

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

**PETITIONER'S REPLY
IN SUPPORT OF *INTER PARTES* REVIEW OF
U.S. PATENT NO. 10,699,008**

TABLE OF CONTENTS

	Page
I. INTRODUCTION	1
II. CLAIM CONSTRUCTION	1
A. “Redefine The First Threat Model By Including In It A Second Threat Model Associated With The Component Group,”	1
B. The Applicability Of <i>Ex Parte Schulhauser</i>	4
III. GROUND 1: JONES ANTICIPATES CLAIMS 1 AND 3	5
A. Jones Anticipates Claim 1 By “Adding A Component Group To A First Threat Model” In Element 1[f]	5
B. Jones Discloses A Graphical User Interface Depicting Compensating Controls And Thus Discloses Element 1[e].....	9
C. Jones Anticipates Claim 3	11
IV. GROUND 2: CLAIMS 1-20 ARE OBVIOUS OVER THE COMBINATION OF JONES, ZHENG, AND KEENAN.....	13
A. Dependent Claim 2	13
B. Independent Claim 4	15
C. Dependent Claim 6 And 7	16
D. Dependent Claim 8.....	16
E. Dependent Claim 9.....	17
F. Dependent Claim 10.....	17
G. Dependent Claim 11	17
H. Independent Claim 12	17
I. Dependent Claim 13.....	18
J. Dependent Claim 14.....	18
K. Dependent Claim 15.....	18
L. Dependent Claim 16.....	18
M. Dependent Claim 17	18

N. Dependent Claim 19.....18

V. GROUND 3: OBVIOUSNESS OF CLAIMS 1-20 BASED ON
JONES, ZHENG, KEENAN, AND YU.....19

VI. GROUND 4: OBVIOUSNESS OF CLAIMS 1-20 BASED ON
JONES, ZHENG, KEENAN, YU, AND REITH.....21

VII. GROUND 5: OBVIOUSNESS OF CLAIMS 5-8 AND 13-15 BASED
ON THE REFERENCES OF GROUND 4 AND THE KNOWLEDGE
OF A POSITA 23

VIII. PO HAS SHOWN ZERO EVIDENCE OF BIAS.....24

IX. CONCLUSION.....26

PETITIONER'S EXHIBIT LIST

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
EX-1016	Deposition Transcript of Seth James Nielson, Ph.D.

I. INTRODUCTION

IriusRisk Inc. (“Petitioner”) submits this reply to ThreatModeler Software Inc.’s (“PO”) Patent Owner Response (“POR”) (Paper 18) in support of Petitioner’s Petition for *Inter Partes* Review (“Petition”) (Paper 1). PO’s arguments repeatedly misinterpret Jones and other key references and therefore fail to save the claims from unpatentability. Thus, the Board should find claims 1-20 unpatentable.

II. CLAIM CONSTRUCTION

A. “Redefine The First Threat Model By Including In It A Second Threat Model Associated With The Component Group,”

The Board invited the parties to address the proper construction of the limitation “redefine the first threat model by including in it a second threat model associated with the component group.” Institution Decision, 15-16. The Board further noted that “the parties should focus particularly on defining the full scope of what it means to ‘redefine’ the first threat model and to ‘include’ a second threat model ‘in’ a first threat model.” *Id.*, 16. Petitioner asserts that it is not necessary to construe this limitation because the claims are invalid under any interpretation. However, PO’s construction is overly broad, and Petitioner provides its position below.

This limitation should be construed according to its plain and ordinary meaning. *Johnson Worldwide Associates. Inc. v. Zebco Corp.*, 175 F.3d 985, 989

(Fed. Cir. 1999) (when the patent applicant is not deemed to be his own lexicographer, claim terms are given their “ordinary and accustomed meaning.”). The plain and ordinary meaning of “redefine” is to “modify” or “change” and the plain and ordinary meaning of “including” is “adding.” See POR, 16-17 (providing similar interpretations of “redefine” and “including.”); EX-2002, 27:18-28:12 (redefining “is modifying the first threat model so that now it’s a new threat model.”), 29:6-23. Accordingly, the plain and ordinary meaning of this limitation is “modify or change the first threat model by adding to it a second threat model associated with the component group.”

