



IPR2023-00821 U.S. Patent No. 10,699,008

Presentation by Petitioner



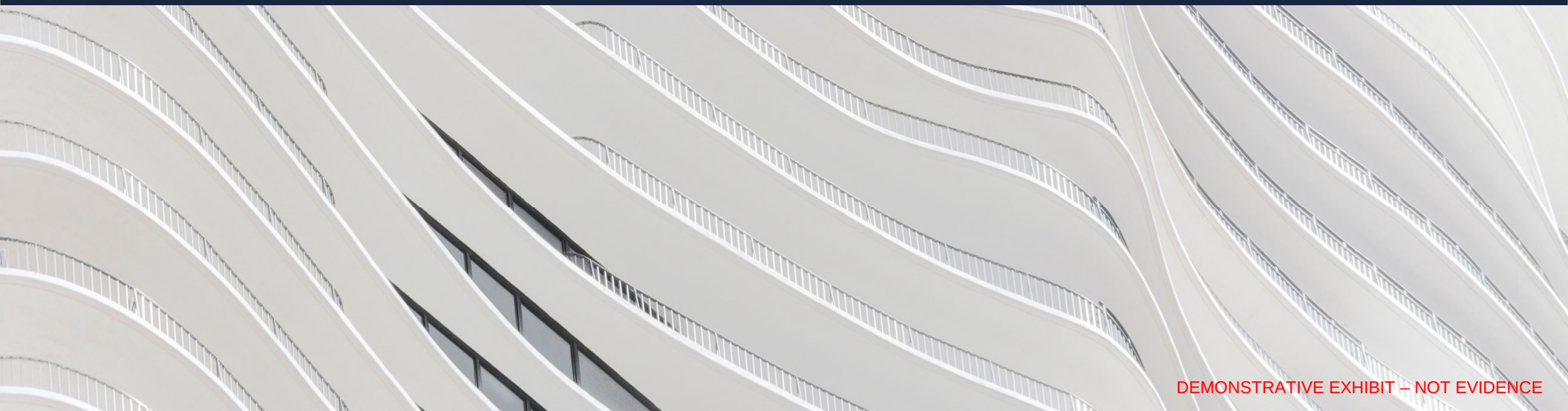
DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Overview of Presentation

- Summary of the '008 Patent
- Claim Construction
- Ground 1: Jones Anticipates Claims 1 and 3
- Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious
- Ground 3: Ground 2 References and Yu Render Claims 1-20 Obvious
- Ground 4: Ground 3 References and Reith Render Claims 1-20 Obvious
- Ground 5: Ground 4 References and Knowledge of POSITA Render Claims 5-8 and 13-15 Obvious

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Summary of the '008 Patent

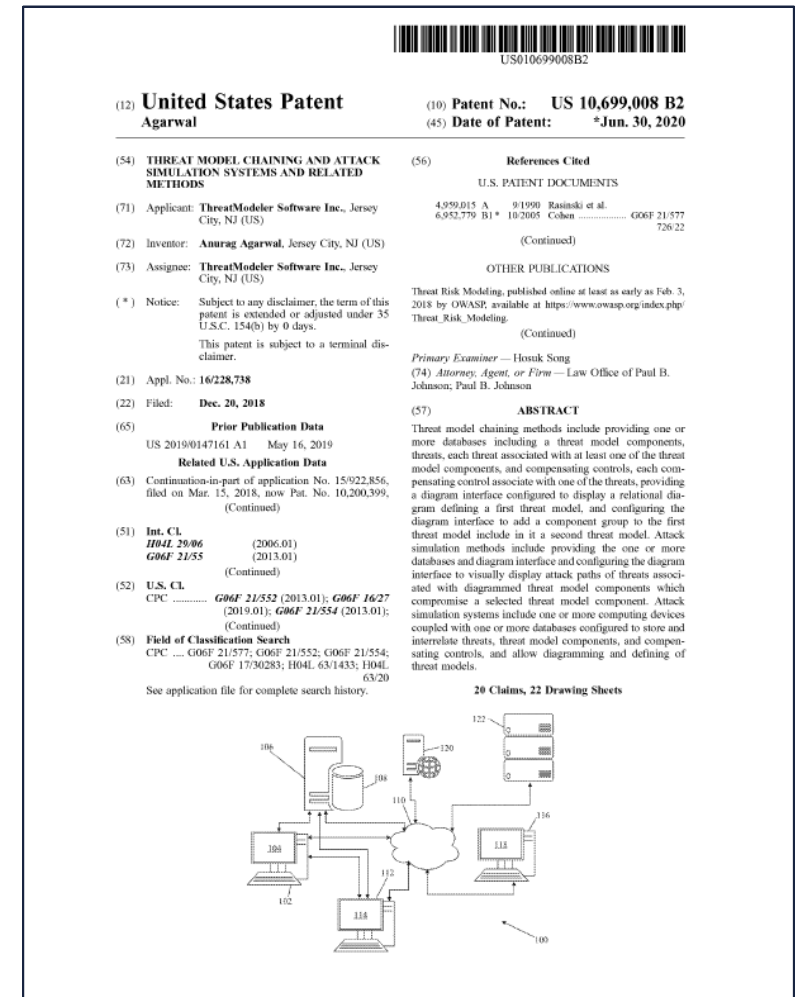


DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Summary of the '008 Patent

Three Key Concepts:

1. Threat Model
2. Compensating Controls
3. Nesting Threat Model in Another Threat Model



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Summary of the '008 Patent

Key Concept No. 1: Threat Model

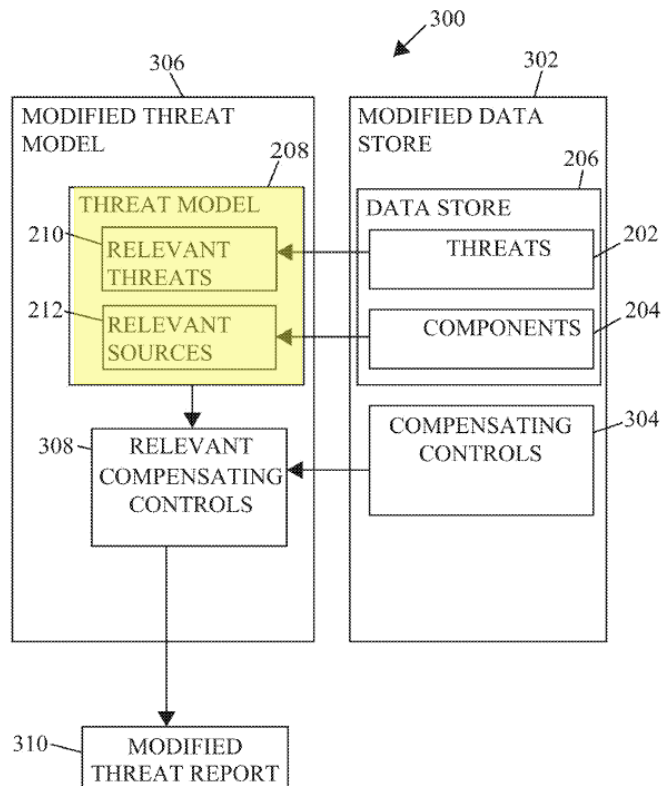


FIG. 3

Threat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized. One example of an existing threat modeler is a modeler marketed under the name THREAT MODELING TOOL by Microsoft Corporation of Redmond, Wash. Threat modeling allows a user to analyze potential attack vectors and prioritize vulnerabilities. While some threat modeling involves threats related to computing networks and systems, threat modeling in general encompasses a broader scope and may involve modeling threats in non-computer-related systems and processes. Some commercial threat modeling tools utilize a dynamic question and answer user interface which generally relies on an underlying data flow diagram (DFD) or process flow diagram (PFD) conceptual basis.

EX-1001 ('008) at 1:48-61

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Summary of the '008 Patent

Key Concept No. 2: Compensating Controls

COMPENSATING CONTROLS				
DRAG A COLUMN HEADER AND DROP IT HERE TO GROUP BY THAT COLUMN				
CONTROL	THREAT	SOURCE	RISK	STATUS
FIREWALL	TCP WINDOW SCAN	WINDOWS 7	LOW	MITIGATED
FIREWALL	TCY SYN SCAN	TCP	LOW	OPEN
FIREWALL	TCP ISN CTR RATE PROBE	TCP	LOW	OPEN
FIREEYE	MAN IN THE BROWSER	IE 11	VERY HIGH	MITIGATED
CYLANCE	MALWARE PROP VIA USB	USB PORT	VERY HIGH	MITIGATED
AV DLP	FORCE USE CORRUPT FILE	FILE SYSTEM	VERY HIGH	MITIGATED
MCAFFEE DLP	MAN IN THE MIDDLE ATK	WIFI PORT	VERY HIGH	MITIGATED
BIT9	FILE MANIPULATION	FILE SYSTEM	MEDIUM	MITIGATED
BIT9	ACCOUNT FOOTPRINTING	IE 11	VERY HIGH	OPEN
BIT9	AUTOMATION ATTACK	IE 11	VERY HIGH	MITIGATED
AV HIPS	PHYSICAL THEFT	LAPTOP	VERY HIGH	MITIGATED
BITLOCKER	PHYSICAL THEFT	LAPTOP	VERY HIGH	MITIGATED
IPC	BLUEJACKING	BLUETOOTH PORT	VERY HIGH	OPEN
IRONPORT	PHISHING	OUTLOOK 2010	VERY HIGH	MITIGATED
IRONPORT	SPAM	OUTLOOK 2010	VERY HIGH	MITIGATED
AKAMAI DNS	DNS CACHE POISONING	EMAIL SERVER	VERY HIGH	OPEN

1200

FIG. 12

security requirements through the database. As further indicated with respect to FIG. 9, each security requirement may be identified through the database as a compensating control. Accordingly, based on these relationships and selections the list populated in FIG. 12 shows all possible compensating controls that could be implemented to mitigate threats that are present in the diagrammed system, application or process.

