UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE, INC.,
Patent Owner.

Case IPR2023-00821
Patent 10,699,008

PATENT OWNER RESPONSE

TABLE OF CONTENTS

I. INTRODUCTION 1

II. LEVEL OF ORDINARY SKILL IN THE ART 3

III. BACKGROUND 3

A. Priority Date of the '008 Patent 3

B. Overview of the '008 Patent 3

C. File History of the '008 Patent 9

IV. SUMMARY OF REFERENCES 11

A. U.S. Patent No. 9,602,529 ("Jones") (EX-1004) 12

B. U.S. Patent No. 10,503,907 ("Zheng") (EX-1005) 13

C. U.S. Patent No. 11,200,228 ("Keenan") (EX-1006) 14

D. U.S. Patent No. 9,948,652 ("Yu") (EX-1007) 15

E. U.S. Patent No. 10,216,938 ("Reith") (EX-1008) 15

V. CLAIM CONSTRUCTION 16

A. "Redefine the First Threat Model by Including In It a Second Threat Model Associated with the Component Group" 16

B. "Threat Model Components" 20

C. Applicability of *Ex Parte Schulhauser* 21

VI. THE CHALLENGED CLAIMS ARE NOT UNPATENTABLE 23

A. Ground 1: Jones Does Not Anticipate Claims 1 and 3 23

1. Jones Does Not Disclose Adding a Component Group to a First Threat Model 23

2. Jones Does Not Disclose "Display[ing] a Relational Diagram

… Using … Visual Representations of One or More of the Compensating Controls" as Required by Element 1[e] 29

3. Jones Does Not Teach or Suggest Claim 3 31

B. Ground 2: Alleged Obviousness of Claims 1-20 Over Jones, Zheng, and Keenan 33

1. Dependent Claim 2 33

2. Independent Claim 4 39

3. Dependent Claims 6 and 7 40

4. Dependent Claim 8 42

5. Dependent Claim 9 43

6. Dependent Claim 10 44

7. Dependent Claim 11 45

8. Independent Claim 12 45

9. Dependent Claim 13 46

10. Dependent Claim 14 47

11. Dependent Claim 15 47

12. Dependent Claim 16 47

13. Dependent Claim 17 47

14. Dependent Claim 19 47

C. Ground 3: Alleged Obviousness of Claims 1-20 Based on Jones, Zheng, Keenan, and Yu 50

D. Ground 4: Alleged Obviousness of Claims 1-20 Based on Jones, Zheng, Keenan, Yu, and Reith 51

E. Ground 5: Alleged Obviousness of Claims 5-8 and 13-15 Based

on the References of Ground 4 and the Knowledge of a POSITA 54

VII. CONCLUSION.....55

TABLE OF AUTHORITIES

Page(s)

Cases

Applied Med. Res. Corp. v. U.S. Surgical Corp.,
448 F.3d 1324 (Fed. Cir. 2006) 43

CAE Screenplates Inc. v. Heinrich Fiedler GmbH & Co. KG,
224 F.3d 1308 (Fed. Cir. 2000) 43

MicroStrategy Inc. v. Business Objects Americas,
238 F. App'x 605 (Fed. Cir. 2007).....43

SAS Institute, Inc. v. Iancu,
138 S. Ct. 1348 (2018).....34, 39

Ex Parte Schulhauser,
No. 2013-007847, 2016 WL 6277792 (PTAB Apr. 28, 2016).....16, 21, 22, 23

Other Authorities

Consolidated Trial Practice Guide 54

EXHIBITS

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

I. INTRODUCTION

The Board should deny IriusRisk Inc.'s ("IriusRisk" or "Petitioner")[1] Petition against Claims 1-20 (collectively, "the Challenged Claims") of the '008 Patent (EX-1001).

Contrary to the Petition, the Jones reference does not anticipate claims 1 and 3. From claim 1, Jones does not disclose: (1) "add[ing] 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" (Element 1[f]), or (2) "configuring the diagram interface to display a relational diagram" using "visual representations of one or more of the compensating controls" (Element 1[e]). From claim 3, Jones does not disclose the storing of "additional" threat model components, threats, and compensating controls that are in addition to the threat model components, threat, and compensating controls recited in claim 1.

For Ground 2, Zheng does not teach or suggest visually displaying attack paths of all threats associated with a threat model component "in response to

[1] Petitioner and Patent Owner are direct competitors in the threat modeling business.

receiving a user selection of one of the diagrammed threat model components of the first threat model." Zheng does not teach or suggest the selection of any threat model components much less the selection of "one" threat model component. The Petition also fails to provide an adequate explanation of how and why the teachings of Zheng and Jones can be combined. Jones teaches displaying attributes of a single threat – not even all threats for a particular diagram component. Zheng is on the other end of the spectrum. Zheng displays all threats for all diagram components. The Petition and Mr. Hurlbut do not attempt to reconcile these divergent teachings.

Patent Owner also identifies distinguishing characteristics for several of the dependent claims beyond these above-described distinctions.

The references added in Grounds 3-5 are not alleged to cure all of the deficiencies identified by Patent Owner in Grounds 1 and 2. Moreover, at least for Grounds 3-5, the Petitioner and its expert make conclusory assertions about why a POSITA would have combined the cited references. Rather than conclusions, Petitioner and its expert were required to provide evidence supporting their conclusions. They failed to do so.

In Ground 4, Petitioner does not properly apply the claim language to find that Reith discloses threat model chaining as recited in the claims. In addition, the

reason to combine Reith with other references is obviously based on hindsight as it comes from the specification of the '008 Patent.

The Board should determine that Petitioner has not shown that any of the Challenged Claims are unpatentable.

II. LEVEL OF ORDINARY SKILL IN THE ART

Solely for purposes of this IPR, Patent Owner does not contest Petitioner's proposed definition of a person of ordinary skill in the art.

A "POSITA" refers to a person of ordinary skill in the art.

III. BACKGROUND

A. Priority Date of the '008 Patent

U.S. Patent Application No. 16/228,738 ("the '738 Application") was filed on December 20, 2018. The '738 Application issued as the '008 patent on June 30, 2020. The '738 Application claims priority to four U.S. Provisional Applications, the earliest of which was filed on May 17, 2017. EX-1001, 1-2; EX-2003, ¶56.

IriusRisk's petition for *inter partes* review and Mr. Hurlbut's expert opinions are based on the May 17, 2017 priority date. Petition, 8; EX-1003 ¶47. Accordingly, this Patent Owner Response assumes the '008 Patent has a priority date of May 17, 2017. EX-2003, ¶57.

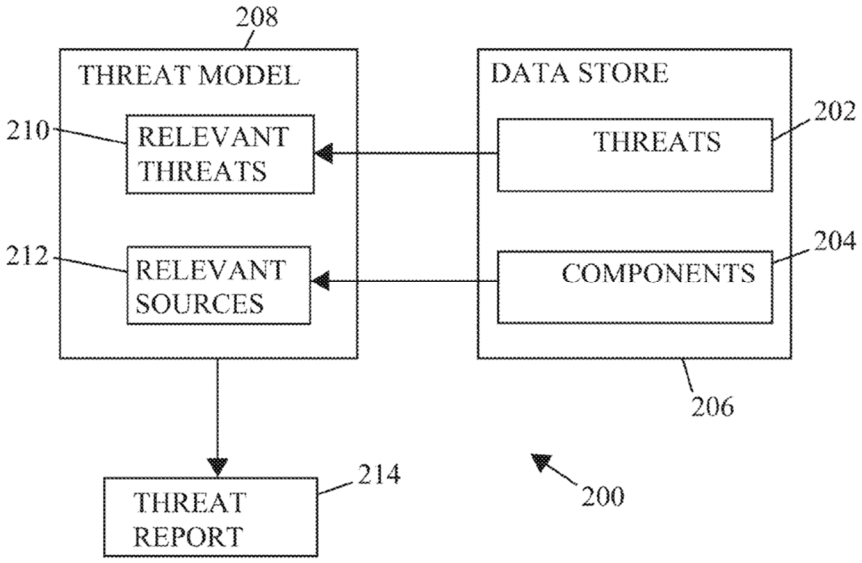
B. Overview of the '008 Patent

The '008 Patent is entitled "Threat Model Chaining and Attack Simulation

Systems and Related Methods" and relates to threat modeling systems and processes. EX-1001, cover page. The '008 Patent explains that "[t]hreat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized." EX-1001, 1:48-49; EX-2003, ¶58.