PO argues 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.” POR, 16-17. PO’s definition is similar to Petitioner’s proposed definition, but PO’s definition adds unnecessary words that go beyond the plain and ordinary meaning of the phrase and imports limitations from other parts of claim 1. For example, the words “predefined interrelated” appears in another part of claim 1. EX-1001, cl. 1. This is improper. See *Robotic Vision Sys., Inc. v. View Eng’g, Inc.*, 189 F.3d 1370, 1376 (Fed. Cir. 1999) (rejecting a construction on the ground that it “would necessarily be redundant and would add no additional limitations.”); *Fortinet, Inc.*

v. Sophos, Inc., 2015 WL 877410, at *13 (N.D. Cal. Feb. 27, 2015) (rejecting proposed construction because “the limitations requested by Fortinet already appear in the relevant claims, and thus its requested construction is redundant.”).

Moreover, the portion of PO’s construction reciting “where the added component group was not a part of the first threat model before being added” adds extraneous words that improperly change the meaning of the claim terms beyond their plain and ordinary meaning. PO argues that this addition is proper because limitation 1[f] must be interpreted such that “the component group could not have been part of the first threat model prior to being added” (POR, 24), but this is not supported by the claims or specification. The claims do not exclude a situation where the component group added to the first threat model already exists in that first threat model. There is no requirement in the claim that the component group be a “new” component group. A first threat model may still be modified or “redefined” if a second threat model is added to it, even if that second threat model already exists in the first threat model. In this scenario, the first threat model has still been modified because it now includes a duplicate set of components when it did not previously. There may or may not be good reasons to add a duplicate component group to a first threat model, but the claims broadly allow for such a situation regardless.

Thus, the plain and ordinary meaning of the limitation “redefine the first threat model by including in it a second threat model associated with the component group” is “modify or change the first threat model by adding to it a second threat model associated with the component group.”

But, even if the Board agrees with PO's construction, this limitation is met under either parties' construction as explained below. Section III.A.

B. The Applicability Of *Ex Parte Schulhauser*

The Board also invited the parties to discuss the applicability of *Ex parte Schulhauser*, No. 2013-007847, 2016 WL 6277792 (PTAB Apr. 28, 2016) (precedential). Specifically, the Board identified the limitation “configuring the diagram interface to, in response to receiving one or more user inputs, add a component group to the first threat model” as one exemplary limitation where *Schulhauser* may be applicable. Petitioner understands the Board to be suggesting that the “user input” is conditional such that the step is performed only if the “user input” is received. Such a construction would similarly apply to any limitation requiring a user action (“user input,” “user selection,” or “user toggle”) rendering those limitations not limiting, including Elements 1[f], 4[e], 12[b], 12[d] and dependent claims 3, 5-11, 13-17, 19-20.

For the purposes of this IPR, Petitioner asserts that it is not necessary for the Board to decide whether *Ex parte Schulhauser* applies to the claims of the '008

patent because the claims are invalid regardless of whether *Ex parte Schulhauser* applies.

III. GROUND 1: JONES ANTICIPATES CLAIMS 1 AND 3

A. Jones Anticipates Claim 1 By “Adding A Component Group To A First Threat Model” In Element 1[f]

As explained in the Petition, Jones discloses limitation 1[f] by describing that its 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.” Petition, 35-36 (quoting Ex. 1004, 6:12-34; citing Ex. 1003 ¶¶ 81-84). In other words, Jones “modifies” (*i.e.*, “redefines”) a “first threat model” (level n) by adding to it (*i.e.*, “including” in it) cybersecurity threats (*e.g.*, via metadata) associated with nested components (*i.e.*, “a second threat model”), to produce the “modified” (*i.e.*, “redefined”) “first threat model” (level n+1).

PO argues that limitation 1[f] must be interpreted such that “the component group could not have been part of the first threat model prior to being added.” POR, 24. Preliminarily, as discussed in Section II.A., the claims do not exclude a situation where the component group added to the first threat model already exists in that first threat model. There may or may not be good reasons to add an existing component group to a first threat model, but the claims broadly allow for such a situation regardless.

But, even accepting PO's construction that "the component group could not have been part of the first threat model prior to being added," Jones meets this limitation. PO argues that "[a]dding 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." POR, 26. PO essentially argues that, since components are predefined in the information system, the components cannot be "added." But PO's argument conflates Jones' information system and threat model DFD—the components are predefined in the information system and then "added" to the threat model DFD. See EX-1004, 5:45-6:34.

