

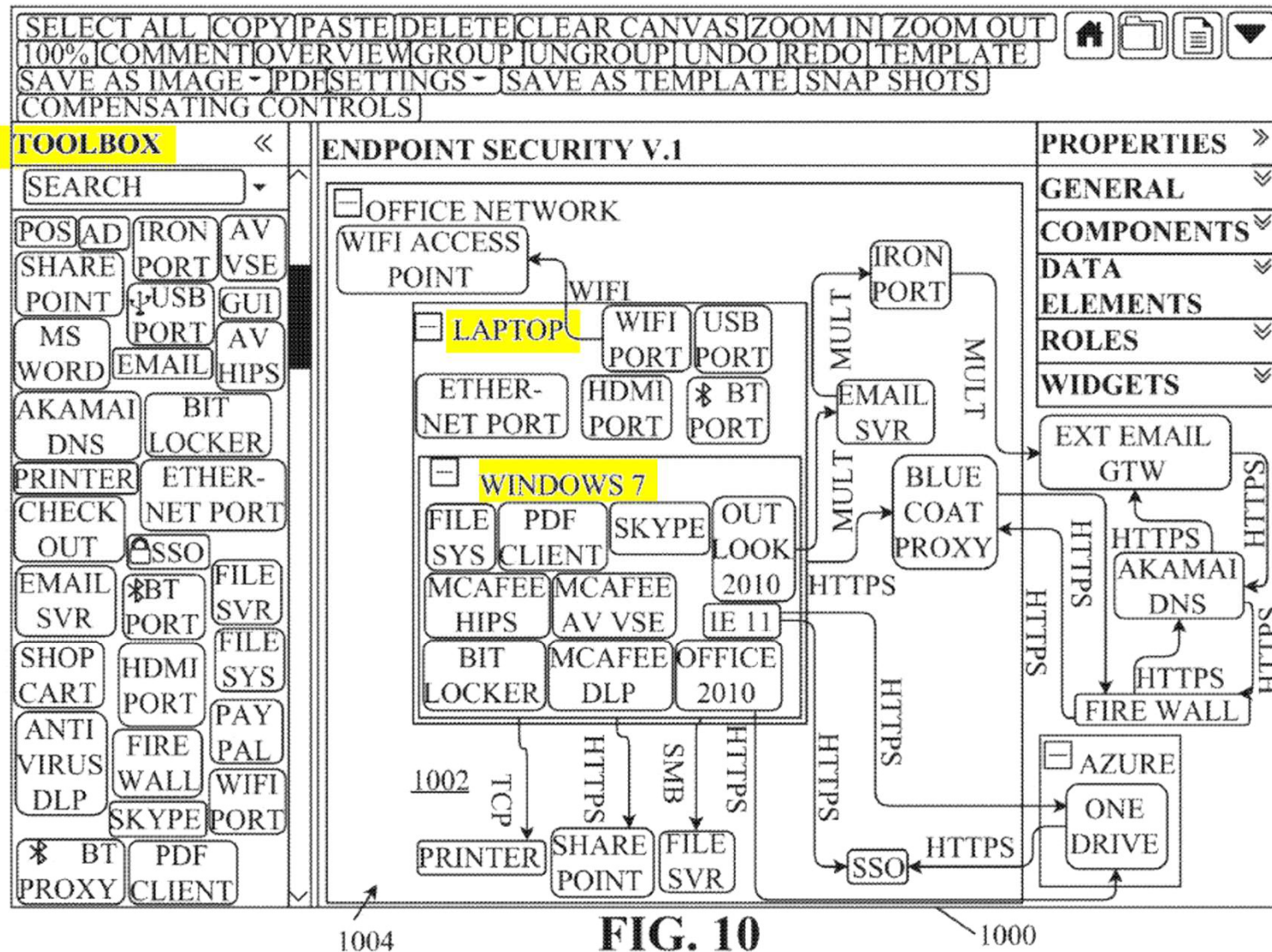
IriusRisk v. ThreatModeler

IPR2023-00821

Patent No. 10,699,008 B2

ThreatModeler Oral Argument

Threat Model Nesting or Chaining



EX-1001, Fig. 10.