Threat modeling can be applied to a broad range of environments or activities. EX-1001, 1:54-58. "With regards to modeling computing networks, traditional threat modeling systems and methods exist for assessing risk from potential cyber threats at an individual application level without fully accounting for application-application interactions, thereby miscalculating organizational risk." EX-1001, 1:62-66; EX-2003, ¶59.

Figure 2 of the '008 Patent is one example of a threat modeling process of the invention that is applicable to any application, process, or system under consideration. EX-1001, 8:38-41; EX-2003, ¶60.



The '008 Patent explains that threat models are created from defined threats and threat model components, which are stored within a database. EX-1001, 8:50-56 ("As illustrated in FIG. 2, process 200 may include storing a plurality of threats 202 and threat model components (components) 204 in a data store 206. This may include, by non-limiting example, storing titles, definitions or descriptions, and/or associated images in the database 108 for each component and/or threat. The threats and components are used to create threat model 208."). The "database allows for the correlation of any threat to any number of components and likewise, the correlation of any component to any number of threats." EX-1001, 9:48-52. "[E]ach asset could have any number of threats that could threaten to compromise it. … Some assets may be threatened by only a single threat, some may be

threatened by two or three threats, or more, and so forth." EX-1001, 24:4-10; EX-2003, ¶61.

Referring to Figure 2, a user selects from among the available components those components which are relevant to any given system, process or application being examined. This process is represented by the arrow between the components 204 and the relevant sources 212. The relevant sources are the sources determined by the system that are involved in the specific application, system or process and defining relationships between and among the relevant components. The system also retrieves from the database where the threats and components are stored, the threats that were previously correlated with the components to thereby form the threat model 208. The threat model includes the relevant threats and the relevant sources of those threats related in a manner that corresponds to the architecture of the system being modeled. The threat model can be used to generate a threat report 214. EX-2003, ¶62.

The '008 Patent describes each "threat model component" as "a potential relevant source for one or more threats." EX-1001, 9:28-30. One example provided in the specification is that one threat may be "Bluejacking," in which a potential attacker may seek to gain improper access to a system via its Bluetooth interface. In this example, the threat model component is the "Bluetooth port," *i.e.*,

the potential source of the threat. EX-1001, 9:28-32. As another example, an "online banking interface" may be stored as a threat model "component," and "a threat may be a virus being introduced to the bank's environment through a breach in the banking interface." EX-1001, 24:42-52; EX-2003, ¶63.

Similar to the described embodiments above, the challenged claims of the '008 Patent recite a "database," and in claim 1, the database comprises, in relevant part, "a plurality of threat model components stored therein; a plurality of threats stored therein, each threat associated with at least one of the threat model components through the one or more databases; and a plurality of compensating controls stored therein, each compensating control associated with at least one of the threats through the one or more databases." Independent claims 4 and 12 include substantially similar features. As claimed, the "database" does not simply store a numeric value as a property or characteristic of a component. Rather, as claimed, the one or more databases expressly stores "a plurality of threats," and associates each of the threats with "at least one of the threat model components through the one or more databases." EX-2003, ¶64.

The independent claims of the '008 Patent recite at least two inventive features. Independent claim 1 of the '008 patent recites that the diagram interface is configured to "add a component group to the first threat model and thereby

redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components." EX-1001, 35:56-63. Independent claims 4 and 12 of the '008 Patent recite that, in response to a user selection of one of the diagramed threat model components, the diagram interface is configured to "visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component." EX-1001, 36:36-42, 37:44-38:3; EX-2003, ¶65.

The '008 Patent explains that a group of threat model components can be diagrammed separately as an independent threat model and then saved as a component so that it can be imported into another threat model. EX-1001, 20:23-26. That newly created "component" can be saved, for example, in a toolbox menu as a single item. EX-1001, 20:37-39. For example, a user could define a "Windows 7" component group. EX-1001, 20:39-41. That group may include, for example, a file system, PDF client, Skype, Outlook 2010, McAfee HIPS, McAfee AV VSE, Internet Explorer 11, Office 2010 and other components. EX-1001, 19:52-56. Once created and stored, a user could add the Windows 7 component to another threat model thereby importing into the threat model the threats associated with the Windows 7 threat model. EX-1001, 20:41-45. When a user adds a

component group to an existing threat model, the threat model of the component group is added to (or "nested" within) the existing threat model. EX-1001, 20:26-30. In this way, a user can modify a threat model by incorporating previously defined threat models for the component groups. EX-1001, 20:30-32. The '008 Patent also refers to this as "threat model chaining." EX-1001, 20:32-33; EX-2003, ¶66.

The second inventive aspect of the independent claims relates to displaying attack paths. The '008 Patent explains that a user can select a particular one of the threat model components (*e.g.*, an asset) and the system will display all attack paths (or what the '008 Patent also refers to as "attack vectors") associated with the threats which may compromise the asset. EX-1001, 23:13-16. Displaying all attack paths allows a user to determine what compensating controls may be included to protect the asset. EX-1001, 23:16-18. The user can add or remove compensating controls (or toggle compensating controls on or off) to see the effectiveness of the compensating controls. EX-1001, 23:18-26; EX-2003, ¶67.

C. File History of the '008 Patent

The '008 Patent was filed as U.S. Patent Application No. 16/228,738 ("the '738 application") on December 20, 2018. EX-1002, p.358; EX-2003, ¶68.

The Examiner issued an office action on August 8, 2019 rejecting all

pending claims based on judicially created double patenting and as being directed to nonpatentable subject matter. EX-1002, pp.392-401. On October 25, 2019, the applicant filed a response to the August 8, 2019 office action arguing against the non-patentable subject matter rejection and indicating that a terminal disclaimer would be filed to overcome the double patenting rejection. EX-1002, pp.427-454. Applicant filed the terminal disclaimer on the same day. EX-1002, pp.456-457. On November 20, 2019, the Examiner issued a second office action in which the Examiner withdrew the non-patentable subject matter rejection but maintained the double patenting rejection. EX-1002, pp.461-470. Counsel for applicant called the Examiner to advise that the applicant had already filed the required terminal disclaimer. The Examiner called back to say that a notice of allowance would be issued. EX-1002, p.492. The Examiner issued the Notice of Allowance on February 24, 2020. EX-1002, p.523; EX-2003, ¶69.

The '008 Patent issued on June 30, 2020 after, in relation to claims 1 and 4, the Examiner found that the cited prior art did not disclose or teach "*configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model, and*

configuring the diagram interface to, in response to receiving one or more inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components." EX-1002, p.528. The Examiner found that claim 12 was substantially similar to claims 1 and 4 as it relates to the reason for allowance and therefore allowed claim 4 and all dependent claims on that basis. *Id*.; EX-2003, ¶70.

On March 2, 2020, the applicant commented on the Examiner's reasons for allowance by stating that the applicant believed that each claim was patentable in its own right, for other reasons raised during prosecution, or as explained in the patent's specification. EX-1002, p.557. The '008 Patent issued on June 30, 2020. On July 6, 2020, the applicant's counsel filed a certificate of correction request. EX-1002, pp.584-585. The Patent Office issued two certificates of correction – one issued on October 5, 2020 correcting the specification (EX-1002, p.623) and the second issued on December 8, 2020 correcting the drawings (EX1002, pp.629-632); EX-2003, ¶71.

IV. SUMMARY OF REFERENCES

Petitioner requests review of the '008 Patent on the following grounds:

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

Petition, 11; EX-1003, ¶20; EX-2003, ¶72.

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

Jones discloses a system for modeling threats in "information systems." EX-1004, Abstract. In relevant part, Jones' information systems may include components such as hosts, processes, data stores and/or external entities, and data flows between those components. EX-1004, 5:4-6. The information system may be described as having a "hierarchical breakdown" or "hierarchy" of its components at different levels. EX-1004, 5:10-14. The information system may have multiple "nested" components, one or more of which may further have its own additional "nested" components at lower levels of the hierarchy. EX-1004, 5:14-19. In other words, the components of Jones' information system may have components that have subcomponents, and some of the subcomponents may have

their own subcomponents, etc. By moving from one layer of the hierarchy to another allows a user to examine threats at different "levels" of the information system. EX-1004, 5:4-19; EX-2003, ¶73.