Jones' system in fact discloses creating a new threat model DFD from the information system and then modifying that threat model DFD with the nested components associated with a decomposed component, creating an $n+1$ threat model. See *id.* In other words, the nested components associated with the decomposed component are predefined in the information system, but not yet modeled in the threat model DFD. PO's expert agrees. EX-1016, 53:7-11 (Jones discloses "the creation of a new DFD"), 59:2-9 ("Q So the group of decomposed components exist in the information system but they're not yet modeled in the threat modeled DFD? A Correct."). Thus, the nested components are predefined in the information system and "added" to the first threat model DFD, thereby

redefining the first threat model by including in it a second threat model, and PO's argument fails.

This is confirmed by a close examination of Jones' specification. Jones discloses a "DFD creator 106" that identifies and composes "a DFD for the information system." EX-1004, 5:45-63. Jones' "threat indicator 108" identifies "a cybersecurity threat to a particular element of the elements of the information system" and adds "a secondary note representing the cybersecurity threat to the DFD to thereby produce a threat model DFD for the information system." EX-1004, 5:64-6:11. Jones then discloses modifying the first "threat" model from a level "n" model to a level "n+1" model by including therein nested components and threats associated with a particular layer of components (nested components). EX-1004, 6:12-34. Jones states:

[T]he decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows therebetween. The decomposer may then provide feedback of its decomposition to the DFD creator 106, which may modify the threat-model DFD for the decomposed components to include their nested components and data flows (and appropriate metadata), thereby producing a level n+1 threat-model DFD.

Id. And, as with the components of the threat model DFD, Jones' threat indicator may "identify any cybersecurity threats to elements (nested components and data flows) of the decomposed components, and add appropriate secondary nodes (and appropriate metadata) representing those threats." *Id.*, 6:23-28. Thus, Jones discloses Element 1[f].

Dr. Nielson's testimony further confirms, contrary to ThreatModeler's argument (POR, 27-29), that the nested components in Jones' system are predefined. Dr. Nielson testified that the nested components for a decomposed component "already exist" in the information system.¹ EX-1016, 59:2-5 ("Q So the group of decomposed components already exist in the information system before the decomposition begins? A Yes."). These decomposed components are a group of components related to the decomposed component. *See id.*, 58:11-19. This is confirmed in Jones' specification, where it states that a component is decomposed "***into its nested components and data flows therebetween***"—i.e., a predefined group of components related to one another via the decomposed component. EX-1004, 6:15-18; *see also id.*, 6:23-28 (discussing threat indicator), 14:1-18, 16:51-62.

¹ Notably, PO's argument that the nested components in Jones "already exist" in the information system but are also not "predefined" appears contradictory. EX-2003, ¶102 ("Jones describes the decomposer as doing analysis when ***decomposing existing components***.").

B. Jones Discloses A Graphical User Interface Depicting Compensating Controls And Thus Discloses Element 1[e]

Element 1[e] requires “configuring the diagram interface to display a relational diagram” using “visual representations of one or more of the compensating controls.” As discussed in the Petition, Jones discloses an interface that displays a relational diagram (DFDs), the relational diagram defining a threat model. Petition, 33 (citing EX-1004, 3:25-28); *see also* EX-1003, ¶80. Jones’ Fig. 9, shown below, depicts “an example graphical user interface in which a DFD, threat-model DFD and their metadata may be composed.” EX-1004, 3:25-28.