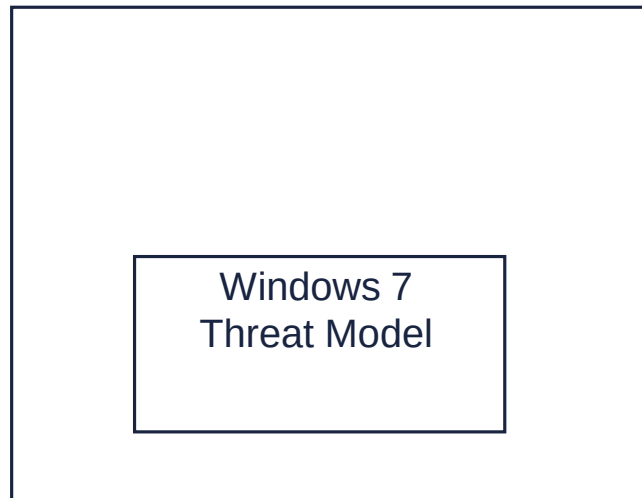
EX-1001 ('008) at 21:1-8

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Summary of the '008 Patent

Key Concept No. 3: Nesting a Threat Model in Another Threat Model

Windows Laptop Threat Model



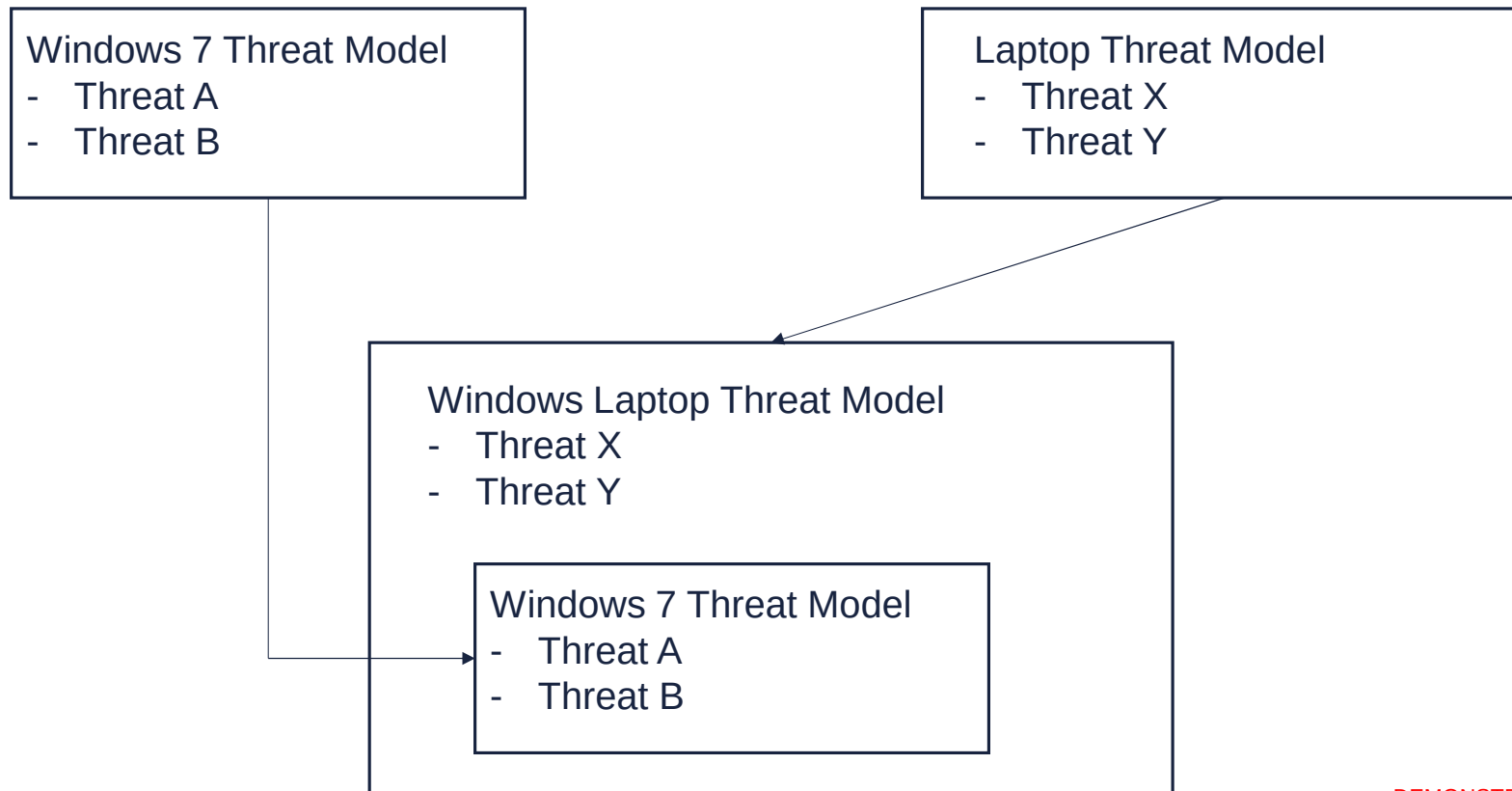
Each component group may thus be redefined as a discrete “component” and may then be included as a single icon in the toolbox menu. By non-limiting example, referring to FIG. 10, the WINDOWS 7 component group could be defined as a component, then the user could, in another diagram (or the same diagram), select and add a WINDOWS 7 component to the diagram to import into the diagram and associated threat model the threats associated with the WINDOWS 7 threat model. That same could be done for the LAPTOP component group. Accordingly, a component group and associated threats added to a diagram may in turn already include other nested/chained threat models therein, so for example if a user defined a laptop component group such as that in FIG. 10 as a “WINDOWS LAPTOP” component then, when a user later adds a WINDOWS LAPTOP element to a diagram/threat model by selecting a WINDOWS LAPTOP component from the toolbox and dragging it onto the diagram, the threats associated with the laptop itself, as well as the nested/chained threats associated with the included WINDOWS 7 threat model, are automatically included in the threat model for the then displayed diagram.

EX-1001 ('008) at 20:37-58, Fig. 10

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

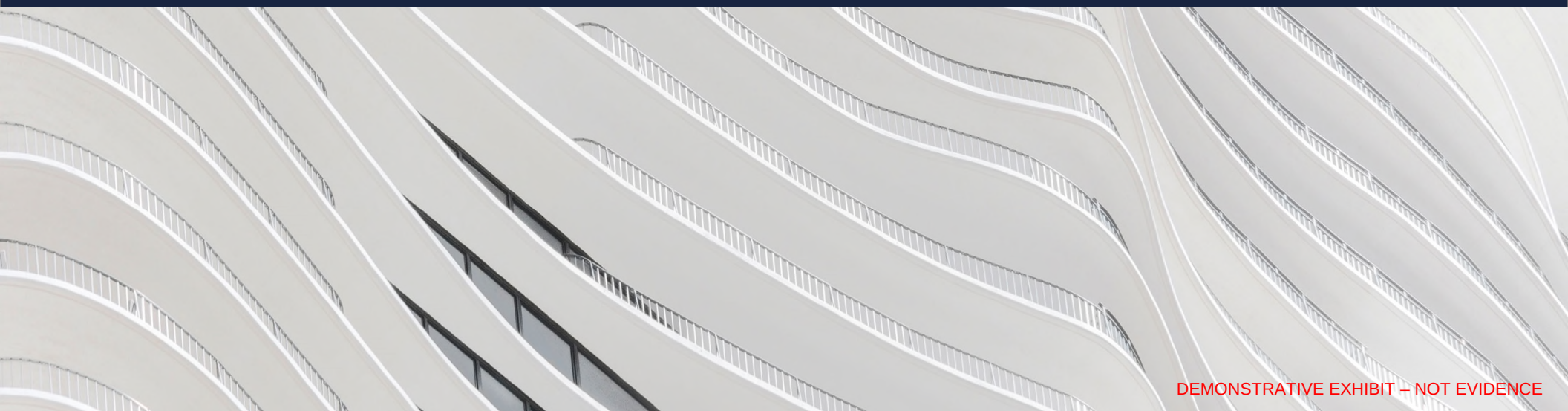
Summary of the '008 Patent

Key Concept No. 3: Nesting a Threat Model in Another Threat Model



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Claim Construction



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Claim Construction

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

Petitioner’s Proposed Construction	PO’s Proposed Construction
“modify or change the first threat model by adding to it a second threat model associated with the component group”	“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”

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Claim Construction

“threat model components” (AGREED)

Petitioner’s Proposed Construction	PO’s Proposed Construction
“a potential relevant source for one or more threats”	“a potential relevant source for one or more threats”

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

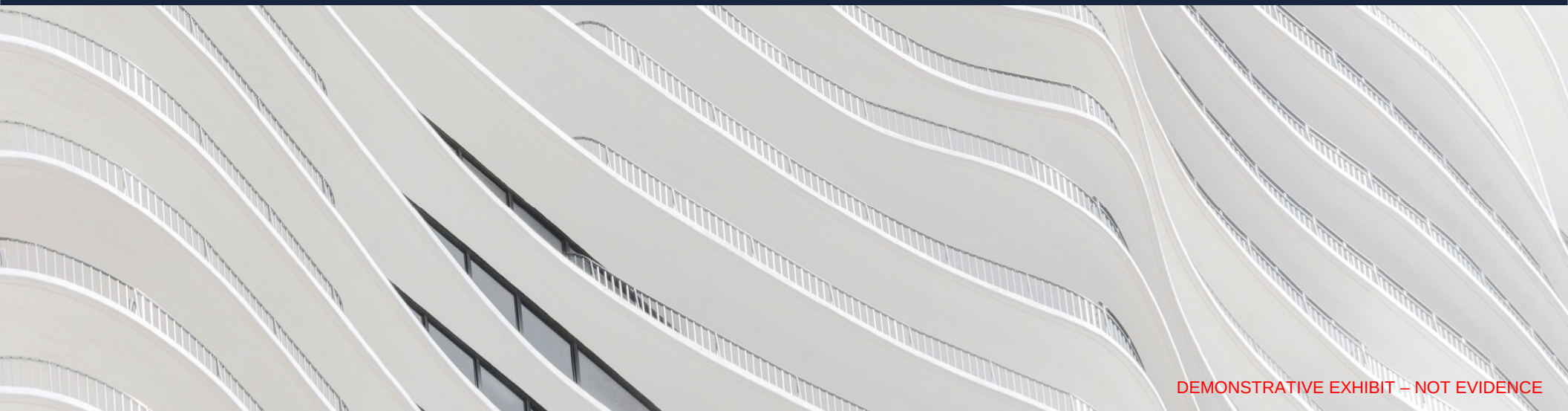
Claim Construction

“attack paths”

Petitioner’s Proposed Construction	PO’s Proposed Construction
“the routes from all potential attackers to a selected asset are the ‘attack vectors’ or attack paths to that asset.”	(no construction offered)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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.

