

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'S PRELIMINARY RESPONSE

TABLE OF CONTENTS

I.	THE ‘008 PATENT DISCLOSES AND CLAIMS THREAT MODELING METHODS AND SYSTEMS NOT DISCLOSED OR SUGGESTED BY THE ASSERTED ART	1
A.	The ‘008 Patent Discloses and Claims Adding a Second Threat Model into a First Model and Redefining the First Threat Model.....	2
B.	The ‘008 Patent Also Discloses and Claims Displaying All Attack Vectors Affecting a Selected Component	5
C.	Summary of the Petition’s Challenges	8
II.	THE BOARD NEED NOT REACH ANY CLAIM CONSTRUCTION ISSUES TO DENY THE PETITION.....	11
III.	PETITIONER’S CHALLENGES FAIL ON THE MERITS	11
A.	Jones Fails to Disclose at least Element 1[f] of Claim 1 and Fails to Anticipate Claims 1 and 3	12
B.	Ground 2 Also Fails	17
i.	Claims 2, 11, and 20 Survive Ground 2 For Reasons Already Explained for Element 1[f].....	18
ii.	Dependent Claim 2 is also Independently Patentable Over the References of Ground 2	18
iii.	Independent Claims 4 and 12, and Their Respective Dependent Claims, Also Survive Ground 2.....	20
C.	Ground 3 Also Fails	20
D.	Ground 4 Also Fails Because Reith Fails to Remedy Jones’s Shortcomings for Element 1[f].....	21
E.	Ground 5 Also Fails	23
IV.	CONCLUSION.....	23

TABLE OF AUTHORITIES

Cases

<i>Samsung Elec. Co., Ltd. v. Rightquestion, LLC</i> , IPR2022-00251, Paper 17 (PTAB June 9, 2022)	16
<i>Verdegaal Bros., Inc. v. Union Oil Co. of Cal.</i> , 814 F.2d 628 (Fed. Cir. 1987)	17

Rules

37 C.F.R. § 42.107	1
37 C.F.R. § 42.120(a).....	1
37 C.F.R. § 42.65(a).....	16

Pursuant to 37 C.F.R. § 42.107, Patent Owner ThreatModeler Software Inc. (“TMS” or “Patent Owner”) files this preliminary response to the Petition, setting forth reasons why the Petition for *inter partes* review (“IPR”) of claims 1-20 of U.S. Patent No. 10,699,008 (the “’008 Patent”), as requested by IriusRisk, Inc. (“Petitioner”), should be denied.¹

I. THE ‘008 PATENT DISCLOSES AND CLAIMS THREAT MODELING METHODS AND SYSTEMS NOT DISCLOSED OR SUGGESTED BY THE ASSERTED ART

The ’008 Patent is entitled, “Threat Model Chaining and Attack Simulation Systems and Related Methods,” and relates to threat modeling technology. “Threat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized.” ’008 Pat., 1:48-49. As examples, the ’008 Patent explains that threat modeling “could include modeling the possible threats to commuting to work safely, modeling the possible threats to preventing the spread of an infectious disease, or modeling the possible attacks on a computer network (cybersecurity).” ’008 Pat., 8:41-45. A threat model can be used to generate a “threat report” that can identify “threats, the status of identified threats (threat status), and the source(s) of identified threats, among other things.” ’008 Pat., 8:46-49. Exemplary threats disclosed in the ’008 Patent include specific dangers

¹ By submitting this Preliminary Response, no waiver of any argument is intended by Patent Owner. Patent Owner will have a right to file a complete response to the Petition, should the Board institute *inter partes* review. 37 C.F.R. § 42.120(a).

or vulnerabilities such as “Bluejacking” where a modeled system includes a Bluetooth port, and “freeway collision” where the modeled process is “commuting to work.” ’008 Pat., 9:28-9:61. 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.” ’008 Pat., 24:42-52.

A. The ’008 Patent Discloses and Claims Adding a Second Threat Model into a First Model and Redefining the First Threat Model

The ’008 Patent discloses a novel threatmodeling software system and process that can add a second threat model having a group of components into a first threat model, and redefine the first threat model to include the second threat model. This allows a user to modify a threat model by incorporating one or more previously-defined threat models, which the ’008 Patent describes as “threat model chaining.” ’008 Pat., 20:30-36. In an exemplary embodiment, the ’008 Patent describes an “overall threat model A” that includes “components B, C, and D.” ’008 Pat., 24:17-18. Of these components B, C, and D, “component C could be a previously modeled group of components having its own threat model.” ’008 Pat., 24:19-21. The “component D could be a previously modeled group of components having its own threat model that also includes therein a nested threat model for a component group E.” ’008 Pat., 24:21-24. In this manner, “threat model A would

include all threat models associated with components and component groups B, C, D, and E, including all nest threat models.” ’008 Pat., 24:24-27.