Jones explains that if it is desired to look at the components of the information system in greater detail so as to examine their specific security threats, the decomposer 110 is used to "decompose" the components of the information system modeled by the data flow diagram ("DFD") into their "nested" subcomponents and the data flows between those subcomponents. EX-1004, 6:12-18. The "nested" subcomponents were already present in the information system and the threat model created by Jones' system for analyzing the information system. *See* EX-2002, 71:9-72:3, *see also* 51:25-52:22, 53:4-10, 70:6-23, 116:15-117:7. But the nested subcomponents were not visible at level "n" of the hierarchy, for example. Those subcomponents may become visible when the threat model components are "decomposed" into their level "n+1" subcomponents. *See* EX-2002, 71:9-72:3, *see also* 51:25-52:22, 53:4-10, 70:6-23, 116:15-117:7. The threats associated with the subcomponents and their threat modeling are included in the threat model for the component itself. *See* EX-2002, 54:4-14; EX-2003, ¶74.

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

Zheng is directed to a system for visualizing and analyzing security threats

in a suite of software applications. EX-1005, Abstract. Zheng's system includes multiple layers for visualizing different information available from the system. The system includes a base layer includes components representative of the software applications and relationships among the software applications. EX-1005, 1:46-52. The system includes a threat modeling module configured to identify security threats I the suite of software applications. EX-1005, 1:53-59. The system also includes a security controls module for implementing security controls to mitigate threats, and a threat update module for assessing the current state of security on a visually displayed map. EX-1005, 1:59-67. Zheng's system also includes a data flow module to facilitate display of simulated data flow through the components of the map. EX-1005, 2:19-25. Zheng defines a "security threat" as a threat actor, a threat target, and a displayable vector connecting the threat actor to the threat target. EX-1005, 2:36-39; EX-2003, ¶75.

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

Keenan relates to risk management – not threat modeling. Keenan was filed by and assigned to an insurance company: American International Group, Inc. Keenan assigns a risk value to certain aspects of a system, but the threats underlying that risk value are neither determined by Keenan nor important to Keenan. The purpose of Keenan is to provide a view that allows a user to see (via

a "view") an overall risk level associated with an infrastructure for business and insurance purposes, not to detail or prioritize vulnerabilities or threats. Keenan, 1:33-38. Keenan teaches that different "views" can display colors according to different properties, including the risk level, associated with various objects. EX-2003, ¶76.

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

Yu is directed to systems and methods for identifying threat vectors and implanting controls for security resources within a network. Yu determines threat vectors associated with the resources, and determines controls associated with the threat vectors. EX-1007, Abstract; EX-2003, ¶77.

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

Rieth discloses a system in which a "threat matrix" may include multiple "threat landscapes." Each threat landscape may include one or more "recombinant" threat models. EX-1008, 4:30-32. Each threat model may stand on its own within the threat landscape or it may be connected to other threat models. EX-1008, 4:32-35. A threat matrix represents all of the threats faced by an enterprise, government, or an organization in general. EX-1008, 4:41-44; EX-2003, ¶78.

The threat matrix may be comprised of recombinant threat models which

would allow for the cross-correlation of information from different threat models. EX-1008, 7:65-8:1. The threat matrix and threat models may be shows in a diagram or graph. EX-1008, 8:9-12. Each node in the graph represents an entity within the threat matrix. EX-1008, 8:16-18. Nodes have relationships to other nodes. EX-1008, 8:20-21. A node from one threat model may be connected to a node from a different threat model. EX-1008, 8:27-29; EX-2003, ¶79.

V. CLAIM CONSTRUCTION

In the Institution Decision, the Board invited the parties to address the proper construction of the following claim term: "redefine the first threat model by including in it a second threat model associated with the component group." Decision Granting Institution of *Inter Partes* Review, 15-16. Additionally, the Board invited the parties to address the potential applicability of *Ex Parte Schulhauser*, No. 2013-007847, 2016 WL 6277792 (PTAB Apr. 28, 2016) (precedential).

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

The claim phrase "redefine the first threat model by including in it a second threat model associated with the component group" appears in independent claim 1 and dependent claims 11 and 20. This phrase should be construed to mean "change the first threat model by adding a predefined interrelated component group

and its associated second threat model to the first threat model where the added component group was not a part of the first threat model before being added." This proposed construction is supported by the plain language of the claims and the specification. EX-2003, ¶81.

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

first threat model. EX-2003, ¶82.

The specification explains this further. The '008 Patent explains that a group of threat model components can be diagrammed separately as an independent threat model and then saved as a component so that it can be imported into another threat model. EX-1001, 20:23-26. That newly created "component" (*i.e.*, a "component group" in the language of the claims) can be saved, for example, in a toolbox menu as a single item. EX-1001, 20:37-39. For example, according to the specification, a user could define a "Windows 7" component group. EX-1001, 20:39-41. That group may include, for example, a file system, PDF client, Skype, Outlook 2010, McAfee HIPS, McAfee AV VSE, Internet Explorer 11, Office 2010 and other components. EX-1001, 19:52-56. Once created and stored, a user could add the Windows 7 component to another threat model thereby importing into the threat model the threats and threat model associated with the Windows 7 component group. EX-1001, 20:41-45. When a user adds a component group to an existing threat model, the threat model of the component group is added to (or "nested" within) the existing threat model. EX-1001, 20:26-30. In this way, a user can modify a threat model by incorporating previously defined threat models for the component groups. EX-1001, 20:30-32. The '008 Patent also refers to this as "threat model chaining." EX-1001, 20:32-33;

24:10-30; 32:11-39. Notably, however, the "nesting" is not simply an expansion of detail on the existing model. The "Windows 7" component is not an expansion on an existing computer component but is an addition that "redefines" the threat model and introduces new threat model components into the existing threat model. EX-2003, ¶83.

Figure 10 from the '008 Patent shows this "nested" arrangement graphically after the Windows 7 component group has been added to a first threat model. EX-2003, ¶84.

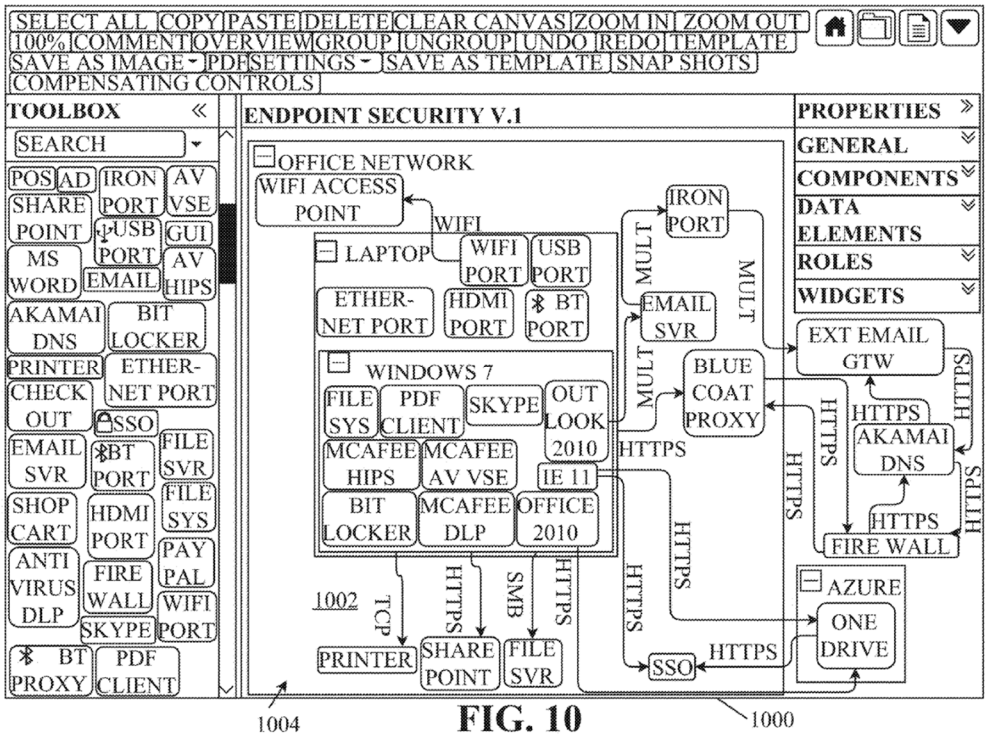


FIG. 10

In the center of Figure 10, the Windows 7 component group (shown in a box within the "laptop" box) has been added to the "Laptop" group. EX-2003, ¶85.