Display All Attack Paths

order. In step **1408**, once a user has selected an asset to analyze, the system summarizes data to show all attack vectors associated with threats which may compromise that asset. At step **1410** the user analyzes the various attack vectors to determine what compensating controls may be included to protect the asset. At step **1412** the user adds or removes compensating controls to the diagram and/or toggles compensating controls between ON/OFF states. At step **1414** the user determines the effectiveness of the compensating controls or other risk management methods (such as changing communication protocols, changing the relative location of the asset within the modeled environment, adding non-compensating control elements between the asset and attack locations, and so forth).

Claim Construction: “Redefine the First Threat Model ...”

“Redefine the first threat model by including in it a second threat model associated with the component group” means:

“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.”

Claim Construction: *Ex parte Schulhauser*

Schulhauser claim 1:

“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.*”

The claim is satisfied even if the stated conditions are not met.

Schulhauser at 6.

Claim Construction: *Ex parte Schulhauser*

'008 Patent, claim 1:

“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.
- To satisfy this step, both the user input(s) must be received and the diagram interface must be configured to add a component group.

EX-1001, 35:56-58.

Ground 1: Jones Does Not Disclose Element 1[f]

Element 1[f]:

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

EX-1001, 35:56-63.

Ground 1: Jones Does Not Disclose Element 1[f]

on which the data store is configured to run. In some examples, the information system may be describable in terms of a hierarchical breakdown (hereinafter referred to as a “hierarchy”) of its components (interconnected by appropriate data flows) at different levels. In this regard, one or more of the information system’s components—more often a process, host or data store—may include multiple nested components, one or more of which may include further additional nested components at lower levels of the hierarchy.

EX-1004, 5:10-19.

Ground 1: Jones Does Not Disclose Element 1[f]

their cybersecurity threats. In these examples, the decomposer 110 may be configured to decompose one or more components of the information system modeled by the DFD into its nested components and data flows therebetween. The

EX-1004, 6:15-18.

Ground 1: Jones Does Not Disclose Element 1[f]

The DFD creator **106** may be configured to identify elements of the information system, and compose a DFD for the information system from those elements and in accordance with the threat-model level identified by the DFD level establishment system **104**. The DFD may include nodes representing the components and edges representing the data flows. The DFD represent the information system at some level n of the hierarchy, and may at times be referred to as a level n DFD (e.g., level 2 DFD).

EX-1004, 5:45-53.

Ground 1: Jones Does Not Disclose Element 1[f]

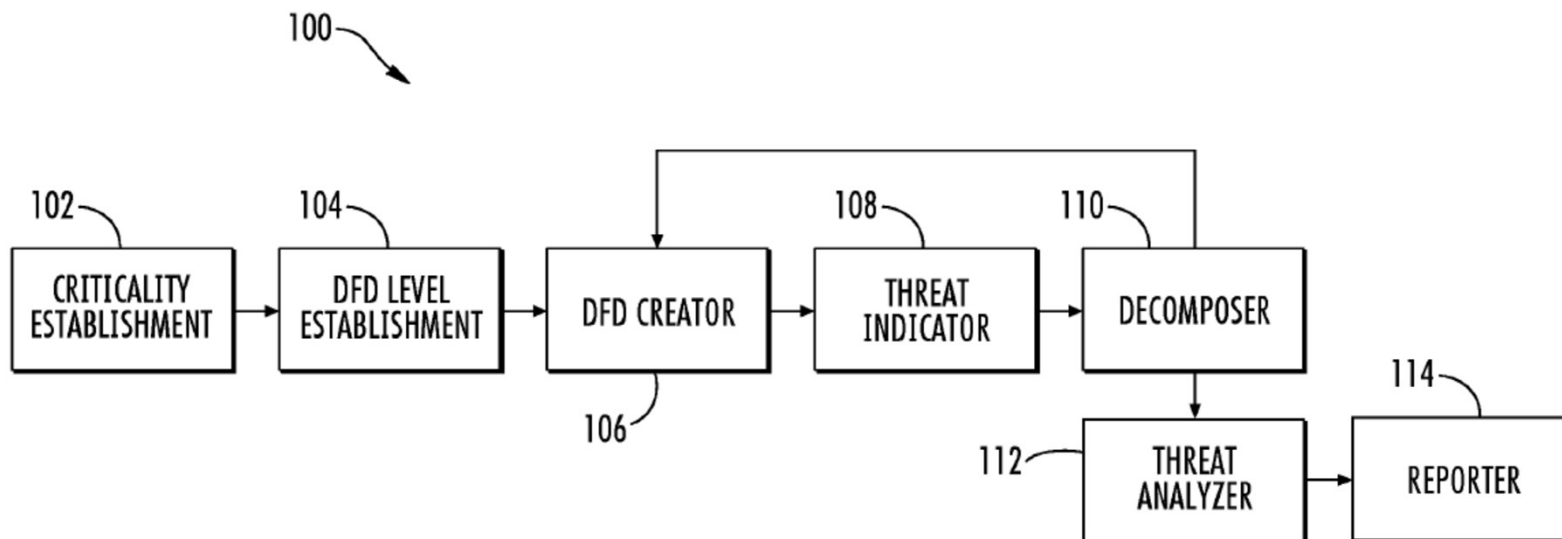


FIG. 1

EX-1004, Fig. 1.