Claims 1, 11, and 20 recite features related to this disclosed aspect of the ’008 Patent. Claim 1 is reproduced below:

1. A threat model chaining method, comprising:
providing one or more databases, the one or more databases
comprising:
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;
providing one or more interfaces, including a diagram interface,
configured to be displayed on one or more end user computing
devices communicatively coupled with the one or more
databases;
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 user inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.

'008 Pat., 35:36-63. Dependent claims 11 and 20 recite features substantially similar to the final “configuring” element of claim 1. To illustrate these similarities, claim 20 is reproduced below in annotated form, with italics added to identify the claim language that is identical to language in the final “configuring” element of claim 1:

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

'008 Pat., 38:39-46 (emphasis added). These claimed features are addressed prominently in Grounds 1 and 4 of the Petition. These Grounds, and their deficiencies, are introduced in Section I.C below.

B. The '008 Patent Also Discloses and Claims Displaying All Attack Vectors Affecting a Selected Component

The '008 Patent also discloses a novel threatmodeling software system and process that can display “relevant threat attack paths” for a threat model component upon receiving a user selection of that threat model component. '008 Pat., 23:38-42. As the '008 Patent recognizes, “each asset could have any number of threats to compromise it. Accordingly, the system identifies all threats which may compromise the asset in order to visually diagram attack vectors for the user.” '008 Pat., 24:4-7. In an exemplary illustration, the '008 Patent's FIG. 18 “shows components A-G. Component A has been selected as an asset, and the attack vectors of all threats threatening the asset (component A) are diagrammed using arrows.” '008 Pat., 25:35-38.² FIG. 18 is reproduced below:

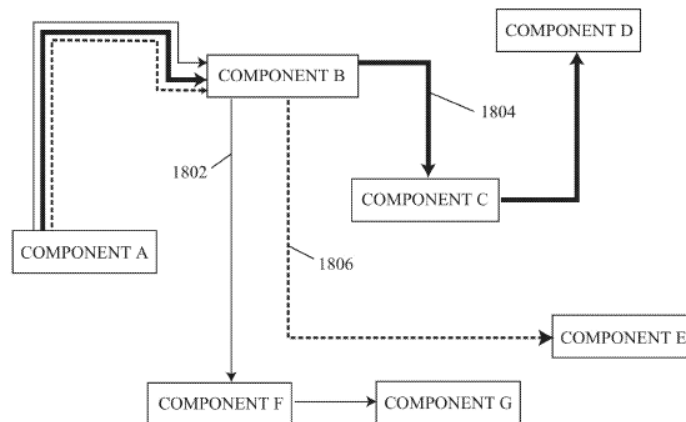


FIG. 18

² The '008 Patent disclose that in FIG. 18, the “arrows are also shown pointing away from the asset, but in other implementations this may be reversed so that arrows point towards the asset from the underlying threats.” '008 Pat., 25:41-43.

In this illustration, “a threat emanating from component G threatens to compromise component A (or the asset within or associated with component A), [as shown by] the attack vector 1802 passing through component F and component B to reach component A.” ’008 Pat., 25:44-48. “A threat emanating from component E also threatens to compromise component A, [as shown by] the attack vector 1806 passing through component B to reach component A.” ’008 Pat., 25:48-50. “A threat emanating from component D also threatens to compromise the asset, [as shown by] the attack vector 1804 passing through component C and component B to reach component A.” ’008 Pat., 25:50-53.

Claims 4 and 12 recite features related to this disclosed aspect of the ’008 Patent. Claim 4 is reproduced below:

4. An attack simulation method, comprising:
providing one or more databases, the one or more databases
comprising:
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;
providing one or more interfaces, including a diagram interface,
configured to be displayed on one or more end user computing

devices communicatively coupled with the one or more databases;

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 a user selection of one of the diagrammed threat model components of the first threat model through the one or more interfaces, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component..