EX-1001 claim 1.

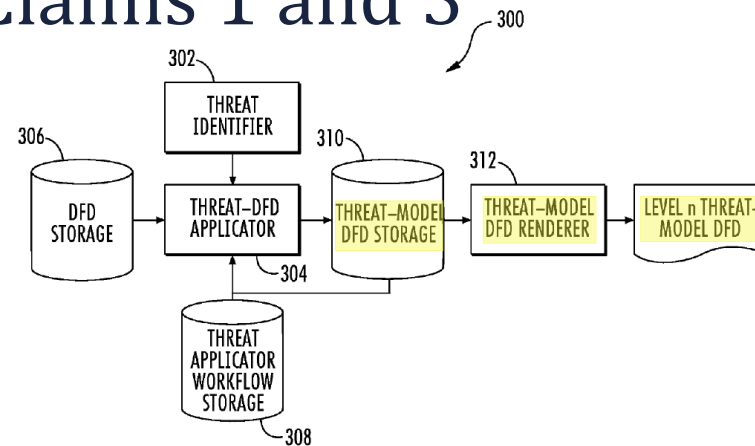


FIG. 3

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 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. And

EX-1004 (Jones) at 6:15-23.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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.

EX-1001 claim 1.

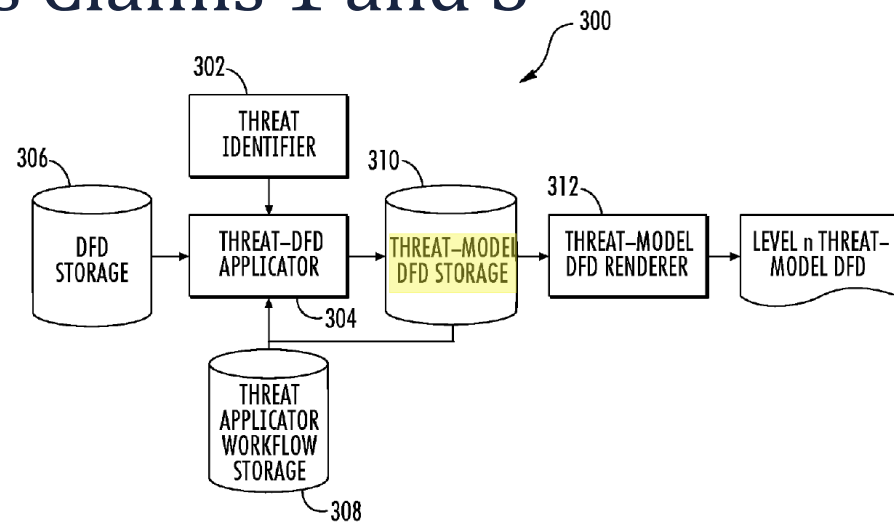


FIG. 3

with the DFD creator. As described herein, information and other data may be formatted and stored in any of a number of different manners, and hence, their storage may be of any of a number of different types. Examples of suitable types of storage as described herein include file storage, database storage, cloud storage or the like.

EX-1004 (Jones) at 8:4-10.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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.

EX-1001 claim 1.

(57)

ABSTRACT

A system is provided for modeling and analysis of cybersecurity threats may include a data flow diagram (DFD) creator, threat indicator and threat analyzer. The DFD creator may identify elements of an information system, and compose a DFD including nodes and edges representing components and data flows of the information system. The threat indicator may identify a cybersecurity threat to a particular element of the information system, and add a secondary node representing the cybersecurity threat to the DFD to thereby produce a threat-model DFD for the information system. In metadata associated with the nodes, edges and secondary node, the DFD creator and threat indicator may provide structured information including attributes of the components, data flows and cybersecurity threat. And the threat analyzer may perform an analysis of the cybersecurity threat based on the threat-model DFD and metadata associated with the nodes, edges and secondary node thereof.

EX-1004 (Jones) at 8:4-10.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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.

EX-1001 claim 1.

The threat analyzer may be configured to perform an analysis of the cybersecurity threat based on the threat-model DFD and metadata associated with the nodes, edges and secondary node thereof. In some examples, this may include the threat analyzer being configured to identify a measure of current risk of the cybersecurity threat to a particular element, and identify a suggested mitigation implementable to reduce the measure of current risk to a lower, measure of residual risk.

EX-1004 (Jones) at 2:33-42.

Numbering for this table – this does not correspond to numbering in the Visio diagram.	Security controls that are recommended to bring the Current Risk rating lower.	Risk given that suggested mitigations are implemented.	The data flow diagram (DFD) element(s) that the threat applies to.	Additional clarifying information. If a finding is preliminary, meaning it needs further research indicate "Preliminary" here.	Use to note whether the review process has resulted in acceptance of this threat and associated impact and risk ratings.
REF #	SUGGESTED MITIGATIONS	RESIDUAL RISK	APPLIES TO	REMARKS	REVIEW STATUS
1	Encrypt client-server connections	Medium	Data flows between client app and server.	This is an information disclosure threat that may lead to a follow-on threat of spoofing threat.	Reviewed
2	Protect RPC connections with a protocol that provides integrity-protection (like SSL/TLS)	Medium	Master-to-Backup data flow		Likelihood rating not agreed
3	Fix buffer overflow.	Medium	Login process	CVSS rating of threat indicated high difficulty to reproduce, which is why likelihood is rated Medium	Not Reviewed
4	Use strong two-factor authentication.	Low	Database system	Preliminary: <Describe why finding is preliminary>	Waiting to clear Preliminary status
5	Implement a failover server in the same datacenter as primary server. Implement regional failover server.	Medium	Web server Application server	Preliminary: <Describe why finding is preliminary> Regional failover needed to bring residual risk to Low.	Waiting to clear Preliminary status
6	Background check	Low	Top level sys admins	Not a traditional STRIDE threat. Improper admin designation could result in all STRIDE threats.	Reviewed
7	Log admin success and fail actions.	Low	Application Server		Reviewed
8	Turn on host-based FW	Low	Web server	Type is "Undetermined" as the vulnerability is very general.	Not Reviewed

● YELLOW ● GREEN

FIG. 10B

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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.