Ground 1: Jones Does Not Disclose Element 1[f]

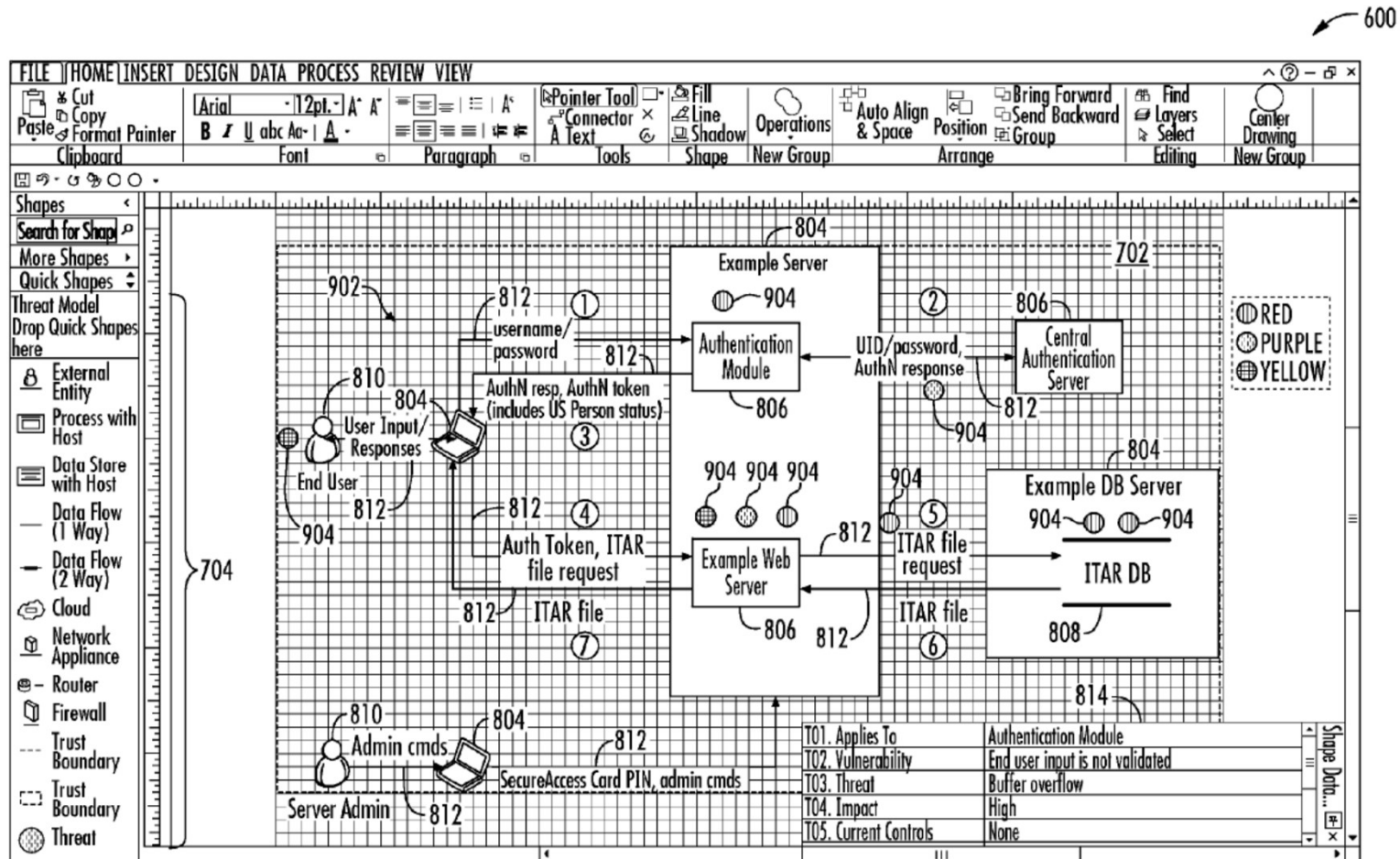


FIG. 9

EX-1004, Fig. 9.