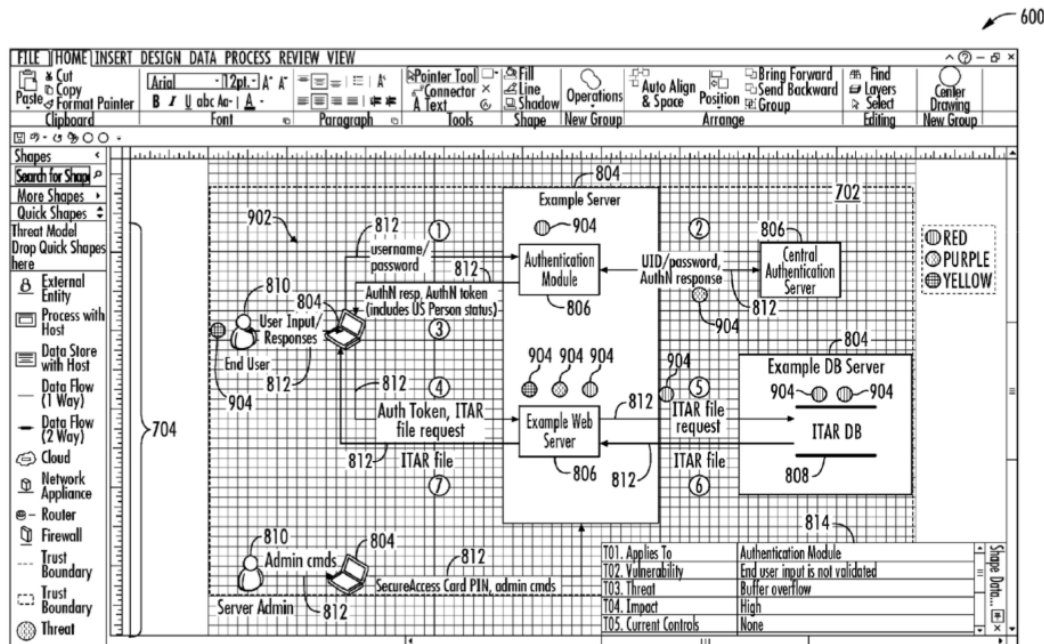


FIG. 9

PO admits that “Jones Figure 9 does show visual representations of threat model components and threats.” POR, 29. PO also does not dispute that Jones discloses “compensating controls” (EX-1016, 64:7-18 (“I do not have any analysis

about whether or not there is a database with compensating controls in Jones.”)), but instead argues that Fig. 9 does not show “visual representations of compensating controls” (POR, 29). But PO misses that Jones depicts compensating controls in a rectangular box in the bottom right corner under the label “Current Controls.” See Petition, 34 (depicting a zoomed in version of the detail in Fig. 9 and specifically calling out label 814).

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

Again, PO does not dispute that Jones discloses compensating controls. EX-1016, 64:7-18. And there is no dispute that the “current controls” in Jones are compensating controls. *See id.*; *see also id.*, 34:6-22 (“an example of a compensating control would be [] a mitigation for a potential threat.”); EX-1004, (“current security controls designed to mitigate the cybersecurity threat.”); EX-1004, 14:1-18. As shown in Fig. 9, this rectangular box is on the relational diagram. Thus, Fig. 9 shows a relational diagram using “visual representations of one or more of the compensating controls.”

Notably, PO’s argument is based on a not proffered construction of “visual representations,” where the rectangular box is somehow not a “visual

representation.” Element 1[e] does not require that the “visual representation” be a particular shape or in a particular place on the relational diagram. Thus, the claims do not exclude a rectangular box on the relational diagram from being a “visual representation.” Jones further discloses that each attribute listed in the rectangular box may be represented on the relational diagram as a secondary node. EX-1004, 19:10-28 (“attributes and even further attributes of the cybersecurity threats may be entered for their shapes. ... *the window 814 may be recalled for each of the shapes*, in which data for a shape and thus attributes of a cybersecurity threat may be entered, and thereby included as structured information in metadata associated with the shape (and thus secondary node)).” As such, Jones’ attributes, including the security controls, may be represented as shapes on a diagram. Thus, Jones discloses using “visual representations of one or more of the compensating controls” as required by Element 1[e].

C. Jones Anticipates Claim 3

Claim 3 requires the storing of “additional” threat model components, threats, and compensating controls and 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.” POR, 32; EX-2003, ¶110. Each of these steps is performed in claim 1, and claim 3 merely requires these steps be performed an

“additional” time. *See* Elements 1[b] (storing and associating threats and threat modeling components), 1[c] (storing and associating compensating controls).