EX-1001 claim 1.

As shown in FIG. 7, in some examples, the GUI 700 may include a workspace 702 for composition of a level n DFD from shapes representing its nodes and edges. In some

EX-1004 (Jones) at 18:44-46.

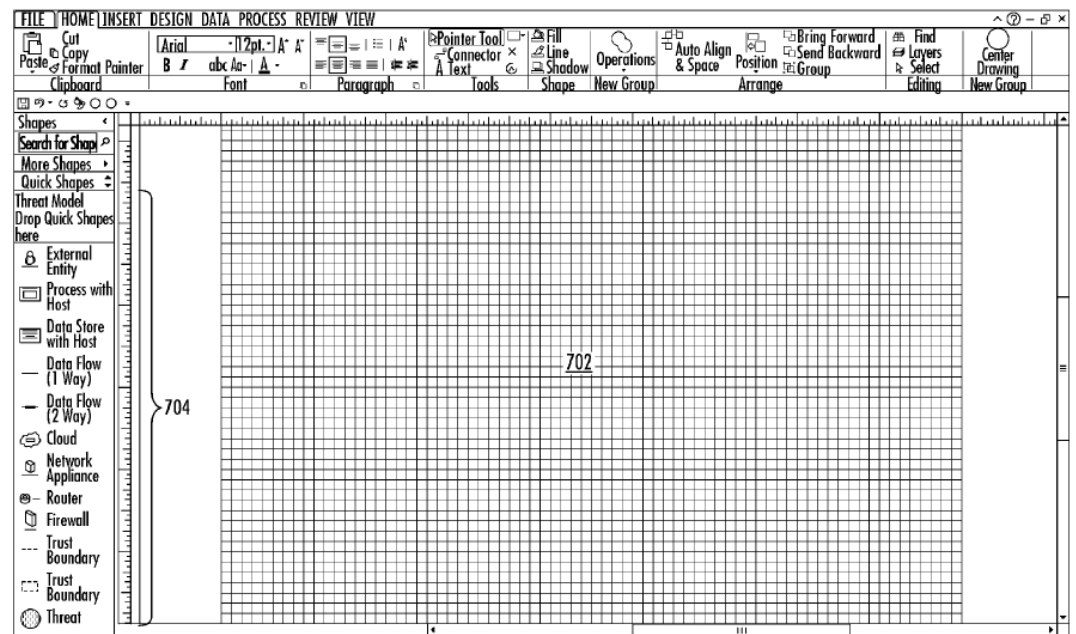


FIG. 7

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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.

EX-1001 claim 1.

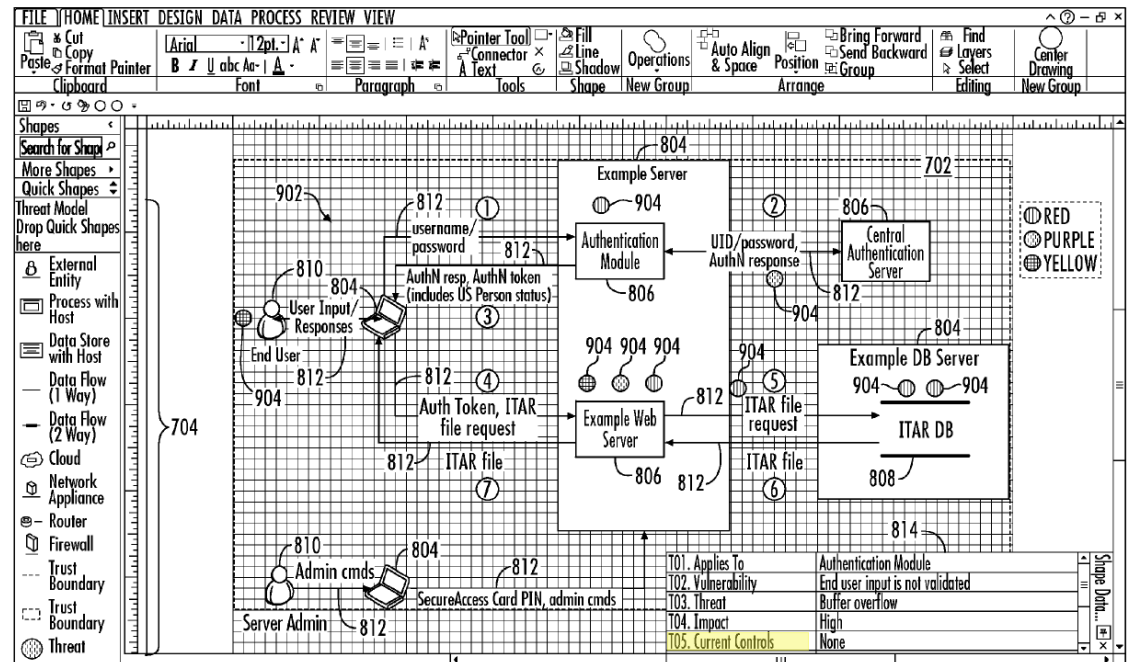


FIG. 9

ments may be entered for their shapes. In some examples, a window 814 may be recalled for each of the shapes. And in this window, data for a shape and thus attributes of an element may be entered, and thereby included as structured information in metadata associated with the shape (and thus node or edge of the DFD). FIG. 8 illustrates an example in

EX-1004 (Jones) at 18:65-19:3.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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.

EX-1001 claim 1.

The information system may include components such as hosts, processes, data stores and/or external entities, and data flows between those components. In some examples, a process may be identified along with the host on which the process is configured to run; and similarly, in some examples, a data store may be identified along with the host 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 (Jones) at 5:4-19.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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.

EX-1001 claim 1.

In some examples it may be desirable to look deeper into one or more components of the information system, such as to provide a more thorough analysis of those components or 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 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. And again, the threat indicator 108 may be applied to 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. Or instead of modifying the existing threat-model DFD, in some examples, the DFD creator and threat indicator may begin again to compose a new DFD and threat-model DFD for this level of the hierarchy. 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.

EX-1004 (Jones) at 6:12-34.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1: Jones Anticipates Claims 1 and 3

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 claim 3.