Ground 1: Jones Does Not Disclose Element 1[f]

The claims of the '008 patent state that the “component group” that is added to the “first threat model” must have its own “second threat model” before the “component group” is included/added to the “first threat model.”

Ground 1: Jones Does Not Disclose Element 1[e]

Element 1[e]:

“configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls”

EX-1001, 35:50-55.

Ground 1: Jones Does Not Disclose Element 1[e]

their shapes. Also similar to before, in some examples, the window 814 may be recalled for each of the shapes, in which data for a shape and thus attributes of a cybersecurity threat may be entered, and thereby included as structured information in metadata associated with the shape (and thus secondary node). FIG. 9 illustrates an example in which the

EX-1004, 19:18-23.

Ground 1: Jones Does Not Disclose Element 1[e]

cation or process to be modeled. By non-limiting example, FIG. 10 shows interface 10 with a relational diagram (diagram) 1004 already fully created by the user. As can be seen, the user has dragged multiple components onto the canvas 1002 and has defined various relationships between them.

EX-1001, 16:48-51.

Ground 1: Jones Does Not Disclose Claim 3

Claim 3:

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

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

Ground 1: Jones Does Not Disclose Claim 3

Q. So the additional threat model components of claim 3 are not satisfied by the threat model components of Claim 1, right?

A. Correct.

Q. And then claim 3 also refers to additional threats, right?

A. Correct.

Q. And the same logic holds true, that the additional threats are threats in addition to the threats that were recited in Claim 1, right?

A. Correct.

Q. And then just to round things out here, claim 3 refers to additional compensating controls. Do you see that?

A. Yes.

Q. And the same is true for those additional compensating controls are in addition to whatever compensating controls are recited in Claim 1, right?

A. Yes, that's correct.

Q. ... Is that the understanding you used when you analyzed claim 3 here in, it looks like paragraph 85?

A. ... So yes. That was my understanding in analyzing claim 3.

EX-2002, 82:17-84:6.

Ground 2: Dependent Claim 2

Claim 2:

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

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

Ground 2: Dependent Claim 2

The Petition relies on Zheng for teaching or suggesting the subject matter of claim 2.

Zheng teaches displaying an entire layer or no layer at all.