PO provides a conclusory argument that “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” (POR, 31-33), but it is simply not credible to suggest that Jones cannot perform the steps of claim 1 an “additional” time. Jones system is not limited to a specific number of threats, threat model components, or compensating controls, or associations between them. Indeed, PO admits that Jones Figs. 9 discloses “multiple threats and components” and Figs. 10A-10B disclose “multiple threats and mitigations.” PO’s argument appears to be that Jones is somehow limited to only those “multiple threats and components” without the ability to more, which is simply not credible. *See also*, *e.g.*, EX-1004, 6:15-17 (“the decomposer **110** may be configured to decompose ***one or more components*** of the information system modeled by the DFD”), 6:31-34 (“This decomposition and follow-on ***modeling of the information system’s components and threats may continue until a desired level of the information system is achieved.***”).

Dr. Nielson further confirmed at his deposition that Fig. 9 in Jones includes stencil 704 that includes predefined components and threats that a user can drag and drop into the GUI, thus adding additional threats and threat model components

and the associations therebetween. EX-1016, 50:21-52:11. Controls and other “attributes of a cybersecurity threat may be entered, and thereby included as structured information in metadata associated with the shape (and thus secondary node).” EX-1004, 19:10-28. In other words, controls (*i.e.*, compensating controls) may be entered on the diagram (without limitation), thus adding additional compensating controls.

Thus, as discussed in the Petition, a POSITA would have understood from Jones' disclosure that Jones discloses the steps of claim 1, and that each of these steps could be performed an “additional” time. Petition, 40-41 (citing EX-1004, Fig. 9); EX-1003, ¶85.

IV. GROUND 2: CLAIMS 1-20 ARE OBVIOUS OVER THE COMBINATION OF JONES, ZHENG, AND KEENAN

A. Dependent Claim 2

PO admits that “Zheng teaches that all potential paths from a threat to all potential targets can be displayed” (POR, 35), but merely argues that “[b]ecause Zheng either displays an entire layer or not, ... [t]here is no user selection of one threat model components for which all associated threat and attack paths are shown.” POR, 35. In other words, PO acknowledges that all aspects of dependent claim 2 are met, except for the user selection of one component to display the threat and attack paths because the only option in Zheng is to display an entire layer. *Id.*

But PO ignores Zheng's disclosure. Zheng discloses that "[a] user can interact with the resulting visualization (step 820) to achieve the desired display effects." EX-1005, 11:41-42. Indeed, Zheng's layers, including the threat modeling layer, "has sub-categories in the layer that can be toggled (e.g., enabled or disabled) by the user." *Id.*, 11:41-46. For example, "a particular type of threats in the threat modeling layer 204 can be toggled on or off to provide more focused visualization." *Id.*, 11:46-49. Thus, contrary to PO's argument that all attack paths in Zheng must be displayed, a user can display any portion of any layer as desired to provide a more focused visualization. A user could, for example, toggle off all threats except those for a specific component and thus display all attack paths for that specific component.

PO's remaining arguments appear to be based on PO's mischaracterization that an entire layer must be displayed in Zheng. PO argues that the Petition fails to provide an adequate explanation of how and why Zheng and Jones can be combined because Jones looks at attributes "one at a time," while Zheng must display all attack paths. POR, 36-38. This argument mischaracterizes both Zheng and Jones. As discussed above, a user can select or toggle specific aspects of Zheng's layers to display specific attack paths "to provide a more focused visualization." EX-1005, 11:41-55. And Jones' Fig. 9 shows a GUI displaying threats as secondary nodes with the numeric label 904, showing that Jones' threats

may be viewed all at once, or individually in detail, such as in the rectangular box in the bottom right corner of Fig. 9. EX-1004, 19:14-17 (“cybersecurity threats (or rather their shapes) are placed in the workspace 702.”), Fig. 9 (showing threats represented as secondary nodes 904).

Moreover, PO’s conclusory assertion that Jones has “no need (and in fact does not) display vectors from threat actors to threat actors” is a criticism of a specific reference on obviousness, which is improper. Jones’ system could easily incorporate Zheng’s displayable vectors from threat actors to threats displayed on the GUI. *See also* Petition, Section X.C.19. Jones’ threats are already displayed as secondary nodes 904. A vector between the threat and the threat actor would add additional information for the user to view.

B. Independent Claim 4

Preliminary, Petitioner unintentionally omitted the “configuring the diagram interface to display a relational diagram” from the Petition. But as the Board noted and PO agrees, the omitted limitation is identical to Element 1[e]. POR, 40; Institution Decision, 9 n.1. Thus, Jones meets this limitation in claim 4 for the reasons described in Element 1[e].