B. "Threat Model Components"

The '008 Patent describes each "threat model component" as "a potential relevant source for one or more threats." EX-1001, 9:28-30. One example provided in the specification is that one threat may be "Bluejacking," in which a potential attacker may seek to gain improper access to a system via its Bluetooth interface. In this example, the threat model component is the "Bluetooth port," *i.e.*, the potential source of the threat. EX-1001, 9:30-36. As another example, an "online banking interface" may be stored as a threat model "component," and "a threat may be a virus being introduced to the bank's environment through a breach in the banking interface." EX-1001, 24:42-52; EX-2003, ¶86.

Further, the '008 Patent explains that threat model components are not limited to physical components. Components can be steps, actions, or a physical component. EX-1001, 9:38-52. An example of a non-physical component/source is "merging onto freeway" when modeling the threats of commuting to work. "Merging onto freeway" is an action as opposed to a physical component that may be correlated to a threat such as a "freeway collision." EX-1001, 9:39-45; EX-2003, ¶87.

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

including a USB port, SSO (single sign on), Bluetooth port, and Bluetooth proxy. EX-1001, 17:12-17; EX-2003, ¶88.

The term "threat model components" should be construed as "a potential relevant source for one or more threats." Petitioner and its expert agree with this construction. Petition, 12; EX-1003, ¶51; EX-2003, ¶89.

C. Applicability of *Ex Parte Schulhauser*

In the Institution Decision, the Board asked the parties to consider whether *Ex parte Schulhauser*, No. 2013-007847, 2016 WL 6277792 (PTAB Apr. 28, 2016) (precedential), applies to the limitations of the claims of the '008 Patent. Institution Decision, 16. The example limitation the Board asked the parties to consider was "configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model." It is not clear what aspect of *Schulhauser* the Board believed may apply to the '008 Patent claims. Thus, Patent Owner reserves the right to address other aspects of *Schulhauser* in its Sur-Reply should it become clear that the Patent Owner Response addresses the incorrect aspect of *Schulhauser*.

One of the dominant aspects of *Schulhauser* is its analysis of conditional claim language. *Schulhauser* at 6 ("the method includes several steps that only need to be performed if certain conditions precedent are met."). In short,

Schulhauser does not apply to the claims of the '008 Patent.

As stated above, the claims in *Schulhauser* included method steps that were only performed if certain conditions precedent were met. For example, claim 1 in *Schulhauser* recites steps such as "triggering an alarm state *if the electrocardiac signal data is not within the threshold electrocardiac criteria*" and "determining the current activity level of the subject from the activity level data *if the electrocardiac signal data is within the threshold electrocardiac criteria*." *Schulhauser* at 6. By its plain language, each of these two method steps were only performed if the recited condition is met.

The example limitation from the '008 Patent the Board identified is "configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model." There is no condition present in this claim language. EX-2003, ¶91. Instead, to satisfy the claim, the claim requires that the system "receiv[e] one or more user inputs," and in response to the one or more inputs, "configure[e] the diagram interface to … add a component group to the first threat model." To satisfy this step, both the user input(s) must be received and the diagram interface must be configured to add a component group. In fact, this claim language has an additional requirement that the user input is received before the diagram interface is configured. EX-2003,

¶92.

Other claims recite similar language such as "receiving a [user] selection" (claims 2, 4, 12), "receiving one or more user inputs" (claims 3, 5, 8-12, 15-17, 19-20), "receiving a user toggle" (claims 6, 7), and "receiving a user input" (claims 13, 14).[2] In each of these cases, the same analysis applies. The "receiving" of the input, selection, or toggle are required elements of the claims. These are not conditions determining whether a particular method step needs to be performed. *Schulhauser* does not apply to the claims of the '008 Patent. EX-2003, ¶93.

VI. THE CHALLENGED CLAIMS ARE NOT UNPATENTABLE

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

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

Claim 1 reads, in part:

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

[2] Claims 12-20 are not method claims. Thus, the analysis of *Schulhauser* does not apply to these claims for this reason alone. In system claims 12-20, there are no method steps, and thus, there are no method steps that can be conditionally performed.

> interrelated group of two or more of the threat model components.[3]

EX-1001, 35:56-63. This portion of claim 1 requires that the "component group" that is added to the first threat model must comprise "a predefined interrelated group of two or more of the threat model components." Thus, the "component group" must be defined before it is added to the first threat model. The claim language also requires that the "component group" is "add[ed]" to the first threat model. This means that the component group could not have been part of the first threat model prior to being added. The claim language also explains that the addition of the component group to the first threat model "thereby redefine[s]" the first threat model "by including in it a second threat model associated with the component group." Thus, the component group must have had its own "second" threat model before it was added to the first threat model. The addition of the component group also requires that the threat model of the component group is added to the first threat model. EX-2003, ¶¶96-97.

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

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

information system may be described as having a "hierarchical breakdown" or "hierarchy" of its components at different levels. EX-1004, 5:10-14. The information system may have multiple "nested" components, one or more of which may further have its own additional "nested" components at lower levels of the hierarchy. EX-1004, 5:14-19. In other words, the components of Jones' information system may have components that have subcomponents, and some of the subcomponents may have their own subcomponents, etc. By moving from one layer of the hierarchy to another allows a user to examine threats at different "levels" of the information system. EX-1004, 5:4-19; EX-2003, ¶98.

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

model components are "decomposed" into their level "n+1" subcomponents. *See* EX-2002, 71:9-72:3, *see also* 51:25-52:22, 53:4-10, 70:6-23, 116:15-117:7. The threats associated with the subcomponents and their threat modeling are included in the threat model for the component itself. *See* EX-2002, 54:4-14. Notably, the DFD creator modifies the "threat-model DFD ***for*** the decomposed components." *Id.*, 6:18-22. This illustrates that the threat model is updated to show more detail as existing components are further analyzed. EX-2003, ¶99.

In Jones, the subcomponents at the n+1 level of the hierarchy are already included in the level n threat model. The decomposer 110 simply exposes some selection of those level n+1 subcomponents so that the threats associated with those subcomponents can be analyzed. EX-2003, ¶100.

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

system. EX-2003, ¶101.

Element 1[f] also requires that the "component group" that is added to the first threat model must be a "predefined" interrelated group of threat model components. Petitioner and its expert, Mr. Hurlbut, argue that Jones discloses a "predefined" group of threat model components because the underlying information system is predefined. EX-1003, ¶82 (p.45); EX-2002, 76:5-19. Just because the information system in Jones is "predefined" says nothing about whether there is a "component group" including a "predefined interrelated group" of threat model components. There is no teaching in Jones that a "component group" of threat model components is "predefined." Petitioner's and Mr. Hurlbut's assertion to the contrary is conclusory and not based on any evidence.[4] On the other hand, Jones describes the decomposer as doing analysis when decomposing

[4] Mr. Hurlbut's testimony is tainted by bias. Mr. Hurlbut knows many of the leaders of IriusRisk including its CEO, COO, VP of Product Development, and one of its technical advisors. EX-2002, 10:10-16; 11:5-11; 11:16-12:9; 12:20-22. In fact, IriusRisk's CEO personally asked Mr. Hurlbut to serve as an expert in this IPR and related IPR2023-00656. EX-2002, 17:21-23. Mr. Hurlbut works for another company that is in the threat modeling business named Aquia where he is head of their threat modeling business. EX-2002, 13:5-11; 14:5-8; 7:25-8:11. Mr. Hurlbut has stock options in his employer. EX-2002, 8:4-11. One of the reasons why Mr. Hurlbut wanted to work on these IPRs was to see "[h]ow I could help …." EX-2002, 18:21-22. Given the personal and professional connections to IriusRisk, and his personal interest in competitor Aquia, Mr. Hurlbut is not a disinterested participant in these proceedings.

existing components. As discussed above, Jones discloses decomposing components based on their existing hierarchy; however, how it chooses to decompose (which elements get included in the n+1 decomposition) is up to the decomposer, indicating that there is no "predefined" component group. Jones states, "In these examples, the decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows there between. The decomposer may then provide feedback of its decomposition to the DFD creator 106…." EX-1004, 6:15-20; EX-2003, ¶102.