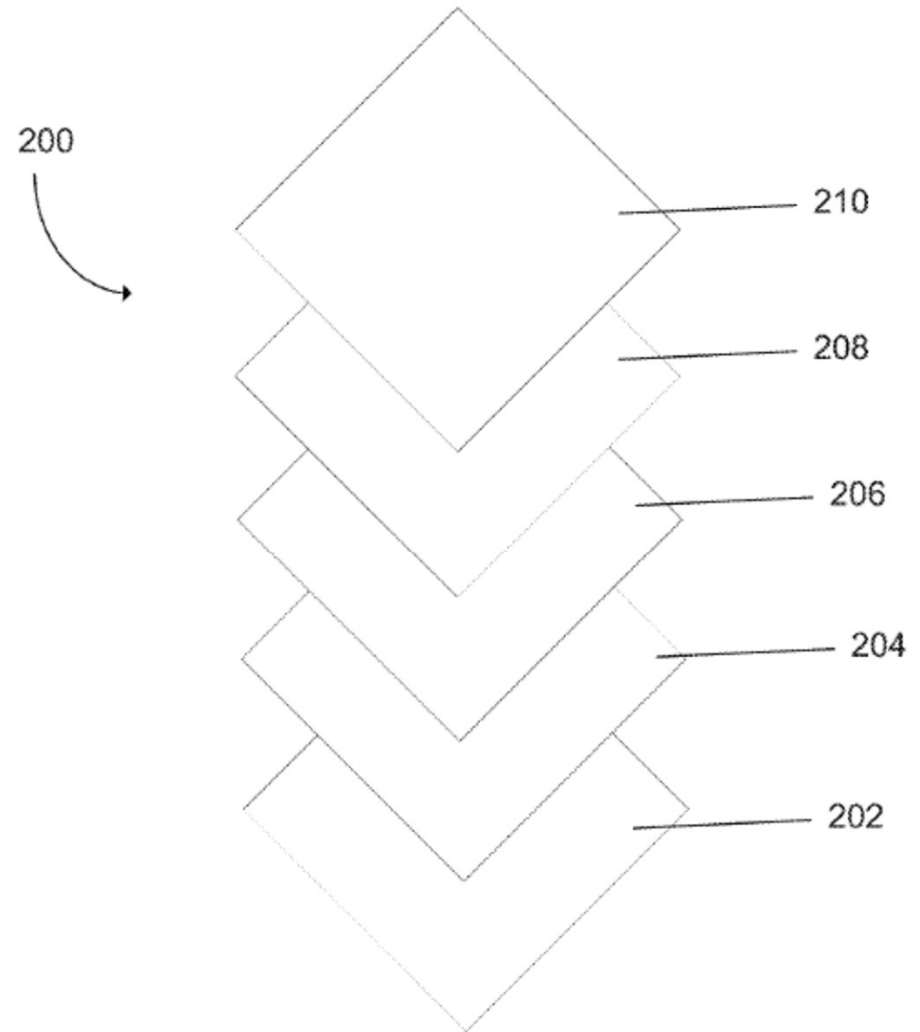


FIG. 2

EX-1005, Fig. 2.

Ground 2: Dependent Claim 2 (Zheng)

tate data extraction. The **base layer 202** serves as the foundational piece of the security risk analysis system **100**. The additional layers of the system **100** (akin to terrains, traffics, etc. of a map) include a layer representing threat modeling **204** of perceived threats, a layer representing security controls **206**, a layer representing real-time (or near real-time) actual threats **208**, and a layer representing simulated data flow **210** throughout the application ecosystem. These 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. These additional layers **204-210** can overlay the base layer **202** in the order as illustrated in FIG. 2 or any other order. As an example, in the threat update

EX-1005, 4:5-18.

Ground 2: Dependent Claim 2 (Zheng)