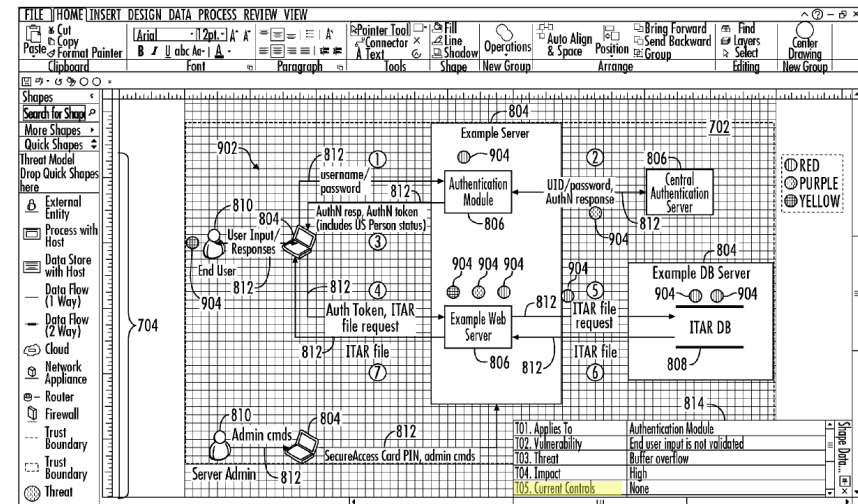
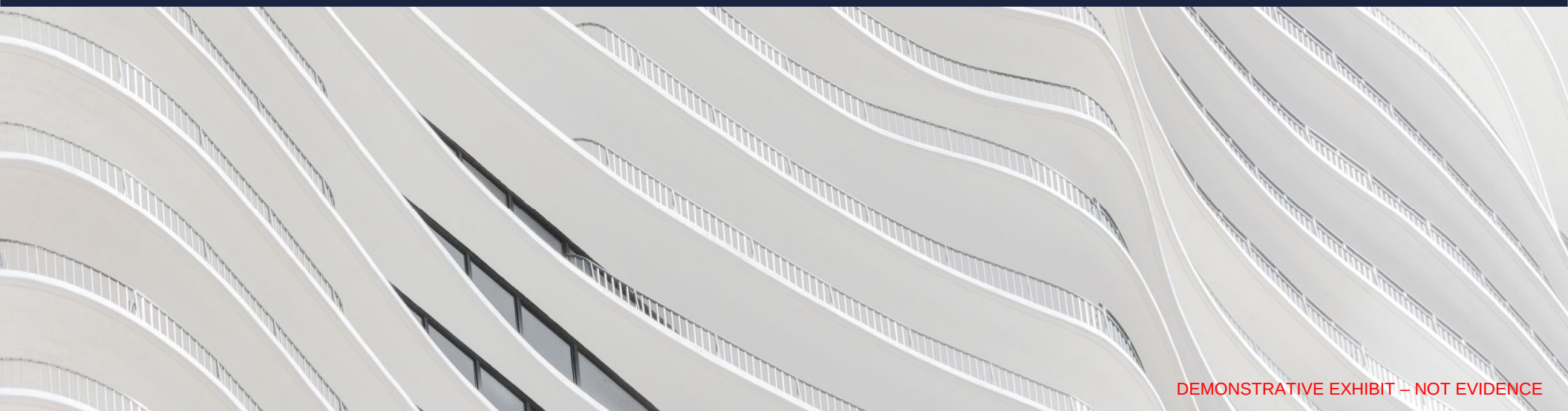


FIG. 9 illustrates the GUI including a level n threat-model DFD 902 produced from the level n DFD 902 and further including a number of shapes for cybersecurity threats 904 to various elements of the information system modeled by the DFD. Similar to elements of the information system, as or after the cybersecurity threats (or rather their shapes) are placed in the workspace 702, attributes and even further attributes of the cybersecurity threats may be entered for 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 (Jones) at 19:10-23.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious

Dependent Claim 2 and Limitation 12[e]

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, claim 2

In some embodiments, the threat modeling layer visualizes each security threat as a threat actor, a threat target and a displayable vector connecting the threat actor to the threat target. At least one of the threat actor or the threat agent is a component of the map. The displayable vector can visualize an attack methodology by the threat actor on the threat target.

EX-1005, 2:36-42

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious

Dependent Claims 6, 7, 13, and 14

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

EX-1001, claim 6

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

EX-1001, claim 7

The GUI of the IOE preferably includes a variety of interactive functions for the user. One such interactive function is path highlighting, described herein with reference to FIG. 9. The user clicks on an object in the topology on the screen and the View then highlights the upstream and downstream flows into and out of the object selected. The highlighting is preferably accomplished by using the thicker line weighting on the Flow Objects in different color than normally used for lines. Clicking again on the object toggles this feature off. Paths upstream and downstream from up to six objects can be toggled on at the same time. A different highlighting color may be used for each. The GUI further permits selection of multiple objects for path highlighting, as shown in FIG. 10. The Path Highlight can be converted into a Report by clicking a report icon 902 on the screen. Clicking this icon prompts a box to appear asking the user if they would like the Upstream Paths, Downstream Paths or both. Following this selection, the user is asked to select which object classes they wish to include in the report. Following this selection the user is asked which Characteristics of the Object Classes selected would they like on the report.

EX-1006 at 12:29-35

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious

Dependent Claim 8 and 15

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, claim 8

The GUI of the IOE preferably includes a variety of interactive functions for the user. One such interactive function is path highlighting, described herein with reference to FIG. 9. The user clicks on an object in the topology on the screen and the View then highlights the upstream and downstream flows into and out of the object selected. The highlighting is preferably accomplished by using the thicker line weighting on the Flow Objects in different color than normally used for lines. Clicking again on the object toggles this feature off. Paths upstream and downstream from up to six objects can be toggled on at the same time. A different highlighting color may be used for each. The GUI further permits selection of multiple objects for path highlighting, as shown in FIG. 10. The Path Highlight can be converted into a Report by clicking a report icon 902 on the screen. Clicking this icon prompts a box to appear asking the user if they would like the Upstream Paths, Downstream Paths or both. Following this selection, the user is asked to select which object classes they wish to include in the report. Following this selection the user is asked which Characteristics of the Object Classes selected would they like on the report.

EX-1006 at 12:29-35

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious

Dependent Claim 9 and 16

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, claim 9

The GUI of the IOE preferably includes a variety of interactive functions for the user. One such interactive function is path highlighting, described herein with reference to FIG. 9. The user clicks on an object in the topology on the screen and the View then highlights the upstream and downstream flows into and out of the object selected. The highlighting is preferably accomplished by using the thicker line weighting on the Flow Objects in different color than normally used for lines. Clicking again on the object toggles this feature off. Paths upstream and downstream from up to six objects can be toggled on at the same time. A different highlighting color may be used for each. The GUI further permits selection of multiple objects for path highlighting, as shown in FIG. 10. The Path Highlight can be converted into a Report by clicking a report icon 902 on the screen. Clicking this icon prompts a box to appear asking the user if they would like the Upstream Paths, Downstream Paths or both. Following this selection, the user is asked to select which object classes they wish to include in the report. Following this selection the user is asked which Characteristics of the Object Classes selected would they like on the report.