Element 1[f] explains that adding the component group to the first threat model "thereby redefine[s]" the first threat model "by including in it a second threat model associated with the component group." Thus, the component group must have its own "second threat model" before it is added to the first threat model because the claim requires that the addition of the component group is what causes the first threat model to be "redefined." This is supported by the specification of the '008 Patent as well. *See* Section V.A, *supra*; EX-2003, ¶103.

Because Jones does not teach or suggest a "predefined, interrelated" "component group," Jones necessarily does not teach or suggest such a "component group" that has a "second threat model" associated with the

"component group" before the "component group" is added to the first threat model. EX-2003, ¶104.

Jones does not teach or suggest Element 1[f]. EX-2003, ¶105.

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

Element 1[e] from claim 1 of the '008 patent requires "configuring the diagram interface to display a relational diagram" using "visual representations of one or more of the compensating controls." Jones does not teach or suggest a relational diagram using "visual representations of one or more of the compensating controls." Jones Figure 9 does show visual representations of threat model components and threats. But visual representations ***of compensating controls*** are not depicted at all. EX-2003, ¶106.

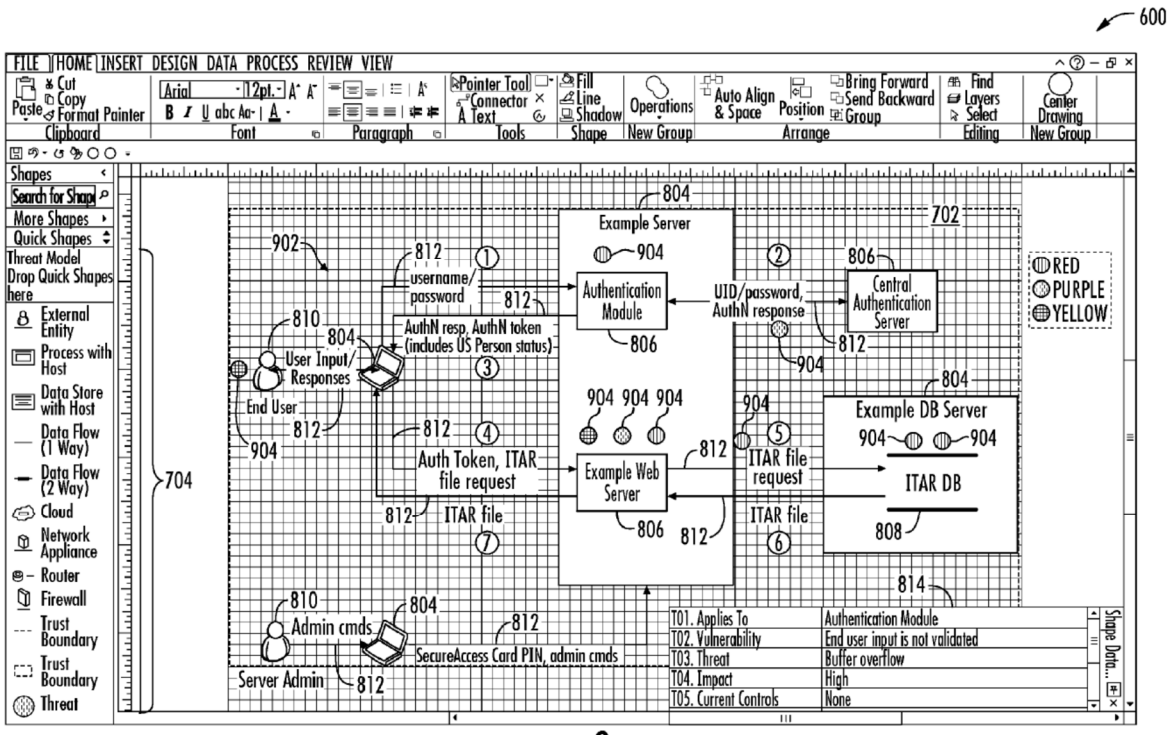


FIG. 9

As support for their assertion that Jones discloses Element 1[e], Petitioner and Mr. Hurlbut cite to Jones' Figures 7-9 and 10B, col. 18:44-19:28, and the analysis for Element 1[d]. Petition, 33; EX-1003, ¶80. Figure 9 is a more complete version of Figures 7 and 8. As shown above, none of those figures disclose visual representations of compensating controls on a relational diagram. Jones states that Figure 10B is a "report" – not a relational diagram. EX-1004, 3:29-30. The paragraphs at Jones' column 18:44-19:28 are the textual descriptions of Figures 7-9. That portion of Jones does not even mention the concept of compensating controls. Finally, Petitioner's and Mr. Hurlbut's reliance on the analysis of Element 1[d] is misplaced. Element 1[d] has nothing to do with

compensating controls or visual representations of compensating controls. Element 1[d] recites a diagram interface displayed on a user computing device communicatively coupled to a database. At deposition, Mr. Hurlbut testified that he was not relying on an inherency argument for Element 1[e]. EX-2002, 30:9-31:21. Thus, there is no argument that Jones inherently discloses a "relational diagram" using "visual representations of one or more compensating controls." EX-2003, ¶107.

Jones does not teach or suggest a "relational diagram" using "visual representations of one or more compensating controls" as required by Element 1[e]. EX-2003, ¶108.

3. Jones Does Not Teach or Suggest Claim 3

Dependent claim 3 recites:

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

with at least one of the additional threats through the one or more databases.

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

Claim 3 (and claim 1 from which claim 3 depends) is a method claim. Claim 3 requires the storing of "additional" threat model components, threats, and compensating controls. Claim 3 further requires that "each additional threat" is associated with "at least one of the additional threat model components." Claim 3 also requires that "each additional compensating control" is associated with "at least one of the additional threats." EX-2003, ¶110.

At deposition, Mr. Hurlbut confirmed that in his analysis the "additional" threats, threat model components, and compensating controls recited in claim 3 were not satisfied by the threats, threat model components, and compensating controls identified in connection with claim 1. EX-2002, 82:17-84:6; EX-2003, ¶111.

None of the portions of Jones cited by Mr. Hurlbut or the Petition disclose the storing of a second set of threats, threat model components, and compensating controls and making associations among those threats, threat model components, and compensating controls, as required by claim 3. Column 4:13-21 of Jones only says that one or more of the functions of its system can be performed manually or automatically. None of Figures 7-10B show a second set of threats, threat model

components, and compensating controls being stored in a database with the claimed associations among themselves. Figure 9 shows multiple threats and components, but there is no teaching or suggestion of storing additional threats, threat model components, and compensating controls as required by claim 3. Similarly, the report shown in Figures 10A and 10B shows multiple threats and mitigations, but there is no teaching or suggestion of storing additional threats, threat model components, and compensating controls and making the associations among themselves recited in claim 3. EX-2003, ¶112.

Jones does not teach or suggest claim 3. EX-2003, ¶113.

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

1. Dependent Claim 2

Claim 2 recites:

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

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

Petitioner and Mr. Hurlbut solely rely on Zheng for the teaching or

suggestion of the elements of claim 2. Petition, 42; EX-1003, ¶87, EX-2002, 85:15-24; EX-2003, ¶115. No other reference is alleged to teach or suggest these claim features.

The Petition lays out the theory of invalidity relied upon by the Petitioner. Thus, the Petition's invalidity theory or theories are what are to be evaluated by the Board in this IPR. *See SAS Institute, Inc. v. Iancu*, 138 S. Ct. 1348, 1358 (2018) ("*The statute* hinges inter partes review on the filing of a petition challenging specific patent claims; *it makes the petition the centerpiece of the proceeding both before and after institution*; and it requires the Board's final written decision to address every claim the petitioner presents for review.") (emphasis added). Thus, the question is whether Zheng (as relied upon in the Petition) teaches or suggests the features of claim 2.