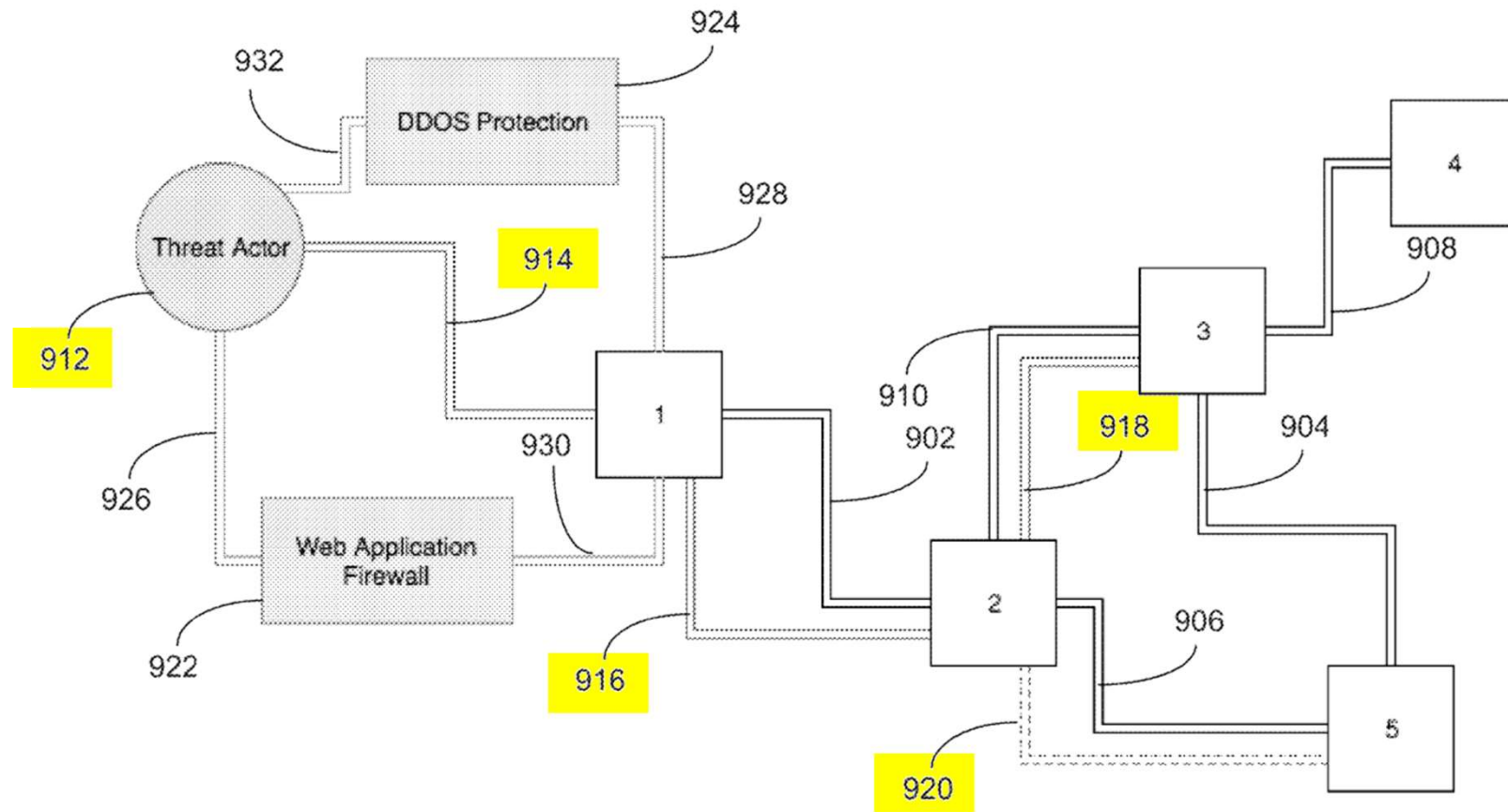


FIG. 8

 = threat model layer

EX-1005, Fig. 8.

Ground 2: Dependent Claim 2

Reply cites to 11:41-55:

- Toggling subcategories within a layer.
- Enabling or disabling particular type (i.e., category) of threats.
- No selection of “one of” the diagrammed threat model components.
- No selection of a “threat model component.” Only enabling or disabling types/categories of threats.

Ground 2: Dependent Claim 2

No Motivation to Combine Zheng with Jones:

- Jones teaches selecting individual threats and viewing the threat attributes. (EX-1004, 19:23-25).
- Zheng teaches selecting an entire layer (such as the threat model layer). (EX-1005, 5:6-24)
- Jones is superior to Zheng because Jones allows a user to edit the attribute information for a threat. Zheng does not offer that feature. (EX-2003, ¶121)

Ground 2: Dependent Claim 2

Keenan:

- Not relied upon in the Petition
- Risk analysis (not threat analysis)
- Col. 17:12-20 relates to displaying upstream and downstream data flows or paths.
- No selection of threat model components and displaying all attack paths

EX-1006, 17:12-20.

Ground 2: Independent Claim 4

Claim 4:

- Element 1[e] analysis applies
- Claim 2 analysis applies

Ground 2: Dependent Claims 6 and 7

Claim 6:

- Toggle first compensating control “on” to toggle all attack paths mitigatable by the first control to a mitigated state.

Claim 7:

- Toggle first compensating control “off” to toggle all attack paths mitigatable by the first control to an unmitigated state.

EX-1001, 36:49-61.

Ground 2: Dependent Claims 6 and 7

- Jones does not teach or suggest the display of “compensating controls” on the relational diagram recited in claim 4. (PO Response, 41).
- 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.” (PO Response, 41).
 - Petitioner and its expert provide no analysis of this claim requirement whatsoever. (see Petition, 45-46; EX-1003, ¶¶97-99; EX-2003, ¶128).
- No motivation to combine Jones and Zheng for “attack paths.” (See Claim 2 analysis).

Ground 2: Dependent Claim 8

Claim 8:

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

EX-1001, 36:62-67.

Ground 2: Dependent Claim 8

- Petitioner says removing a compensating control is the same as toggling the compensating control off. (Petition, 47).
- Removing a compensating control is different than turning it off. (PO Response, 42-43).
- Different words are presumed to have a different meaning. (PO Response, 43).

Ground 2: Dependent Claim 9

Claim 9:

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

EX-1001, 37:1-6.

Ground 2: Dependent Claim 9

- The Petition’s analysis is entirely conclusory. (Petition, 47).
- Expert’s analysis is equally conclusory. (Petition, 47).
- Zheng displays an entire layer. (EX-1005, Fig. 2).
- Zheng displays all paths from a threat to all potential targets or no paths whatsoever. (EX-1005, 11:56-12:14).
- There is no in-between teaching of a “subset.”
- The Reply attempts to change the analysis. (Reply, 17).