PO’s challenge to claim 4 is entirely dependent on PO’s arguments above related to Element 1[e] regarding “display[ing] a relational diagram ... using ...

visual representations of one or more of the compensating controls” and claim 2.

Thus, for the reasons above, PO's arguments fail.

C. Dependent Claim 6 And 7

PO's challenges to dependent claims 6 and 7 appear to primarily relate back to PO's arguments for claims 1 and 4 and thus fail for the same reasons above. POR, 40-42. PO also provides the conclusory assertion that “none of the cited references teach” the limitation “toggle all attack paths mitigatable by the first control to a mitigated display state.” POR, 41. Petitioner cited Keenan's ability to toggle various aspects of its system in combination with the disclosures of Zheng and Jones. Petition, 45-46. PO does not cite to Keenan at all or explain how Keenan does not meet this limitation in combination with Zheng and Jones.

D. Dependent Claim 8

The Petition argued that claims 6 and 7 are identical to claim 8 “*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.’” Petition, 47. As explained in the Petition, 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. In other words, the

Petition argued that a POSITA would have found it obvious to simply remove a control instead of using a user toggle. Contrary to PO's argument, removing a control is effectively the same as toggling it off, and a user can easily re-add a removed control.

E. Dependent Claim 9

PO misunderstands the Petition's arguments. Contrary to PO's argument, the fact that a user may toggle off "all features except for the attack paths" of specific components (Petition, 47) shows that the combination in ground 2 may visually display the attack paths for a "subset" of the diagrammed components. In other words, since a user may toggle any aspect of the system, the user may select a "subset" of components.

F. Dependent Claim 10

PO's challenge to claim 10 relies on PO's misapprehension that Zheng only discloses displaying entire layer(s). POR, 44-45. This is wrong for the reasons stated above. Section IV.B.

G. Dependent Claim 11

PO's challenge to claim 11 relies on PO's challenge to Element 1[f]. Thus, PO is wrong for the reasons above. Section III.A.

H. Independent Claim 12

PO's challenge to claim 12 relies on PO's challenge to Element 1[e] and claim 2. Thus, PO is wrong for the reasons above. Sections III.B, IV.A.

I. Dependent Claim 13

PO's challenge to claim 13 relies on PO's challenge to claim 6. Thus, PO is wrong for the reasons above. Section IV.C.

J. Dependent Claim 14

PO's challenge to claim 14 relies on PO's challenge to claim 7. Thus, PO is wrong for the reasons above. Section IV.C.

K. Dependent Claim 15

PO's challenge to claim 15 relies on PO's challenge to claim 8. Thus, PO is wrong for the reasons above. Section IV.D.

L. Dependent Claim 16

PO's challenge to claim 16 relies on PO's challenge to claim 9. Thus, PO is wrong for the reasons above. Section IV.E.

M. Dependent Claim 17

PO's challenge to claim 17 relies on PO's challenge to claim 10. Thus, PO is wrong for the reasons above. Section IV.F.

N. Dependent Claim 19

Jones discloses claim 19 for the reasons stated in the Petition. Mr. Hurlbut's deposition testimony does not contradict his declaration. Mr. Hurlbut testified at his deposition that a communication protocol is "a way of communicating from one point to another." EX-2002, 105:13-106:7. Mr. Hurlbut further testified a "user name and password" is not a communication protocol, but that they are

“transmitted using a communication protocol.” *Id.*, 108:13-24. This is correct.

The user name and password is the data being transferred, and one communication protocol (*i.e.*, the method of communicating) is the user input or responses—which is exactly what Mr. Hurlbut testified is the communication protocol. EX-1003, ¶116 (“the communication protocol between the end user 810 and the computing device 804 is ‘User Input/Responses.’”). Jones Fig. 9 diagrams the “User Input / Responses” and then shows an arrow 812 labeled “username / password” showing the transfer of the user name and password data via the “User Input / Responses.” EX-1004, Fig. 9. Moreover, even to the extent Jones’ alphanumeric indicators are data, a POSITA would understand that Jones’ alphanumeric indicators are representations of communication protocols because such data is transferred by a communication protocol. EX-2002, 108:13-24.