EX-1006 at 12:29-35

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious

Dependent Claim 10 and 17

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.

EX-1001, claim 10

In embodiments of the present system, there are preferably four modes for the user to interact with the IOE via a Graphical User Interface (GUI): 1) a View mode, where the user can view any section of the topology and Characteristics by Object; 2) a Modify mode, where the user can add, change and delete Objects or Characteristics; 3) a Compare mode, where the user can visualize the difference between two diagrams; and 4) a Query mode, where the user can interrogate the topology and Characteristics using standard queries and user-generated queries (script writing). Query results can be tabular (reports) or diagrammatic results in which case the diagram will appear in the View Box. Each mode brings up a different screen format. The portion of the GUI that the user sees is referred to herein as the “screen” as opposed to the logic which dictates what appears on the screen which would be the unseen parts of the GUI.

Turning to FIGS. 2 and 3, an exemplary GUI for a View mode is now described, in accordance with an embodiment. The screen contains a view box 202 that occupies most of the screen. Within the view box the user is presented with the topology to view, modify or compare. The view box is view-only in the View and Compare modes, while it is interactive in the Modify mode.

EX-1006, at 11:42-56

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 2: Jones, Zheng, and Keenan Render Claims 1-20 Obvious

Dependent Claim 19

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, claim 19

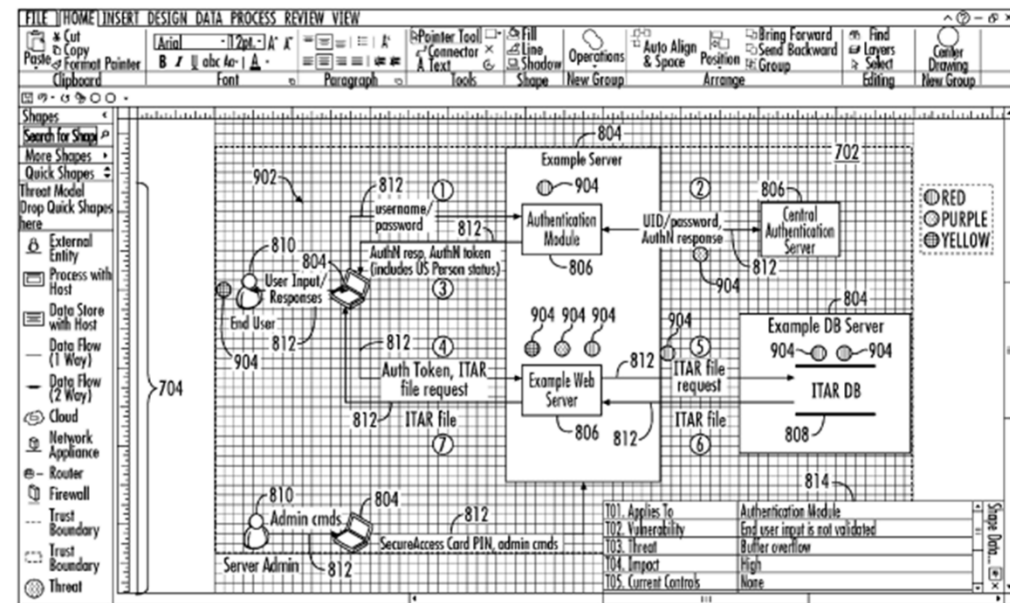
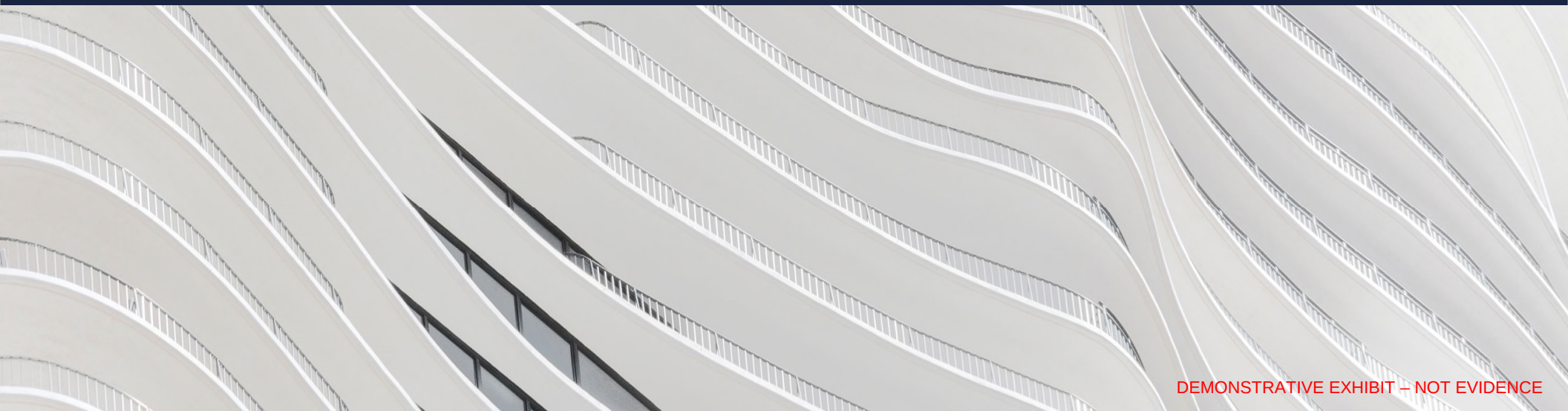


FIG. 9

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 3: Ground 2 References and Yu Render Claims 1-20 Obvious



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 3: Ground 2 References + Yu

compensating controls limitations of claims 1, 11, 20

Claim 1 Excerpt:

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;

With a focus on finding compensating controls, this invention provides a resource-centric threat modeling system that allows resource owners to create a threat model while requiring only basic familiarity of the resource's functions and interactions with other resources. In addition, this invention enables resource owners to match the strength of controls against the frequency of attack and the magnitude of impact from the identified threat vectors to ensure that the controls can sufficiently mitigate the impact in accordance with the resource owner's level of risk tolerance.