Ground 2: Dependent Claim 10

Claim 10:

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

Ground 2: Dependent Claim 10

- Petitioner provides no legitimate reason why a POSITA would have combined Zheng's teachings of displaying entire layers with either Jones or Keenan which teach editing individual element.
- Claim 10 requires a very specifically claimed type of alteration.
- Petitioner makes no attempt to show that the prior art teaches or suggests the claimed alteration.

PO Response, 44-45; Sur-Reply, 12-13.

Ground 2: Dependent Claim 11

Claim 11:

- Same analysis as for Element 1[f].

Ground 2: Independent Claim 12

Claim 12:

- Element 12[d] – Same analysis as for Element 1[e].
- Element 12[e] – Same analysis as for Claim 2 and Element 4[e].

Ground 2: Dependent Claim 13

Claim 13:

- Same analysis as for Claim 6.

Ground 2: Dependent Claim 14

Claim 14:

- Same analysis as for Claim 7.

Ground 2: Dependent Claim 15

Claim 15:

- Same analysis as for Claim 8.

Ground 2: Dependent Claim 16

Claim 16:

- Same analysis as for Claim 9.

Ground 2: Dependent Claim 17

Claim 17:

- Same analysis as for Claim 10.

Ground 2: Dependent Claim 19

Claim 19:

The attack simulation system of claim 18, wherein the diagram interface is further configured to, in response to receiving one or more user inputs, diagram a communication protocol between two of the diagrammed threat model components, the diagrammed communication protocol including an alphanumeric indicator.

EX-1001, 38:33-38.

Ground 2: Dependent Claim 19

- The Petition and Mr. Hurlbut's Declaration said "User Input/Responses," "Auth N token," and "ITAR file request" labels were the claimed "communication protocols." (Sur-Reply, 15; Petition, 53-54; EX-1003, ¶116).
- Mr. Hurlbut admitted at deposition that information like user name and password are not "communication protocols." (EX-2002, 108:13-16).

EX-1001, 38:33-38.

Ground 2: Dependent Claim 20

Claim 20:

- Same analysis as Element 1[f].
- Same analysis as Claim 11.

Ground 3: Ground 2 References plus Yu

- Yu does not remedy the Ground 1 and 2 deficiencies.
- Petitioner does not provide an evidence-based analysis for why a POSITA would have combined the Ground 2 references with Yu.
- Petitioner cannot say that it would have been obvious to combine the teachings of two or more references and then pick and choose pieces from those references.
 - *ActiveVideo Networks, Inc. v. Verizon Comm's, Inc.*, 694 F.3d 1312, 1328 (Fed. Cir. 2012) (“It [*i.e.*, the motivation to combine evidence] also fails to explain why a person of ordinary skill in the art would have combined elements from specific references *in the way the claimed invention does.*”) (emphasis in original);
 - *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 419-20 (2007)).

PO Response, 50-51; Sur-Reply, 16-18.

Ground 4: Ground 3 References plus Reith

- Petition relies on Reith for the “threat model chaining” features of Element 1[f] and Claims 11 and 20.
- Element 1[f] – “redefine the first threat model by including in it a second threat model associated with the component group”
- 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.

Ground 4: Ground 3 References plus Reith

Reith, Figure 4:

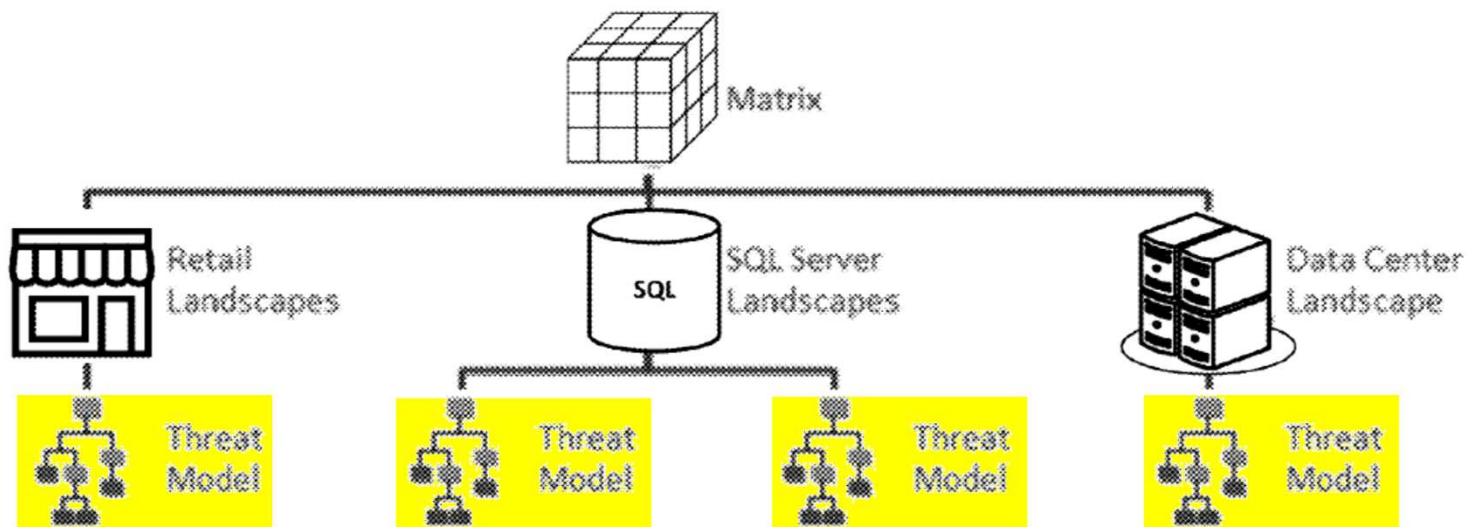


Figure 4

EX-1008, Fig. 4.

Ground 4: Ground 3 References plus Reith

Reith, 4:32-35:

Recombinant Threat Models (see FIG. 4). A Recombinant Threat Model may stand on its own within the threat landscape. Alternatively, multiple Recombinant Threat Models may be interconnected together. A threat landscape

- Reith never says that a second threat model is “added” to a first threat model “thereby redefining” the first threat model, as required by the ‘008 Patent claims.

EX-1008, 4:32-35.

Ground 4: Ground 3 References plus Reith

- No motivation to combine Reith with the Ground 3 references.
- A desire to “save time” is not a proper motivation.
- That “motivation” is hindsight based on the ‘008 Patent itself. (EX-1001, 20:26-36)
 - “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.”

PO Response, 52-53; Sur-Reply, 19-20.

Ground 5: Ground 4 References plus POSITA Knowledge

- Ground 5 only applies to claims 5-8 and 13-15.
- Knowledge of POSITA is relied upon for “toggling” features.
- Petition relies on Mr. Hurlbut’s declaration.
 - But Hurlbut declaration cites to no supporting evidence.
 - An expert’s *ipse dixit* statements are of little value.
 - *Cephalon, Inc. v. Watson Pharms, Inc.*, 707 F.3d 1330, 1338 (Fed. Cir. 2013) (“Dr. Mumper’s *ipse dixit* statements that co-administration would be ‘difficult’ and ‘complicated,’ however, cannot be enough to constitute clear and convincing evidence” of invalidity.).
 - *Ashland Oil, Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 281 (Fed. Cir. 1985) (“Lack of factual support” equals “little probative value.”).

PO Response, 54-55; Sur-Reply, 20-21.

Ground 5: Ground 4 References plus POSITA Knowledge

- No proper motivation to combine.
- Petition cites generic *KSR* categories of motivations to combine.
 - Petition alleges “reasonable expectation of success,” “very predictable technologies,” and “would not encounter any insurmountable challenge[s].” (Petition, 62-63, EX-1003, ¶134).
- Recitation of *KSR* categories is not sufficient to establish a proper motivation to combine references.
 - *ActiveVideo*, 694 F.3d at 1328; *KSR*, 550 U.S. at 419-20.

PO Response, 54-55; Sur-Reply, 20-21.

Mr. Hurlbut is Biased

Mr. Hurlbut:

- Personally knows Petitioner's CEO, COO, VP of Product Development, and one of Petitioner's technical advisors. (EX-2002, 10:10-16; 11:5-11; 11:16-12:9; 12:20-22).
- Petitioner's CEO personally asked Mr. Hurlbut to be Petitioner's expert. (EX-2002, 17:21-25).
- Mr. Hurlbut testified that he wanted to work on the IPRs to see "how I could contribute" and "[h]ow I could help" (EX-2002, 18:8-22).
- His employer, Aquia, is in the threat modeling business. (EX-2002, 13:5-11; 14:5-8; 7:25-8:11).
- Mr. Hurlbut has stock options (and thus a financial interest) in Aquia. (EX-2002, 8:4-11).

PO Response, 27 n.4; Sur-Reply, 21-22.

End