Zheng does not teach or suggest visually displaying attack paths of all threats associated with a threat model component "in response to receiving a user selection of one of the diagrammed threat model components of the first threat model." As the claim language states, a user selects "one" of the threat model components which in turn causes all attack paths of all threats associated with the selected component to be displayed. EX-2003, ¶116.

Zheng does not teach or suggest the selection of any threat model

components much less the selection of "one" threat model component. The central thrust of Zheng is the creation and display of various layers, such as a base layer, a threat modeling layer, security controls layer, a real-time actual threats layer, and a simulated data flow layer. EX-1005, 4:5-12, *see also* 3:35-39. Zheng explains that "[t]hese additional layers 204-210 can overlay the foundational map layer 202, similar to how traffic and other information (in addition to basic cartographical details) is represented on maps." EX-1005, 4:13-16. Zheng further explains that "[t]hese additional layers 204-210 can overlay the base layer 202 in the order as illustrated in FIG. 2 or any other order." EX-1005, 4:16-18. In Zheng, the display of information in various layers is an all or nothing proposition – the entire layer is displayed or the entire layer is not displayed. Zheng neither teaches nor suggests any other option because the layering concept is central to the system in Zheng. EX-2003, ¶117.

Because Zheng either displays an entire layer or not, Zheng teaches that all potential paths from a threat to all potential targets can be displayed. In Figure 8, the threat model layer is represented by threat actor 912, and connections 914, 916, 918, and 920. All threat model connections for all applications 1-5 are shown. There is no user selection of one threat model component for which all associated threat and attack paths are shown. EX-2003, ¶118.

The Petition and Mr. Hurlbut fail to provide an adequate explanation of how and why the teachings of Zheng and Jones can be combined. In Jones' visual diagram, Jones shows threats placed above or in the component with which they are associated. EX-1004, Fig. 9. Figure 9 depicts the threats as circles 904 just above the associated component. In the context of this diagram interface, Jones expressly teaches looking at the attributes of threats *one at a time*. Jones explains that a pop-up window 814 can be displayed to show a diagram shape's attributes. EX-1004, 19:23-25. In Figure 9, window 814 shows that the threat is associated with the "authentication module." The vulnerability is described as "end user is not validated." The specific threat is "buffer overflow." Other attributes of the threat are also displayed. EX-1004, Fig. 9. With this information displayed in window 814, Jones has no need (and in fact does not) display vectors from threat actors to threat targets. EX-2003, ¶119.

As explained above, Zheng on the other hand teaches displaying an entire layer or not displaying the layer at all. To the extent Zheng display attack paths, Zheng displays all attack paths for all threats for all diagram components, or Zheng displays none at all. EX-2003, ¶120.

Petitioner mischaracterizes the teachings of Zheng. For example, Petitioner cites to 5:6-24 of Zheng as teaching a "displayable vector and allowing a user to

"visualize and attack methodology by the threat actor on the threat target." Petition, 42. However, this cited portion merely states that an entire "threat modeling layer," *i.e.*, an entire threat model, can be displayed with threat vectors. The remaining portions of Zheng cited by Petitioner similarly teach the display of threat vectors of an entire "threat modeling layer." Petitioner's expert attempts to overcome this limitation in the disclosure of Zheng by stating that (1) "a singular attack path of a threat may comprise 'all' threats in a system," and (2) "Zheng does not limit itself to identifying less than all threats." EX-1003, ¶87. This is a difficult statement to parse. However, part (1) of this statement appears to assert that a threat model could possibly have only one threat path and thus "all threat paths" in a model could be a single threat path. However, the claim is not directed to selecting a single threat path. The claim expressly recites selecting a single threat model component and displaying multiple attach paths of all threats associated with the selected component. Part (2) of the statement seems to allege that Zheng teaches identifying all threats. But Zheng does not teach selecting a specific component and displaying all attack paths of threats to that specific component.

Jones teaches displaying attributes of a single threat – not even all threats for a particular diagram component. Zheng is on the other end of the spectrum.

Zheng displays all threats for all diagram components. The Petition and Mr. Hurlbut do not attempt to reconcile these divergent teachings. Petitioner and its expert have not explained why a POSITA would discard Jones' teaching to display attributes about a single threat in favor of Zheng's teaching to display all threats for all diagram components in a single layer. Jones' single threat approach is more beneficial than Zheng's approach because Jones allows a user to edit the attribute information for a threat. EX-1004, 19:18-25. Zheng does not offer that feature. In fact, Zheng teaches away from building a threat model based on "manual input." EX-1005, 1:1:24-27. Jones allows a user to delve deeper into a threat model on a threat-by-threat basis. Zheng does not allow that threat-by-threat analysis. A POSITA would have wanted the detailed analysis offered by Jones coupled with the ability to edit the attributes of threat available in the system of Jones in order to allow for a more accurate modeling of threats found in the system being modeled. A POSITA would have found Zheng's all or nothing approach (without the ability to edit threat attributes) to be substantially inferior to Jones' system. Thus, contrary to the Petition and Mr. Hurlbut's analysis, a POSITA would not have combined Zheng's teachings with those of Jones. EX-2003, ¶121.

In the Institution Decision, the Board cites to Keenan (EX-1006) at 17:12-20 as additional support for why it found a reasonable basis to believe the prior art

may render claim 2 obvious. Institution Decision 37. But that portion of Keenan is not relied upon in the Petition to show why claim 2 is allegedly obvious. The question before the Board is whether *the Petition* shows that a claim is invalid. *See SAS Institute*, 138 S. Ct. at 1358 ("*The statute* hinges inter partes review on the filing of a petition challenging specific patent claims; *it makes the petition the centerpiece of the proceeding both before and after institution*; and it requires the Board's final written decision to address every claim the petitioner presents for review.") (emphasis added). The cited portion of Keenan should not be considered with respect to evaluating claim 2. For claim 2, Zheng was the only reference relied upon in the Petition and by Mr. Hurlbut. Petition, 42; EX-1003, ¶87, EX-2002, 85:15-24.

The portion of Keenan cited in the Institution Decision does not teach or suggest "visually display[ing] attack paths of all threat associated with the diagrammed threat model components which compromise the selected threat model component," as recited in claim 2. Instead, Keenan 17:12-20 relates to displaying upstream and downstream data flows or paths for objects. EX-1006, 17:12-20. At most, it teaches toggling display features on and off. EX-2003, ¶122.

2. Independent Claim 4

Independent claim 4 has many claim elements in common with claims 1 and

2. In mapping their invalidity contentions, Petitioner and its expert omitted the paragraph of claim 4 that begins "configuring the diagram interface to display a relational diagram …." Institution Decision, 9 n.1. The omitted paragraph from claim 4 is identical to Element 1[e]. For the reasons Patent Owner provided above, Jones does not teach or suggest Element 1[e]. Jones does not teach or suggest "display[ing] a relational diagram … using … visual representations of one or more of the compensating controls." *See* Section VI.A.2, *supra*; EX-2003, ¶123.

In addition, Element 4[e] in the petition is nearly identical to the substance of claim 2. Thus, for the reasons provided above for claim 2, Jones does not teach or suggest Element 4[e]. *See* Section VI.B.1, *supra*; EX-2003, ¶124.

3. Dependent Claims 6 and 7

Claim 6 recites:

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

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

> 7. The attack simulation method of claim 6, further comprising configuring the diagram interface to, in response to receiving a

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

As explained above in connection with claims 1 and 4, Jones does not teach or suggest the display of "compensating controls" on the relational diagram recited in claim 4. Thus, the "compensating controls" of claims 6 and 7 are not taught or suggested by the cited prior art. *See* Sections VI.A.2 and VI.B.2, *supra*; EX-2003, ¶¶125-127.

Second, none of the cited references teach or suggest "security controls" or "mitigations" that can be set to an on state and cause the system to "toggle all attack paths mitigatable by the first control to a mitigated display state." Petitioner and its expert provide no analysis of this claim requirement whatsoever. Petition, 45-46; EX-1003, ¶¶97-99; EX-2003, ¶128.

