor weighs against discretionary denial.

E. Same Party

Petitioner and the PO are the parties in the Litigation. However, members of the Board have noted that *Fintiv* “says nothing about situations in which the petitioner is the same as, or is related to, the district court defendant.” *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15, at *10 (PTAB May 15, 2020) (APJ Crumbley, dissenting). This factor is neutral.

F. Other Considerations

The ’008 patent has never been challenged in a post-issuance proceeding, and the references used herein were not cited during prosecution. This factor weighs against discretionary denial.

Moreover, this Petition presents compelling unpatentability challenges that warrant institution. *See* USPTO Memorandum, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation.

XII. CONCLUSION

Petitioner has shown a reasonable likelihood of prevailing on claims 1-20 and requests institution of *inter partes* review and cancellation of these claims.

Respectfully submitted,

Dated: April 7, 2023

/Brent Yamashita/
Brent Yamashita

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(c) and (d), Petitioner certifies that the word count of Petitioner's Petition for *Inter Partes* Review (exclusive of any table of contents, table of authorities, mandatory notices under § 42.8, certificates of service and word count, and list of exhibits or claim listing) as measured by Microsoft Word is 9,865 words.

By: /Brent Yamashita/
Brent Yamashita

CERTIFICATE OF SERVICE ON PATENT OWNER

UNDER 37 C.F.R. § 42.105

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that, on April 7, 2023, a complete and entire copy of this Petition for *Inter Partes* Review, together with all supporting exhibits, were served on Patent Owner electronically, by agreement, by emailing a copy of the same to the following attorneys for the Patent Owner:

whelge@davidsonberquist.com
jwilson@davidsonberquist.com
esong@davidsonberquist.com

By: /Brent Yamashita/
Brent Yamashita