V. GROUND 3: OBVIOUSNESS OF CLAIMS 1-20 BASED ON JONES, ZHENG, KEENAN, AND YU

As explained in the Petition, 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. Petition, 57-58; EX-1003, ¶¶122-24. Thus, to the extent the Board disagrees that Jones

discloses “visual representations of one or more of the compensating controls” in claims 1 and 12 (see Sections III.B, IV.H.), Yu discloses this limitation. See Petition 57-58 (citing, *e.g.*, EX-1006, 15:9-28 (“[i]n one aspect, the graphical user interface may include one or more categories associated with each of the one or more controls.”)).²

PO includes no analysis that Yu does not meet the claimed limitations. Instead, PO provides nothing more than a conclusory argument regarding the Petition's motivation to combine. POR, 50. Without any analysis, PO argues that the fact that Yu is the “same general field” of technology is insufficient to show a motivation. POR, 50. Petitioner disagrees, but, in any event, the Petition includes a detailed analysis of multiple reasons why a POSITA would have been motivated to add Yu. See Petition, 58-59 (“a POSITA would have been motivated specifically to add the ‘compensating controls’ feature ... 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.”) (citing EX-1015, 1-4; EX-1003, ¶127). PO also argues that Keenan discloses risk modeling only, but this is wrong, and, in any event, Petitioner relies

² Additionally, 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. Petition, 58.

on Keenan's disclosure of toggling features in a GUI—not Keenan's disclosure of threats or risks.³

PO also includes a second conclusory argument that Yu's disclosure is insufficient because "compensating controls" and "attack paths" have "specific relationships to other elements of the claims," but that is the extent of PO's analysis. This is a simple combination. For example, PO does not dispute that Jones already discloses compensating controls and instead only disputes whether Jones visually represents the compensating controls on the relational diagram. This combination merely requires, following Yu, modifying Jones to place the compensating controls that already exist in Jones on the relational diagram.

VI. GROUND 4: OBVIOUSNESS OF CLAIMS 1-20 BASED ON JONES, ZHENG, KEENAN, YU, AND REITH

To the extent the Board disagrees that Jones discloses Element 1[e], 11, and 20 (see Section III.A.), Reith discloses these elements. Reith discloses that a Recombinant Threat Model (1) "***may stand on its own within the threat landscape***"; or (2) "multiple Recombinant Threat Models may be interconnected together." EX-1008, 4:30-44. PO criticizes the second point regarding the "interconnected" language, but notably wholly ignores Reith's alternative disclosure that the Recombinant Threat Model "may stand on its own." POR, 51-

³ Additionally, Keenan is only used for claims 5-10 and 13-17, so a motivation to combine Keenan is not required for claims 1-5, 11-12, or 18-20.

52. In other words, instead of being interconnected multiple threat models can be combined into a single threat model that “stand[s] on its own.”

PO also criticizes the Petition's motivation to combine, arguing that the motivation is only hindsight because the Petition's motivation to “save time” using Reith's method comes from the '008 patent. But Reith itself also mentions the benefits of its threat model chaining “Recombinant Threat Models.” For example, Reith criticizes the prior art: “in practice, Threat Matrices often only use as input internally developed Threat Models. All too often, Threat Matrices are not updated with events on other installations not under the responsibility of the Corporate Security Officer. This is often a result not only of not having access to third party data, but also of prior art techniques already being time intensive to develop an attack tree from internal data alone.” EX-1008, 3:50-59. Thus, the '008 patent did not invent “saving time” using threat model chaining—such disclosure already existed in Reith. Moreover, a POSITA viewing Reith would readily appreciate the ability to “save time” by reusing threat models instead of making them from scratch. EX-1003, ¶131. As such, a POSITA viewing Reith would have been motivated to combine Reith's Recombinant Threat Models with the disclosures of Jones, Zheng, Keenan, and Yu.

VII. GROUND 5: OBVIOUSNESS OF CLAIMS 5-8 AND 13-15 BASED ON THE REFERENCES OF GROUND 4 AND THE KNOWLEDGE OF A POSITA

To the extent the Board disagrees that claims 5-8 and 13-15 are met by the cited references, Mr. Hurlbut provides a reasoned analysis demonstrating “[i]n 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.” Petition, 62; EX-1003, ¶133. PO criticizes Mr. Hurlbut’s analysis as not citing to supporting evidence, but Mr. Hurlbut’s analyses and opinions are supported by his substantial background and experience in threat modeling. EX-1003, ¶¶5-17. Notably PO and its expert Dr. Nielson provide no reasoning or evidence to rebut Mr. Hurlbut’s assertions. EX-2003, ¶¶163-64.