Instead, for the teachings of "compensating controls," Petitioner and Mr. Hurlbut cite back to the analysis of Elements 1[c] and 1[c]. But neither of those elements related to "toggle all attack paths mitigatable by the first control to a mitigated display state." EX-2003, ¶129.

For the concept of "attack paths," Petitioner and Mr. Hurlbut cite to Zheng and their analysis for claims 2 and 5. But as explained above in the analysis of claim 2, neither Petitioner nor its expert provided a reasoned analysis how Jones'

analysis on a threat-by-threat basis can be reconciled with Zheng's disclosure of displaying entire layers which would include all threats for all diagram components. *See* Section VI.B.1, *supra*. In fact, a POSITA would not modify Jones to include the so-called "attack path" teachings of Zheng because, as explained above, Jones offers a more robust and flexible system compared to Zheng. EX-2003, ¶130.

4. Dependent Claim 8

Instead of turning off a compensating control as recited in claim 7, claim 8 requires that the compensating control be removed entirely from the relational diagram. EX-2003, ¶131. Specifically, claim 8 recites:

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

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

have to choose what compensating control to add to the relational diagram, select where to add the control, and choose or edit its parameters, if desired. EX-2003, ¶132. Claims having different words are presumed to have different meanings. *See MicroStrategy Inc. v. Business Objects Americas*, 238 F. App'x 605, 609 (Fed. Cir. 2007); *see also CAE Screenplates Inc. v. Heinrich Fiedler GmbH & Co. KG,* 224 F.3d 1308, 1317 (Fed. Cir. 2000) ("In the absence of any evidence to the contrary, we must presume that the use of these different terms in the claims connotes different meanings."); *Applied Med. Res. Corp. v. U.S. Surgical Corp.,* 448 F.3d 1324, 1333 n.3 (Fed. Cir. 2006) ("[T]he use of two terms in a claim requires that they connote different meanings ....").

5. Dependent Claim 9

Dependent claim 9 recites:

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

In relevant part, claim 9 requires "visually display[ing] only attack paths of all threats associated with *a subset of the diagrammed threat model components*." EX-1001, 37:1-6 (emphasis added). Neither Petitioner nor Mr. Hurlbut make any effort to show that the prior art teaches or suggests displaying attack paths of

threats associated with "a subset" of the diagrammed threat model components. Petition, 47, EX-1003, ¶101. Instead, they simply make the conclusory allegation that this element would have been obvious. Petitioner failed to establish that claim 9 would have been obvious. EX-2003, ¶¶133-134.

6. Dependent Claim 10

Dependent claim 10 recites:

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

Again, Petitioner and Mr. Hurlbut make no effort to show that claim 10 would have been obvious. Instead, Petitioner and Mr. Hurlbut argue that because Keenan allegedly discloses modifying or editing a display, it would have been obvious to allow for the modification of individual attacking components and attack paths. Petition, 48, EX-1003, ¶102. But, as explained above in the context of claim 2, Zheng teaches displaying an entire layer or not displaying the layer at all. *See* Section VI.B.1, *supra*. The point of Zheng is to have different layers displaying different aspect of its system. For claim 10, Petitioner is relying on Keenan's ability to modify individual components. That capability is similar to Jones' ability to view the attributes of individual components. But Jones' and

Keenan's ability to view or edit individual components is at the opposite end of the spectrum compared to Zheng which only display layers with no ability to modify or even view individual components. Petitioner provides no explanation of how to reconcile these divergent teachings. In fact, a POSITA would not modify Zheng to allow for the viewing and editing of individual components because that runs contrary to the entire purpose of Zheng, which is to display a threat model in various layers. EX-2003, ¶136.

7. Dependent Claim 11

Dependent claim 11 is substantively the same as Element 1[f] and Petitioner and Mr. Hurlbut do not argue otherwise. Thus, for the reasons provided above with respect to Element 1[f], claim 11 is not obvious. *See* Section VI.A.1, *supra*; EX-2003, ¶137.

8. Independent Claim 12

The elements of independent claim 12 overlap with elements of prior claims. EX-2003, ¶138. Element 12[d] recites:

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

> diagrammed threat model components

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

Petitioner and Mr. Hurlbut assert that "Jones discloses this element." Petition, 49, EX-1003, ¶107. As explained above with respect to Element 1[e], Jones does not teach or suggest the inclusion of "compensating controls" on a diagram that defines a threat model. *See* Section VI.A.2, *supra*; EX-2003, ¶139.

Element 12[e] recites:

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

EX-1001, 37:43-38:3. Element 12[e] is nearly identical as claim 2 and Element 4[e]. Thus, for the reasons provided above for claim 2, Jones does not teach or suggest Element 12[e]. *See* Section VI.B.1, *supra*; EX-2003, ¶140.

9. Dependent Claim 13

Dependent claim 13 is substantively the same as dependent claim 6. Thus, for the reasons provided above for claim 6, claim 13 is not obvious as alleged in the Petition. *See* Section VI.B.3, *supra*; EX-2003, ¶141.

10. Dependent Claim 14

Dependent claim 14 is substantively the same as dependent claim 7. Thus, for the reasons provided above for claim 7, claim 14 is not obvious as alleged in the Petition. *See* Section VI.B.3, *supra*; EX-2003, ¶142.

11. Dependent Claim 15

Dependent claim 15 is substantively the same as dependent claim 8. Thus, for the reasons provided above for claim 8, claim 15 is not obvious as alleged in the Petition. *See* Section VI.B.4, *supra*; EX-2003, ¶143.

12. Dependent Claim 16

Dependent claim 16 is substantively the same as dependent claim 9. Thus, for the reasons provided above for claim 9, claim 16 is not obvious as alleged in the Petition. *See* Section VI.B.5, *supra*; EX-2003, ¶144.

13. Dependent Claim 17

Dependent claim 17 is substantively the same as dependent claim 10. Thus, for the reasons provided above for claim 10, claim 17 is not obvious as alleged in the Petition. *See* Section VI.B.6, *supra*; EX-2003, ¶145.

14. Dependent Claim 19

Dependent claim 19 recites:

> 19. The attack simulation system of claim 18, wherein the diagram interface is further configured to, in response to

> receiving one or more user inputs, diagram a communication protocol between two of the diagrammed threat model components, the diagrammed communication protocol including an alphanumeric indicator.

Claim 19 requires that "a communication protocol" is diagramed in response to one or more user inputs "between two of the diagrammed threat model components, the diagrammed communication protocol including an alphanumeric indicator." Petitioner and Mr. Hurlbut argue that Jones discloses this limitation. Petition, 52, EX-1003, ¶115. Petitioner and Mr. Hurlbut specifically point to Jones' disclosure of "User Input/Responses" between end user 810 and computing device 804 in Jones' Figure 9. They also cite to the disclosure of "Auth N token" and "ITAR file requests" between computing device 804 and the example server(s) 806. Petition, 54, EX-1003, ¶116; EX-2003, ¶¶146-147.

The '008 Patent provides several examples of communication protocols, some of which are depicted in Figure 10. In Figure 10, the communication protocols include HTTPS, TCP, SMB, and WiFi. EX-2003, ¶148.