’008 Pat., 36:16-42. Dependent claim 2 recites features substantially similar to the final “configuring” element of claim 4. To illustrate these similarities, claim 2 is reproduced below in annotated form, with italics added to identify the claim language that is identical to the final “configuring” element of claim 4:

2. The threat model chaining method of claim 1, further comprising *configuring the diagram interface to, in response to receiving a user selection of one of the diagrammed threat model components of the first threat model,*³ *visually display attack paths of*

³ Claim 2 does not include the “through the one or more interfaces” language that is recited in claim 4.

all threats associated with the diagrammed threat model components which compromise the selected threat model component.

’008 Pat., 38:39-46 (emphasis added). These claimed features are addressed prominently in Ground 2 of the Petition. This Ground, and its deficiencies, is introduced in Section I.C below.

C. Summary of the Petition’s Challenges

Petitioner asserts five grounds against these challenged claims.

In Ground 1, Petitioner contends that claims 1 and 3 are anticipated by the Jones⁴ reference.

In Ground 2, Petitioner contends that claims 1-20 are rendered obvious by Jones in view of the Zheng⁵ reference and the Keenan⁶ reference. (Petitioner refers to Jones, Zheng, and Keenan collectively as the “References of Ground 2”).

In Ground 3, Petitioner contends that claims 1-20 are rendered obvious by the References of Ground 2 further in view of the Yu⁷ reference. (Petitioner refers to Jones, Zheng, Keenan and Yu collectively as the “References of Ground 3”).

⁴ Ex. 1004, U.S. Patent No. 9,602,529 (“Jones”).

⁵ Ex. 1005, U.S. Patent No. 10,503,907 (“Zheng”).

⁶ Ex. 1006, U.S. Patent No. 11,200,228 (“Keenan”).

⁷ Ex. 1007, U.S. Patent No. 9,948,652 (“Yu”).

In Ground 4, Petitioner contends that claims 1-20 are rendered obvious by the References of Ground 3 further in view of the Reith⁸ reference. (Petitioner refers to Jones, Zheng, Keenan Yu, and Reith collectively as the “References of Ground 3”).

In Ground 5, Petitioner contends that claims 5-8 and 13-15 are rendered obvious by the References of Ground 4 further in view of the Knowledge of a POSITA.

However, in each ground, the asserted references—whether considered alone or in Petitioner’s asserted combinations—fail to disclose or suggest every claimed feature. For example, in Ground 1, Petitioner identifies Jones as an anticipatory reference. But Jones fails to disclose or suggest at least any “second threat model” or “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 [a] component group” comprising “a predefined interrelated group of two or more of the threat model components” as claimed. The Petition improperly treats these features as satisfied by Jones’s disclosure of component nesting, but this is incorrect and fails to give meaning to the complete claim language. Considered in

⁸ Ex. 1008, U.S. Patent No. 10,216,938 (“Reith”).

full, every feature of claim 1 is not disclosed by Jones, and Petitioner’s anticipation theory fails.

In Ground 4, Petitioner adds Reith to remedy Jones’ shortcoming in this regard. But the challenge based on Reith fares no better than failed Ground 1, as Reith discloses interconnections between separate threat models but does not include in a first threat model “a second threat model associated with [a] component group,” along with the related claimed features of claim 1. Further, Petitioner’s assertion to the contrary suffers from an interpretation of Reith that is unwarranted by its disclosures and is clearly influenced by impermissible hindsight. Claim 1 plainly survives the Ground 1 and Ground 4 challenges presented in the Petition.

The References of Ground 2—Jones, Zheng, and Keenan—are relied upon by Petitioner in its Ground 2 challenges of the attack vector claims 2, 4, and 12, but these References of Ground 2 are also deficient in their disclosures. According to claims 2, 4, and 12, upon receiving a user selection of a threat model component, the diagram interface visually displays attack paths of all threats associated with the selected threat model component. These features are neither disclosed nor suggested by the References of Ground 2. Petitioner relies on Zheng to disclose the visualization of a displayable vector connecting a threat actor to a threat target, but Zheng does not disclose how a vector is called up, and certainly does not

disclose the display of all attack paths associated with a threat model component upon receiving a user selection of that component. Ground 2 therefore fails.

Finally, the references relied upon in Grounds 3 and 5 do not cure any of the above-identified shortcomings of Grounds 1, 2, or 4 against the challenged claims. As such, each challenge fails, and the Petition should be denied without institution.

II. THE BOARD NEED NOT REACH ANY CLAIM CONSTRUCTION ISSUES TO DENY THE PETITION

The Petitioner identifies two terms as requiring constructions and proposes constructions consistent with the plain and ordinary meaning of these terms:

“threat model components” and “attack paths.” Pet., 12. Without expressly agreeing to Petitioner’s proposed constructions, and without waiving its right to submit constructions in a Patent Owner Response, Patent Owner submits that the Board need not engage in any pre-institution claim construction of these terms.

For the reasons presented in Section III below, Petitioner’s grounds each include fundamental flaws and fail to establish the disclosure of every claimed element in each independent claim. These findings do not require the Board to conduct any construction of the above-identified terms.

III. PETITIONER’S CHALLENGES FAIL ON THE MERITS

Each challenge is facially deficient in establishing the unpatentability of any challenged claim. In Ground 1, Petitioner contends that Jones anticipates claims 1 and 3, but this is wrong. Jones fails to disclose any “second threat model” as

claimed, and the entire Element 1[f] directed to this claimed feature is neither disclosed nor suggested by Jones. Jones's failure to disclose this feature is not remedied by Reith in Ground 4.

Ground 2 also fails. The References of Ground 2 fail to disclose at least "in response to receiving a user selection of one of the diagrammed threat model components of the first threat model, visually display[ing] attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component" as recited in claim 2, and fail to disclose related features in claims 4 and 12.

Finally, Grounds 3 and 5 do not remedy the shortcomings of any of the prior Grounds 1, 2, or 4. The Petition fails to establish unpatentability of any challenged claim and should be denied.

A. Jones Fails to Disclose at least Element 1[f] of Claim 1 and Fails to Anticipate Claims 1 and 3

Claim 1 recites, in relevant 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 interrelated group of two or more of the threat model components.”⁹

Petitioner alleges that Jones discloses this element. Pet., 35. In particular, Petitioner points to Jones’s disclosure of “multiple nested components, one or more of which may include further additional nested components at lower levels of the hierarchy.” Pet., 35-36 (quoting Jones, 5:4-19). Petitioner then reproduces Jones’s Figure 9, along with Figures 1, 2, 3, and 5, and provides a series of string citations to Jones’s specification without providing meaningful discussion of any of these disclosures. See Pet., 36-39. Finally, Petitioner concludes its challenge of this Element 1[f] by alleging that “Jones’ nesting disclosure meets this limitation,” because “the ’008 patent refers to chaining and nesting as the same concept.” Pet., 40. In essence, Petitioner’s theory regarding Element 1[f] is that Jones discloses this element because it discloses nested components. This is wrong.

First, Petitioner’s reduction of Element 1[f] to the concept of “nesting” fails to give full and proper credit to every claimed feature. For example, Element 1[f] includes the following feature: “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.” Nowhere does Petitioner identify a

⁹ Petitioner refers to this claim feature as Element 1[f]. Patent Owner will do the same.

“second threat model” in Jones. Petitioner argues that this feature is satisfied by Jones “creating a level $n+1$ threat model with one or more nested components.” Pet., 36. But Petitioner identifies no “second threat model” in this discussion, and identifies no instance in which Jones redefines a first threat model by including in it a second threat model. Instead, Petitioner’s focus is on Jones’s ability to nest components within a single threat model. Indeed, Jones expressly discloses that “one or more of the information system’s components—more often a process, host or data store—may include multiple nested components, one more of which may include further additional nest components at lower levels of the hierarchy.” Jones, 5:14-19. This nesting of components does not disclose any “second threat model” as required by claim 1.

Even Petitioner’s reliance on Jones’s disclosure at 12:64-13:7 to allegedly teach a “threat model renderer composing a threat model from the components of multiple stored threat models” is unsupported and wrong. See Pet., 37 (citing Jones, 12:64-13:7). Instead, Jones’s 12:64-13:7 discloses that metadata attributes of threats can be filled in from “threat-model DFD storage” 310 “without itself composing the threat-model DFD.” Jones, 12:64-13:7. Retrieving metadata *without* composing a threat-model DFD does not disclose “composing a threat model” as alleged by Petitioner. Pet., 37. Further, there is no discussion in this cited disclosure of Jones directed to “multiple stored threat models,” contrary to

Petitioner’s incorrect assertion. Petitioner fails to establish that modeling a system with nested components meets the claimed feature of “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.”

Second, Petitioner cites to Jones’s Figure 9 and associated description in its challenge of Element 1[f], but this reliance is not explained cogently. Petitioner quotes Jones, 19:10-28, which discloses “a level n threat-model DFD 902 produced from the level n DFD 902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD.” Despite Petitioner’s prior reliance on nested components for Element 1[f], this disclosure has nothing to do with nested components. Further, Jones’s disclosure of a level n DFD 902 including threats 904 is not tantamount to “redefine[ing] the first threat model by including in it a second threat model associated with the component group,” and Petitioner never explains why this quotation from Jones is relevant to its challenge. It simply alleges certain claimed features are present in Jones and reproduces this quotation in conclusory fashion.

In this same paragraph of the Petition, Petitioner also argues that a “POSITA would understand that the interrelated group of two or more threat model components in Jones may be predefined because Jones discloses identifying elements of the information system, which would be dependent on a predefined

system when Jones’ system is applied.” Pet., 36 (citing Ex. 1003, ¶82). But this sentence does not explain which threat model components are allegedly part of a “component group,” does not explain what “predefined system”¹⁰ Petitioner is referring to, and does not identify any “second threat model associated with” any “component group” as required by claim 1. Paragraph 82 of Ex. 1003 provides no additional answers, as it merely parrots the same confusing sentence from the Petition. See Ex. 1003, ¶82 (“A POSITA would understand that the interrelated group of two or more threat model components in Jones may be predefined because Jones discloses identifying elements of the information system, which would be dependent on a predefined system when Jones’ system is applied.”). This type of conclusory statement is entitled to no weight. See 37 C.F.R. § 42.65(a); *Samsung Elec. Co., Ltd. v. Rightquestion, LLC*, IPR2022-00251, Paper 17 at 25 (PTAB June 9, 2022) (declining to credit testimony where “declarant makes these same statements verbatim, without more, and with no additional citations to evidence”).

¹⁰ To the extent Petitioner is arguing that a “predefined system” must be modeled in Jones, this is unsupported. Jones specifically discloses that its implementation “may facilitate the design or modification of an information system to mitigate or further mitigate the risk of ... threats, to an acceptable if not desired level.” Jones, 1:55-58. Modeling a system as part of the design or modification process does not disclose or suggest a “component group compris[ing] a predefined interrelated group of two or more of the threat model components” as claimed.

Third, Petitioner overlooks that claim 1 is a method claim. Aside from pointing generally to Jones's GUI as described at 18:44-57 (*see* Pet., 39-40), Petitioner identifies no way in which Jones allegedly discloses the claimed method step of "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."

For each of these reasons, Jones fails to disclose Element 1[f] of claim 1. Further, it is well-accepted that a "claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co. of Cal.*, 814 F.2d 628, 631 (Fed. Cir. 1987). Jones therefore fails to anticipate claim 1. Claim 3, also challenged in Ground 1, depends from claim 1 and therefore also survives Petitioner's failed Ground 1. Petitioner's Ground 1 fails and does not warrant institution of this proceeding.

B. Ground 2 Also Fails

Petitioner introduces its Ground 2 challenge by stating, "Ground 1 is incorporated by reference in ground 2." Pet., 41. As such, the fatal flaws of Ground 1, discussed above, are also incorporated into Petitioner's Ground 2.

i. Claims 2, 11, and 20 Survive Ground 2 For Reasons Already Explained for Element 1[f]

Claim 2 depends from claim 1, and is not shown to be obvious over the asserted combination of Jones, Zheng, and Keenan because Jones fails to disclose at least the features of Element 1[f]. Zheng and Keenan are not relied upon by Petitioner to remedy these deficiencies of Jones alone, and therefore claim 2 independently survives Petitioner's Ground 2 challenge.

Claim 11 and claim 20 also survive Ground 2. Petitioner cites to its analysis for Element 1[f] in view of Jones for its challenges of these claims. Pet., 48, 54. Zheng and Keenan are not relied upon by Petitioner to remedy these deficiencies of Jones alone, and therefore claims 11 and 20 also survive Petitioner's Ground 2 challenge.

ii. Dependent Claim 2 is also Independently Patentable Over the References of Ground 2

Claim 2 recites in relevant part, "in response to receiving a user selection of one of the diagrammed threat model components of the first threat model, visually display[ing] attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component." Thus, according to claim 2, a user may select a threat model component, and upon receiving that user selection, the diagram interface visually displays attack paths of all threats associated with the selected threat model component. Without

disclaiming the independent patentability of any other dependent claim, this feature of dependent claim 2 is neither disclosed nor suggested by the References of Ground 2.

Petitioner asserts that “Zheng discloses this element.” Pet., 42. This is wrong. Zheng can visualize “each security threat as a threat actor, a threat target and a displayable vector connecting the threat actor to the threat target.” Zheng, 2:36-42. But Zheng does not disclose or suggest any scenario where “all threats” associated with a selected threat model component are displayed. Indeed, Zheng does not disclose how to activate the visual display of any displayable vector, much less displaying the attack paths of all threats associated with a selected component upon receiving a user selection of the component. Petitioner hides behind the disingenuous statement that “Zheng does not limit itself to identifying less than all threats.” Pet., 42. But there is no indication in Zheng whether a displayable vector constitutes all threats to a component or whether there are other vectors that are not displayed, because Zheng discloses nothing about displaying “all threats” associated with a component. In any event, Zheng does not disclose any component selection as causing the displayable vector to be displayed. As a result, Zheng fails to disclose at least a diagram interface visually displaying attack paths of all threats associated with the selected threat model component upon receiving a user selection of the threat model component. Thus, the asserted

combination of Jones, Zheng, and Keenan fails to disclose every feature of challenged claim 2.

iii. Independent Claims 4 and 12, and Their Respective Dependent Claims, Also Survive Ground 2

As introduced above in Section I.C, independent claims 4 and 12 recite substantially similar features as claim 2, and Petitioner relies upon its analysis for claim 2 in challenging these elements of independent claims 4 and 12. Pet., 44 (referring to Petitioner’s claim 2 analysis to satisfy Element 4[e]); *id.*, 50 (referring to Petitioner’s claim 2 analysis to satisfy Element 12[e]). For the same reasons that Zheng fails to disclose or suggest the features of claim 2, Zheng also fails to disclose or suggest Element 4[e] and Element 12[e].

For these same reasons, Petitioner also fails to establish the unpatentability of claims 2 and 4-20 in Ground 2.

C. Ground 3 Also Fails

Petitioner relies upon Yu to disclose “compensating controls” and “attack paths,” but does not rely upon Yu to remedy any of the shortcomings of Ground 2 addressed above in Section IV.B. See Pet., 57-60. Like Zheng, Yu discloses nothing about displaying “all threats,” and does not disclose a diagram interface visually displaying attack paths of all threats associated with a selected threat model component upon receiving a user selection of the threat model component, as claimed. Indeed, Petitioner does not rely on Yu to remedy these shortcomings

of Zheng. As such, the fatal flaws of Ground 2, discussed above, also infect Petitioner’s Ground 3, and Ground 3 fails.

D. Ground 4 Also Fails Because Reith Fails to Remedy Jones’s Shortcomings for Element 1[f]

Petitioner relies upon Reith in combination with Jones, Zheng, Keenan, and Yu as an alternative reference for Element 1[f], claim 11, and claim 20. Pet., 60-62.¹¹ This challenge also fails, however.

First, claim 20 depends from base claim 12, and Reith does not remedy the shortcomings of Ground 2 against claim 12 as addressed above in Section IV.B. Thus, claim 20 survives this Ground 4 for the same reason that base claim 12 survives Ground 2.

Claims 1, 11, and 20 also survive Ground 4 because Reith fails to remedy the shortcomings identified above for Jones and Element 1[f]. Petitioner relies on Reith’s disclosure that “multiple Recombinant Threat Models may be interconnected together” for Element 1[f], claim 11, and claim 20. Pet., 60-61; Reith, 4:30-44. Petitioner then contends that 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.’” Pet., 61. But

¹¹ Petitioner refers to “limitation 1[e]” rather than 1[f] in the Petition. Pet., 60. Given the similarities between Element 1[f] and claims 11 and 20, this appears to be error.

this statement confirms that Petitioner is viewing Reith's disclosures through the lens of impermissible hindsight because Reith does not disclose incorporating an existing threat model into a new threat model while "building the threat model." To the contrary, as illustrated by Reith's Figure 4, Reith only discloses separate threat models that are interconnected without any individual threat model being incorporated into another or redefined, as reproduced below.