PO and Dr. Nielson also criticizes the motivation to combine as a recitation of *KSR* reasons,⁴ but the Petition explains that “[c]omputer-based threat modeling and graphical user interfaces involve very predictable technologies, and a POSITA would not encounter any insurmountable challenge[s] in implementing this combination.” Petition, 62-63 (citing EX-1003, ¶134). Again, this is supported by

⁴ Dr. Nielson criticizes Petitioner’s motivations to combine as “a recitation of various *KSR* categories” in paragraphs 160 and 164. But Dr. Nielson’s declaration and legal understandings section (paragraphs 31-51) does not indicate that Dr. Nielson understood what “*KSR* categories” actually are.

Mr. Hurlbut's vast experience in threat modeling, and PO cites no evidence or reasoning to the contrary.

VIII. PO HAS SHOWN ZERO EVIDENCE OF BIAS

PO is incorrect that Mr. Hurlbut's testimony is "tainted by bias." POR, 27 n.4. Mr. Hurlbut was forthcoming, objective, and truthful throughout his declaration and deposition. *See generally* EX-2002. Moreover, the fact that Mr. Hurlbut personally knows individuals at IriusRisk is not surprising—Mr. Hurlbut regularly attends and speaks at threat modeling conferences that IriusRisk also attends. EX-2002, 10:10-11:4 (Mr. Hurlbut met IriusRisk's CEO at "[c]onfernces that he has spoken at, or I have attended and he has spoken at, or just conferences that we just happen to be at the same place."). Indeed, Mr. Hurlbut also has "personal and professional connections" to ThreatModeler: Mr. Hurlbut personally knows Mr. Agarwal, ThreatModeler's CEO and inventor of the '008 patent.

Additionally, threat modeling represents only a small part of Aquia's business. EX-2002, 14:9-14 (Aquia has one threat modeling client), 13:7-23 (Aquia is "primarily focused" on cybersecurity in the public sector), 15:16-18 (Aquia and its attorneys "did not foresee or perceive any conflict of interest" in Mr. Hurlbut taking on this IPR matter).

Last, PO quotes Mr. Hurlbut's testimony out of context and misleadingly implies that Mr. Hurlbut testified that he is seeking to "help" IriusRisk. This is not

what Mr. Hurlbut testified at all. To the contrary, Mr. Hurlbut repeatedly testified that he was interested in working on this IPR to see how he can apply his objective understanding and expertise:

Q. Why were you interested in working on these IPRs

A. Based on my expertise. I know threat modeling. ... [M]y interest is threat modeling.

Q. But, in particular, in these IPRs, where as a general matter, you are opining that the patent claims are not valid, what was your reason for being interested in taking those positions?

MR. MIDDLETON: Objection. Form.⁵

A. Again, I was interested in trying to understand a little bit more about the scenarios and their particular issues there and so that was part of that as well.

I also am familiar with threat modeling tools in general, and so, again, interested in learning and how I could contribute. How I could help based on my own understanding and experiences.

EX-2002, 18:2-22.

⁵ PO's question lacked foundation because it presumed, without evidence or testimony, that Mr. Hurlbut was "interested in taking" certain positions.

IX. CONCLUSION

Petitioner has shown that claims 1-20 are unpatentable and thus requests cancellation of these claims.

Respectfully submitted,

Dated: May 1, 2024

/Matthew Middleton/
Matthew Middleton

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(c) and (d), Petitioner certifies that the word count of Petitioner's Reply in Support of its Petition for *Inter Partes* Review (exclusive of any table of contents, table of authorities, certificates of service and word count, and list of exhibits or claim listing) as measured by Microsoft Word is 5,436 words.

By: /Matthew Middleton/
Matthew Middleton

**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 May 1, 2024, a complete and entire copy of this Reply in Support of its 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:

djackson@dbjg.com
Donald.jackston@rimonlaw.com
mkaufman@reedsmith.com
marc.kaufman@rimonlaw.com

By: /Matthew Middleton/
Matthew Middleton