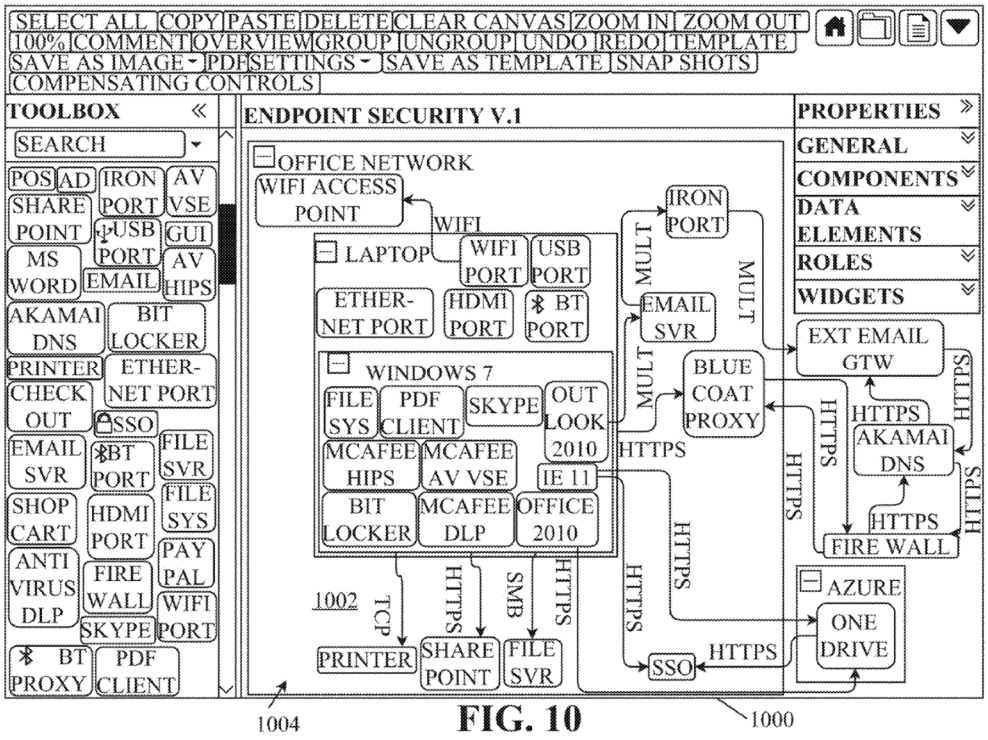


FIG. 10

Contrary to Petitioner's assertion, "User Input/Responses," "Auth N token" and "ITAR file requests" are not communication protocols, they are data. Mr. Hurlbut admitted this distinction at his deposition. Mr. Hurlbut effectively contradicted his declaration and admitted that information such as usernames and passwords were just data and were not communication protocols. EX-2002, 108:9-24; EX-2003, ¶149.

Indeed, Zheng discloses a long list of communication protocols, none of which include the "User Input/Responses," "Auth N token" and "ITAR file requests" relied upon by Petitioner and in Mr. Hurlbut's declaration. EX-1005, 13:60-14:4; EX-2003, ¶150.

The Petition and its cited prior art does not teach or suggest Claim 19. EX-2003, ¶151.

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

The Petition and Mr. Hurlbut do not rely on Yu to remedy all of the deficiencies identified previously with respect to Grounds 1 and 2. Yu is only relied upon as teaching particular aspects of certain of the "compensating controls" and "attack path" limitations. Petition, 57-60, EX-1003, ¶¶122-128. The remaining deficiencies identified with respect to Grounds 1 and 2 remain and show that Petitioner has failed to meet its burden of establishing that claims 1-20 are invalid. EX-2003, ¶152.

Further, the Petition fails to provide sufficient reasons why a POSITA would have combined Yu with the combination of Jones, Zheng, and Keenan. EX-2003, ¶153. Even if Yu relates to the same general technology as that of Jones, Zheng, and Keenan, that does not provide sufficient basis for adding Yu to the combination. Moreover, at best, Keenan relates to risk modeling – not threat modeling. *Id*.

Petitioner and Mr. Hurlbut argue that Yu would add "compensating controls" and "attack paths" to the Jones, Zheng, and Keenan combination. But the claims of the '008 Patent do not simply recite those concepts as claim elements.

"Compensating controls" and "attack paths" are recited in the claims as having specific relationships to other elements of the claims. Even if Yu discloses "compensating controls" and "attack paths," that is not sufficient to establish that all aspects of the claims of the '008 Patent are taught or suggested. EX-2003, ¶154.

The addition of Yu does not render claims 1-20 obvious. EX-2003, ¶155.

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

The Petition and Mr. Hurlbut rely on Reith for allegedly disclosing the so-called "threat model chaining" features of Element 1[f] and claims 11 and 20. Petition, 60, EX-1003, ¶129; EX-2003, ¶156.

The claim phrase "redefine the first threat model by including in it a second threat model associated with the component group" appears in Element 1[f] and dependent claims 11 and 20. This claim language requires that the "component group" is "add[ed]" to the first threat model. This means that the component group could not have been part of the first threat model prior to being added. The claim language also explains that the addition of the component group to the first threat model "thereby redefine[s]" the first threat model "by including in it a second threat model associated with the component group." Reith's Recombinant Threat Models do not teach or suggest any of these claim features. EX-2003, ¶157.

The Petition relies on Reith's Figure 4 and its associated description. Petition, 60-61, EX-1003, ¶129. Figure 4 shows that there is a hierarchy having individual threat models at the bottom level, multiple threat landscapes that include their respective individual threat models at the middle level, and a single threat matrix that includes each of the threat landscapes. Reith states that a Recombinant Threat Model may stand on its own within the threat landscape or multiple Recombinant Threat Models may be interconnected together. EX-1008, 4:32-35. "Interconnected" merely means that the threat models may be connected to each other. There is no teaching or suggestion that a predefined component group having its own threat model is "added" to a first threat model and "thereby redefining" the first threat model, as required by the '008 Patent claims. EX-2003, ¶158.

Moreover, the alleged reasons provided for combining Reith with the other references is entirely based on hindsight and has no evidentiary support. The Petition and Mr. Hurlbut argue that a POSITA would have been motivated to combine Reith with the other references because "Reith saves time when the user is building the threat model because it allows the user to incorporate existing threat models into the new threat model without 'recreating the wheel.'" Petition, 61, EX-1003, ¶131; EX-2003, ¶159.

This "reason" comes straight from the '008 Patent. EX-2003, ¶160. The '008 Patent explains that:

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

EX-1001, 20:26-36. The rest of the reasons why a POSITA would have combined Reith with the other references is simply a recitation of various *KSR* categories for showing that an invention would have been obvious – namely, "would have been within the skillset of a POSIA," "would require no undue experimentation," "an easily predictable result," "reasonable expectation of success," "very predictable technologies," and "would not encounter any insurmountable challenge[s]." Petition, 61-62, EX-1003, ¶132. Petitioner and Mr. Hurlbut provided no evidence supporting these conclusions. EX-2003, ¶160.

Petitioner has not established that claims 1-20 are obvious based on the references of Ground 4. EX-2003, ¶161.

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

Petitioner and Mr. Hurlbut rely on the knowledge of a POSITA to teach the toggling limitations of claims 5-8, and 13-15. Petition, 62, EX-1003, ¶133. This alleged knowledge of a POSITA does not address all of the reasons why Petitioner has not shown why claims 1-20 are invalid as explained above with respect to Grounds 1-4. Toggling is only one aspect of certain claims. EX-2003, ¶162.

The Petition and Mr. Hurlbut make assertions about what a POSITA would have understood about toggling and why a POSITA would have combined the knowledge of a POSITA with the other references. But the Petition provides no evidence supporting any of the assertions of Ground 5 other than citing to Mr. Hurlbut's declaration. Petition, 62-63. But Mr. Hurlbut's declaration fails to cite to any evidence itself. EX-1003, ¶¶133-134; EX-2003, ¶163. According to the Board's Consolidated Trial Practice Guide, expert testimony must be supported by sufficient facts and data and those facts and data must be disclosed otherwise the expert's opinions are entitled to little or no weight. *See* CTPG, 35.

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

any insurmountable challenge[s].” Petition, 62-63, EX-1003, ¶134. Neither Petitioner nor Mr. Hurlbut provided any evidence supporting these conclusions. EX-2003, ¶164.

VII. CONCLUSION

For the reasons discussed above, the challenged claims are not anticipated and/or rendered obvious over the references relied upon in the Petition.

Dated: February 14, 2024

Respectfully submitted,

/s/ Donald L. Jackson
Donald L. Jackson

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(b), (c) and (d), Patent Owner certifies that the word count of Patent Owner's Response (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 11,190 words.

By: */s/ Donald L. Jackson*
Donald L. Jackson

CERTIFICATE OF SERVICE ON PETITION 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 February 14, 2024, a complete and entire copy of this Patent Owner Response, together with all supporting exhibits, were served on Petitioner electronically, by agreement, by emailing a copy of the same to the following attorneys for Petitioner:

brent.yamashita@us.dlapiper.com
blake.jackson@us.dlapiper.com
matthew.middleton@us.dlapiper.com

By: */s/ Donald L. Jackson*
Donald L. Jackson