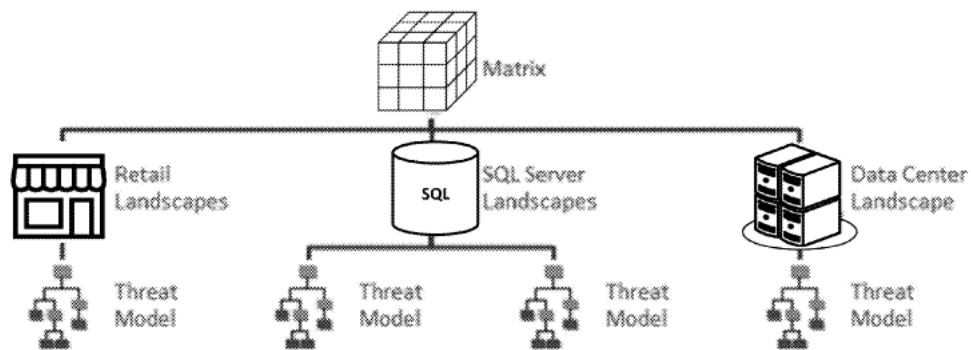


Figure 4

Element 1[f] of claim 1 recites in relevant part "adding 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." In the specification and Figure 4 of Reith, there is no disclosure of a second threat model included in a first threat model that is redefined. As shown in Reith's Figure 4, there are simply separate threat models that are interconnected, without any threat model incorporated into another threat model or any first threat model that is

redefined. As such, Reith also fails to remedy the shortcomings of the Petition as to Element 1[f] and claims 11 and 20. Additionally, since Reith fails to disclose or suggest this claimed Element 1[f], a POSITA would not have had a reason to modify Jones, Zheng, Keenan and Yu to include this missing feature based on Reith.

For all these reasons, Ground 4 also fails to establish unpatentability of any challenged claim.

E. Ground 5 Also Fails

Petitioner adds the knowledge of a POSITA to the References of Ground 4 to challenge dependent claims 5-8 and 13-15. This addition does not remedy the shortcomings of Grounds 2-4 addressed above. *See* Pet., 57-60. As such, the fatal flaws of Grounds 2-4, discussed above, are also incorporated into Petitioner's Ground 5, and Ground 5 fails.

IV. CONCLUSION

For the reasons presented above, the Petition should be denied, and no *inter partes* review should be instituted.

Dated: August 22, 2023

/s/ Wayne M. Helge
Wayne M. Helge (Reg. No. 56,905)
NOSSAMAN, LLP
1401 New York Ave, NW
Suite 800
Washington, DC 20005
Telephone: (202) 887-1400

IPR2023-00821 Patent Owner's Preliminary Response

Email: whelge@nossaman.com

Christopher H. Blaszkowski
(Reg. No. 61,461)
RATNERPRESTIA
2200 Renaissance Blvd
Suite 350
King of Prussia, PA 19406
Telephone: 610-407-0700
Email: cblaszkowski@ratnerprestia.com

Counsel for Patent Owner

CERTIFICATE OF WORD COUNT

The undersigned certifies that the foregoing PATENT OWNER'S PRELIMINARY RESPONSE complies with the type-volume limitation in 37 C.F.R. § 42.24(b)(1). According to the word-processing system's word count, the brief contains 5,012 words, excluding the parts of the brief exempted by 37 C.F.R. § 42.24(a).

By: /s/ Wayne M. Helge
Wayne M. Helge (Reg. No. 56,905)
Attorney for Patent Owner

CERTIFICATE OF SERVICE

I hereby certify that on August 22, 2023, a true and correct copy of the foregoing document was served via email, by consent, to Petitioner by serving the correspondence email addresses of record as follows:

Brent Yamashita
Reg. No. 53,808
DLA Piper LLP (US)
2000 University Avenue
East Palo Alto, California
94303-2214
Phone: 650.833.2348
Fax: 650.833.2001
Email:
brent.yamashita@us.dlapiper.com

Blake Jackson
Reg. No. 66,272
DLA Piper LLP (US)
2000 University Avenue
East Palo Alto, California
94303-2214
Phone: 650.833.2248
Fax: 650.687.1148
Email:
blake.jackson@us.dlapiper.com

Matthew Middleton
Reg. No. 77,117
DLA Piper LLP (US)
1201 N. Market St., Suite 2100
Wilmington, Delaware
19801-1147
Phone: 302.468.5675
Fax: 302.778.7935
Email:
matthew.middleton@us.dlapiper.com

/s/ Wayne M. Helge
Wayne M. Helge (Reg. No. 56,905)
Attorney for Patent Owner