EX-1006 (Yu) at 5:54-63.

blocks 212 and 214). In one aspect, the graphical user interface may include one or more categories associated with each of the one or more controls. For example, the

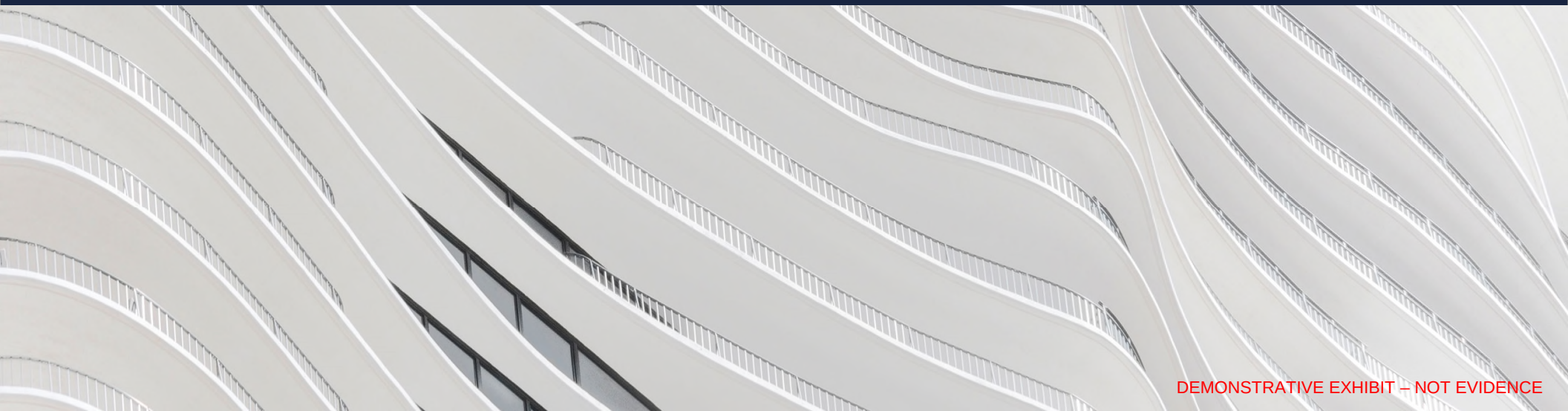
EX-1006 (Yu) at 5:12-14.

effect of the threat on the internal resource. In some embodiments, the graphical user interface may include a recommendation interface including a recommendation for one or more additional controls for implementation. In some

EX-1006 (Yu) at 5:26-28.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 4: Ground 3 References and Reith Render Claims 1-20 Obvious



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 4: Ground 3 References + Reith

threat model chaining limitations of claims 1, 11, 20

Claim 1 Excerpt:

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.

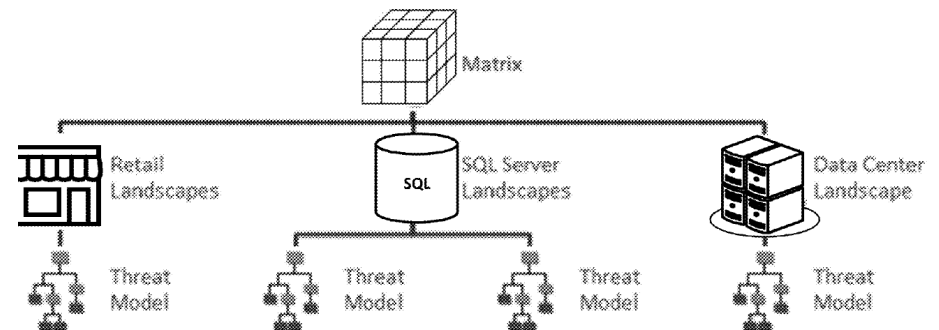


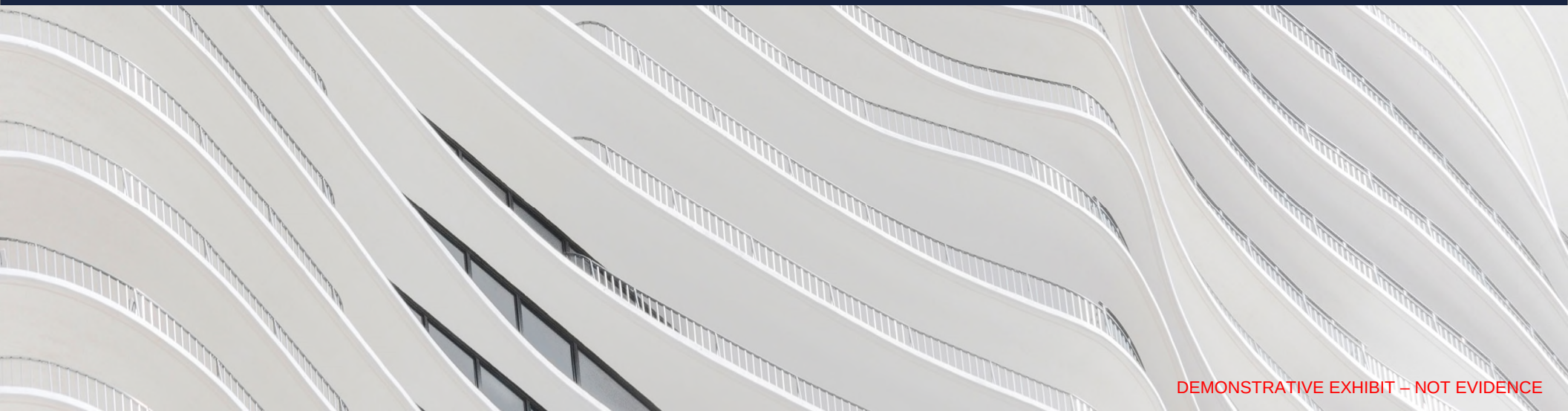
Figure 4

A “threat matrix” is comprised of a set of “threat landscapes” and a threat landscape is comprised of a set of 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

EX-1008 (Reith) at 4:30-35.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 5: Ground 4 References and Knowledge of POSITA Render Claims 5-8 and 13-15 Obvious



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 5: Ground 4 References + POSITA Knowledge

togglng limitations of claims 5-8, 13-15

133. In my opinion, to the extent it is found that the combined system of Jones, Zheng, Keenan, Yu, and Reith do not disclose the togglng limitations of claims 5, 6, 7, 8, 13, 14, 15, that limitation would have been known to a POSITA, and those claims are still rendered obvious by further combining that system with the knowledge of a POSITA. A POSITA would understand that togglng an item displayed in a graphical user interface display was a commonly known technique in user interface design, both within and outside of the threat modeling space. The ability for a user to toggle an item on display is known to be advantageous because, for example, it allows a user to focus on particular concepts within the display and/or it allows a user to view a less cluttered display. In so applying togglng to the system of Jones, Zheng, Keenan, Yu, and Reith a POSITA would arrive at the togglng limitations 5-8 and 13-15.



EX-1003 (Hurlbut Declaration) at ¶ 133.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Thank you

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE