

SECURITY REQUIREMENTS		NAME	PROPERTIES
NAME	LABELS		CODE SNIPPETS
<input type="text"/>	<input type="text"/>	DESCRIPTION	CODE REVIEWS
ENCRYPTION: USE ONLY STR...	AZURE LIB...		
ENCRYPTION: ENSURE RAND...	DOM...		
INPUT VALIDATION WITH...	HARDWARE...		
TM - INPUT VALIDATION	JAVA,INI...	IS COMPENSATING CONTROL ☐	
USING SSL	CERTS...		
KEY MANAGEMENT: ENSU...	OWASP...		
TLS: PREVENT CACHING OF...			
CERTIFICATES: USE AN APP...	CERTS...		
ADD FIREWALL RULES	EVENT,TO,...		
HOST INTEGRITY CHECKING	TO,SSE...		
SECURE BROWSERS	SCRIPT,LOG...		
OUTPUT ENCODING			
APPLY PATCHES	XSS,REL...		
DISABLE HTTP TRACE	INI,HTTP...		

9
G
H

999

FIG. 10

MITIGATIONS				
DRAG A COLUMN HEADER AND DROP IT HERE TO GROUP BY THAT COLUMN				
THREAT	SOURCE	RISK	STATUS	
FILE MANIPULATION	FILE SYSTEM	MEDIUM	OPEN	
ACCESSING EXECUTABLE FILES	FILE SYSTEM	VERY HIGH	OPEN	
CREATE FILES SAME NAME AS...	FILE SYSTEM	VERY HIGH	OPEN	
MAN IN THE BROWSER	IE 11	VERY HIGH	OPEN	
MANIPULATING CONFIG FILE	FILE SYSTEM	VERY HIGH	OPEN	
FORCE USE OF CORRUPT FILE	FILE SYSTEM	VERY HIGH	OPEN	
MANIPULATING INPUT TO CALL	FILE SYSTEM	HIGH	OPEN	
FILE MANIPULATION	FILE SYSTEM	MEDIUM	OPEN	
ACCOUNT FOOTPRINTING	IE 11	VERY HIGH	OPEN	
AUTOMATION ATTACK	IE 11	VERY HIGH	OPEN	
PHYSICAL THEFT	LAPTOP	VERY HIGH	OPEN	
PHYSICAL THEFT	LAPTOP	VERY HIGH	OPEN	
BLUEJACKING	BLUETOOTH PORT	VERY HIGH	OPEN	
PHISHING	OUTLOOK 2010	VERY HIGH	OPEN	
SPAM	OUTLOOK 2010	VERY HIGH	OPEN	
DNS CACHE POISONING	EMAIL SERVER	VERY HIGH	OPEN	
MITIGATE CLOSE				

1100

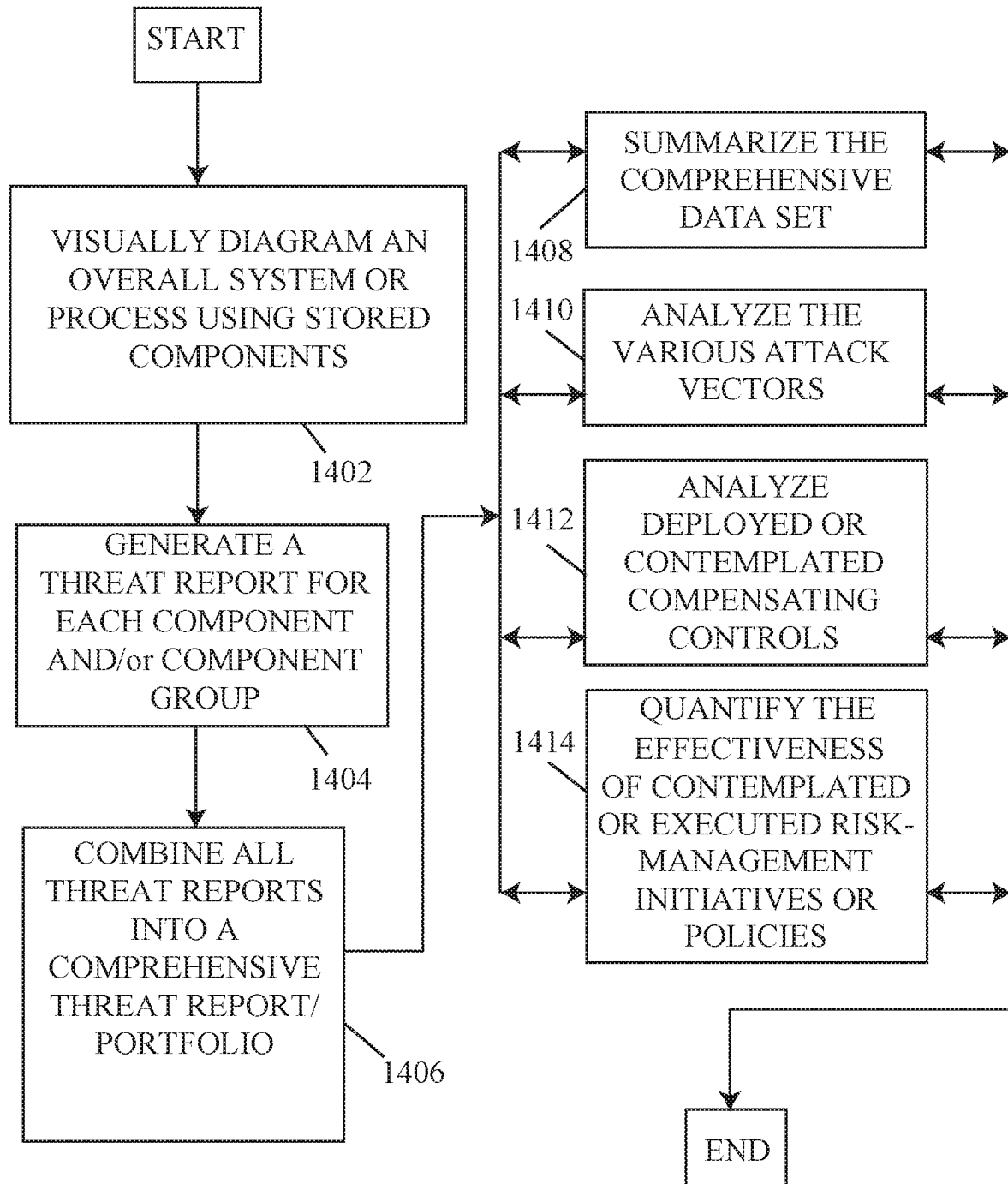
FIG. 11

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	TCP 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	
MCAFEES 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

FIG 13

**FIG. 14**

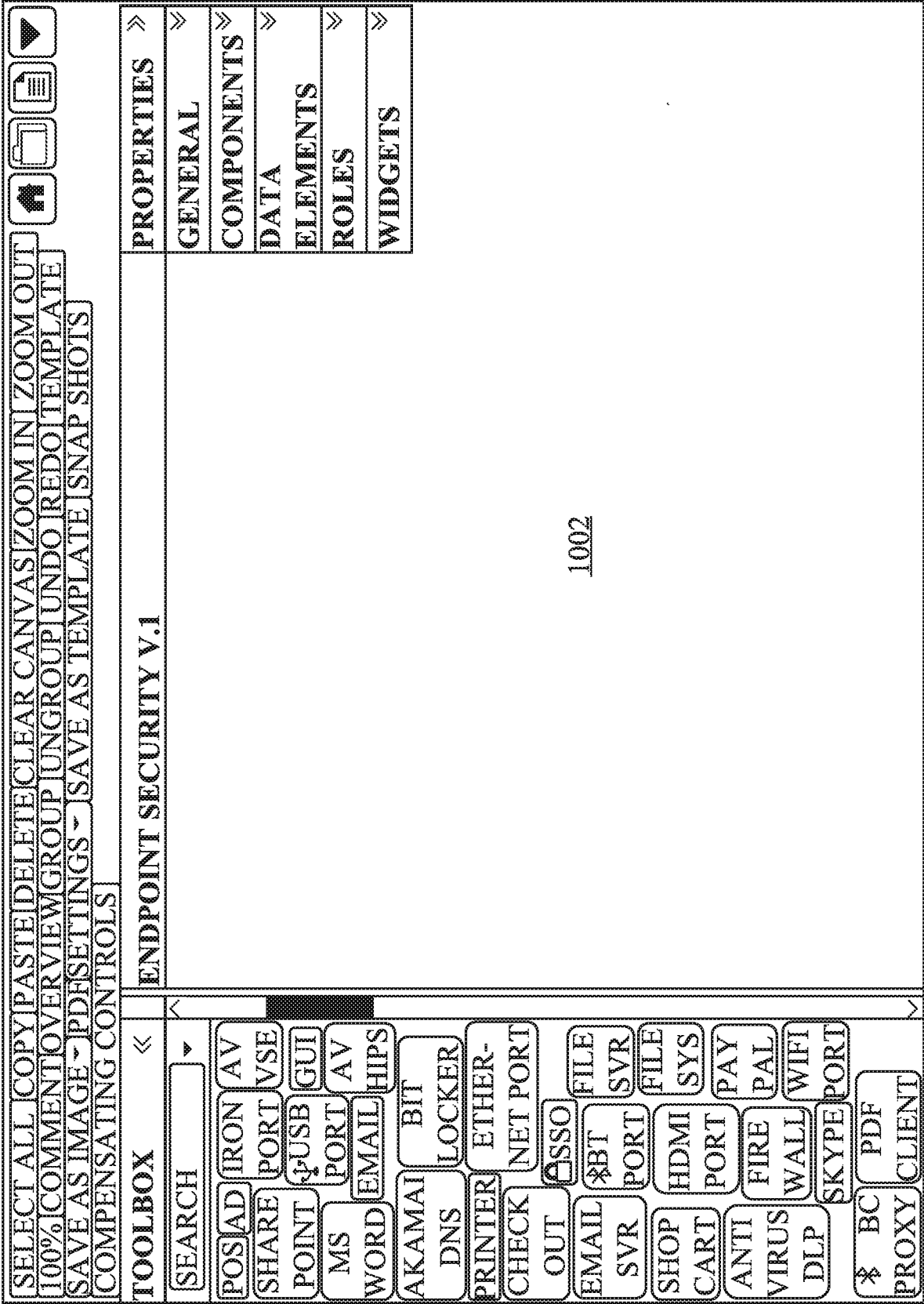


FIG. 15

1000

16/22

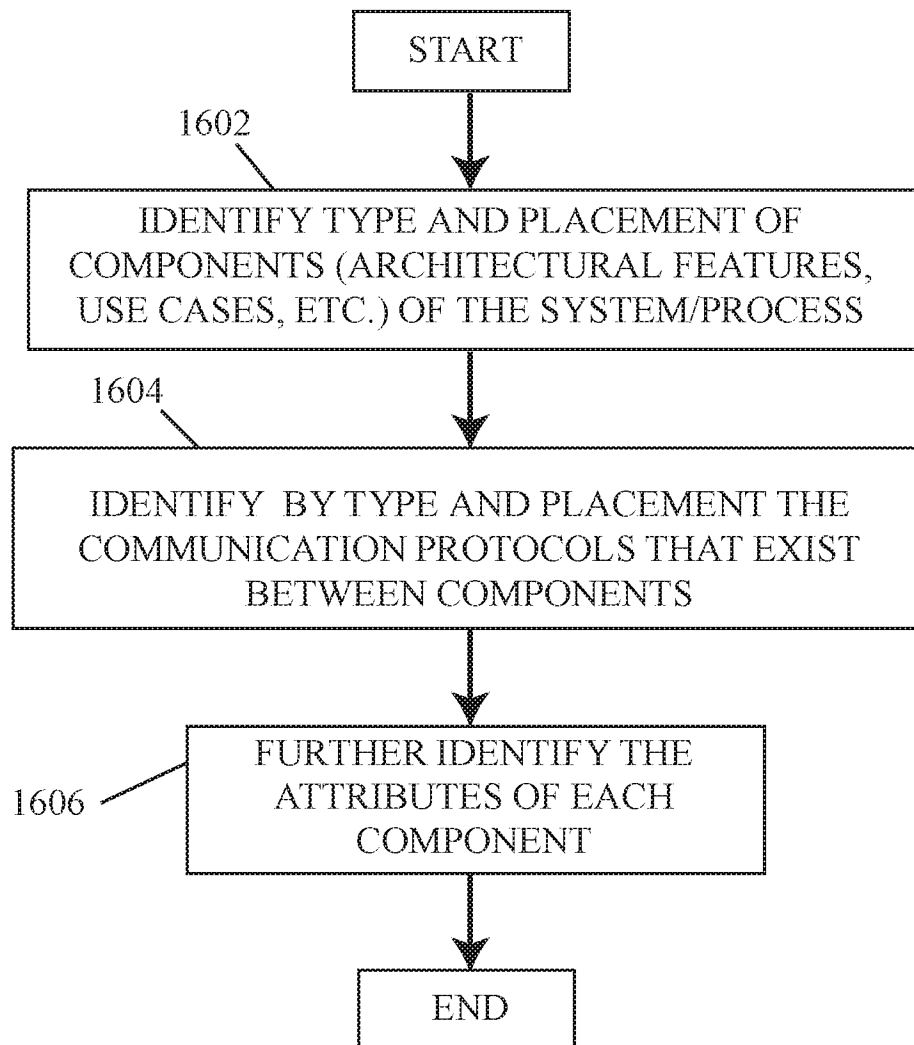


FIG. 16

17/22

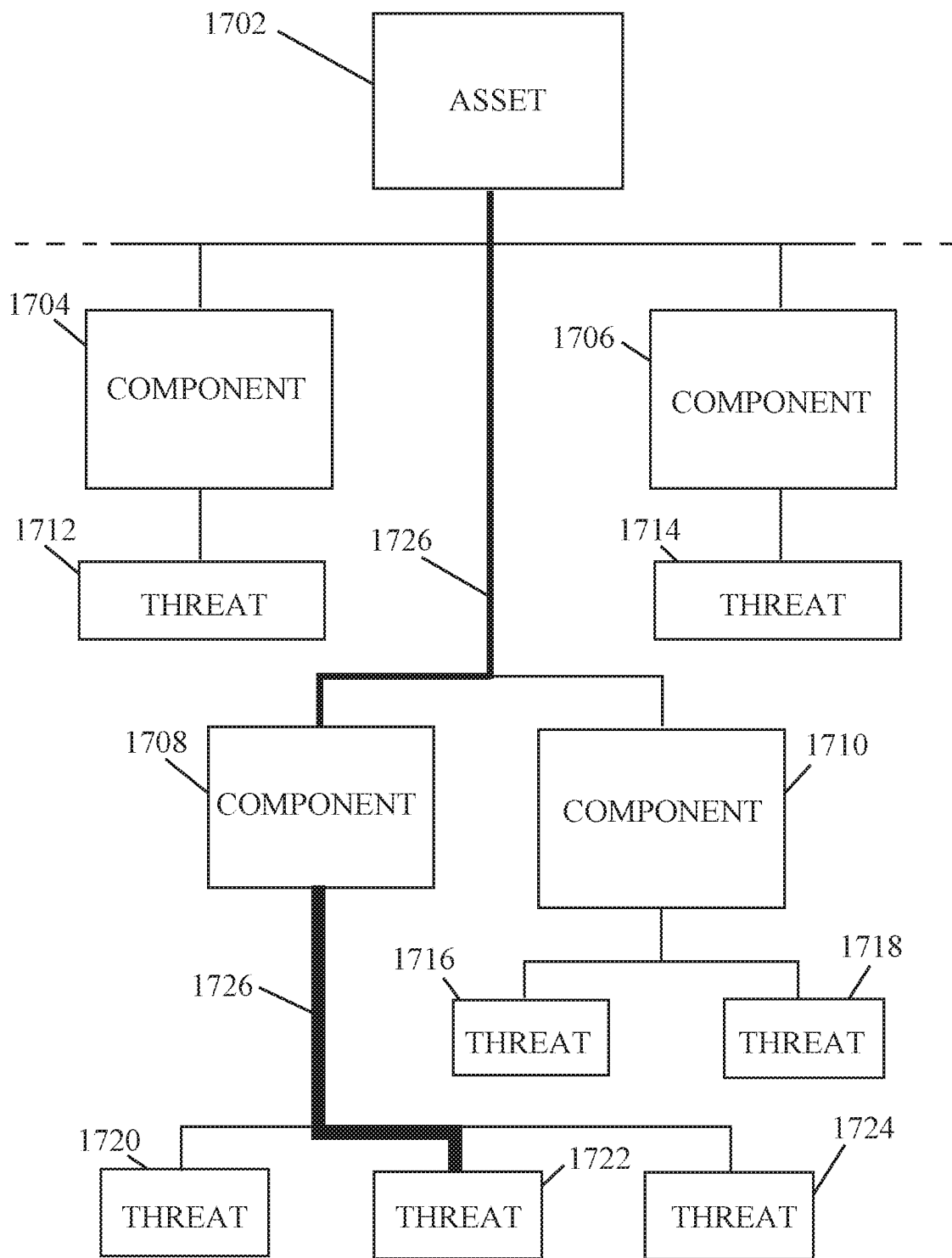


FIG. 17

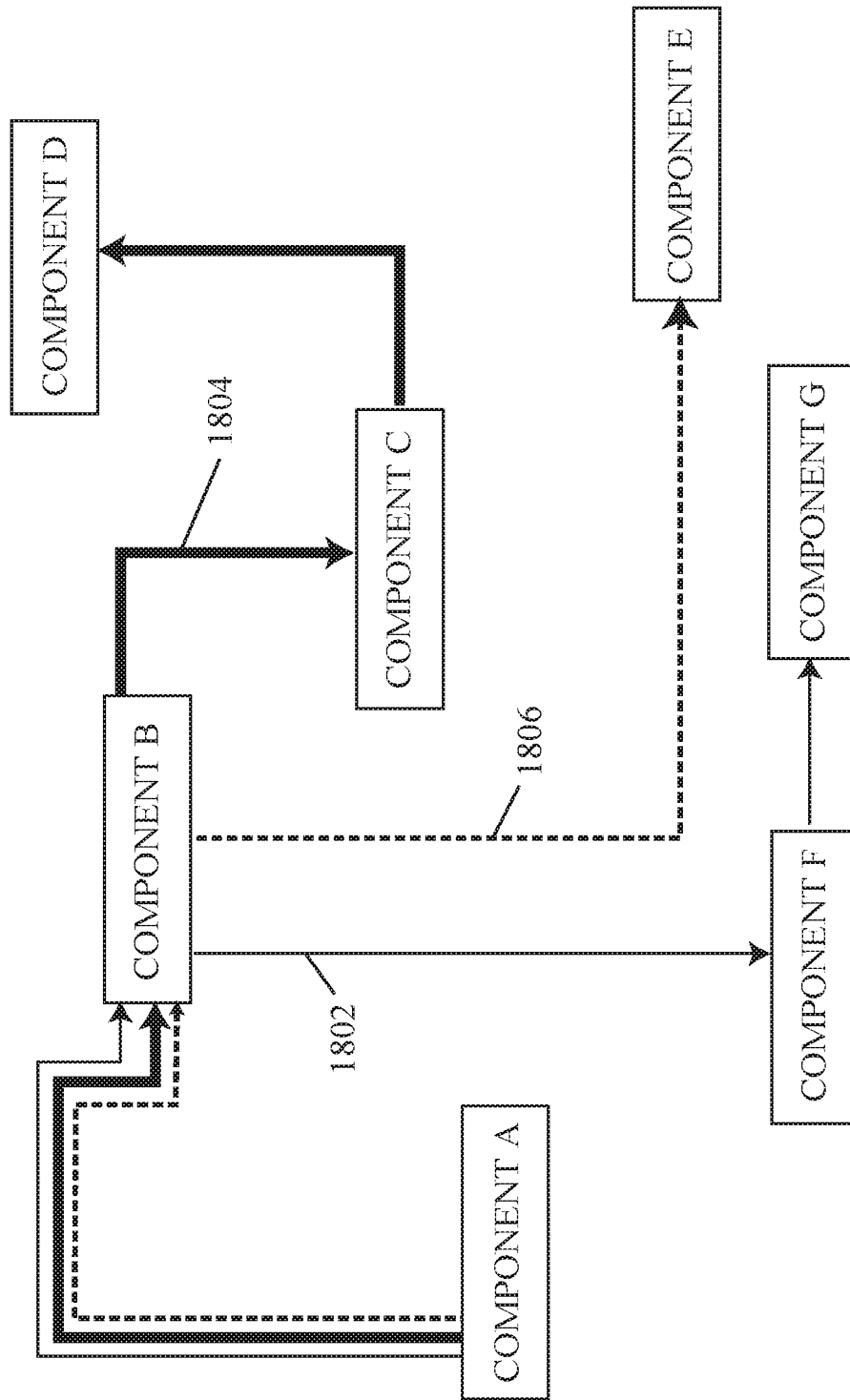


FIG. 18

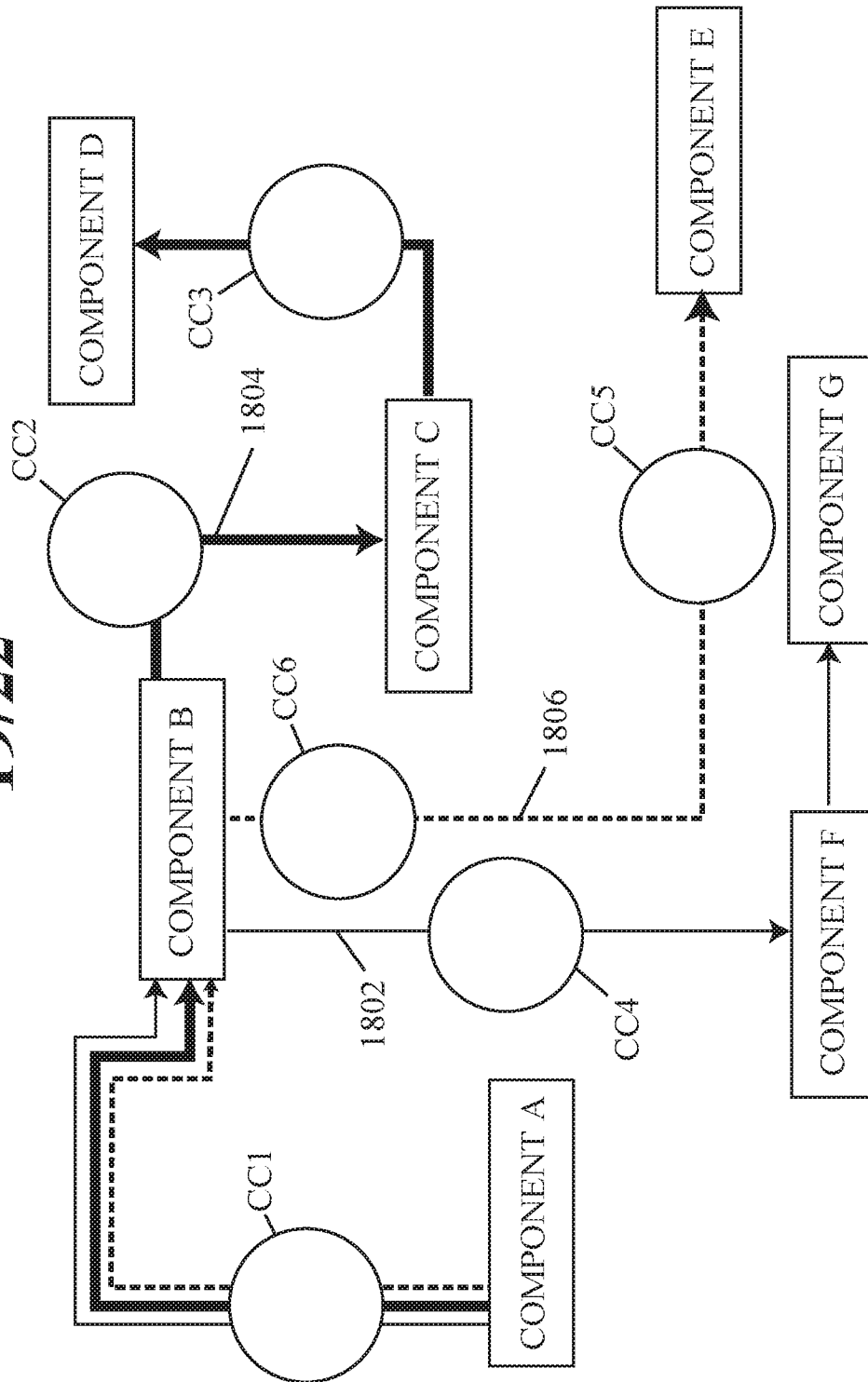


FIG. 19

20/22

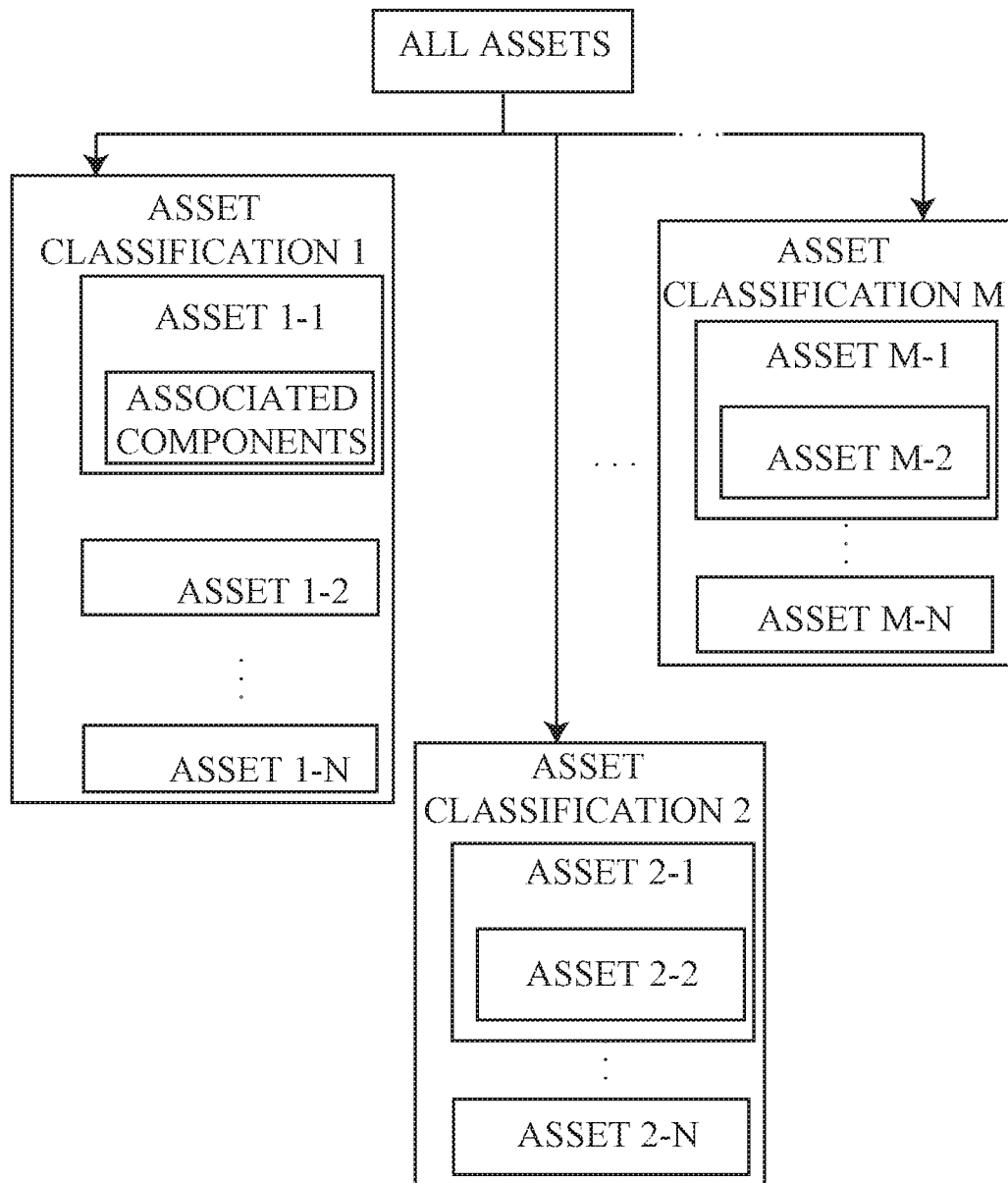


FIG. 20

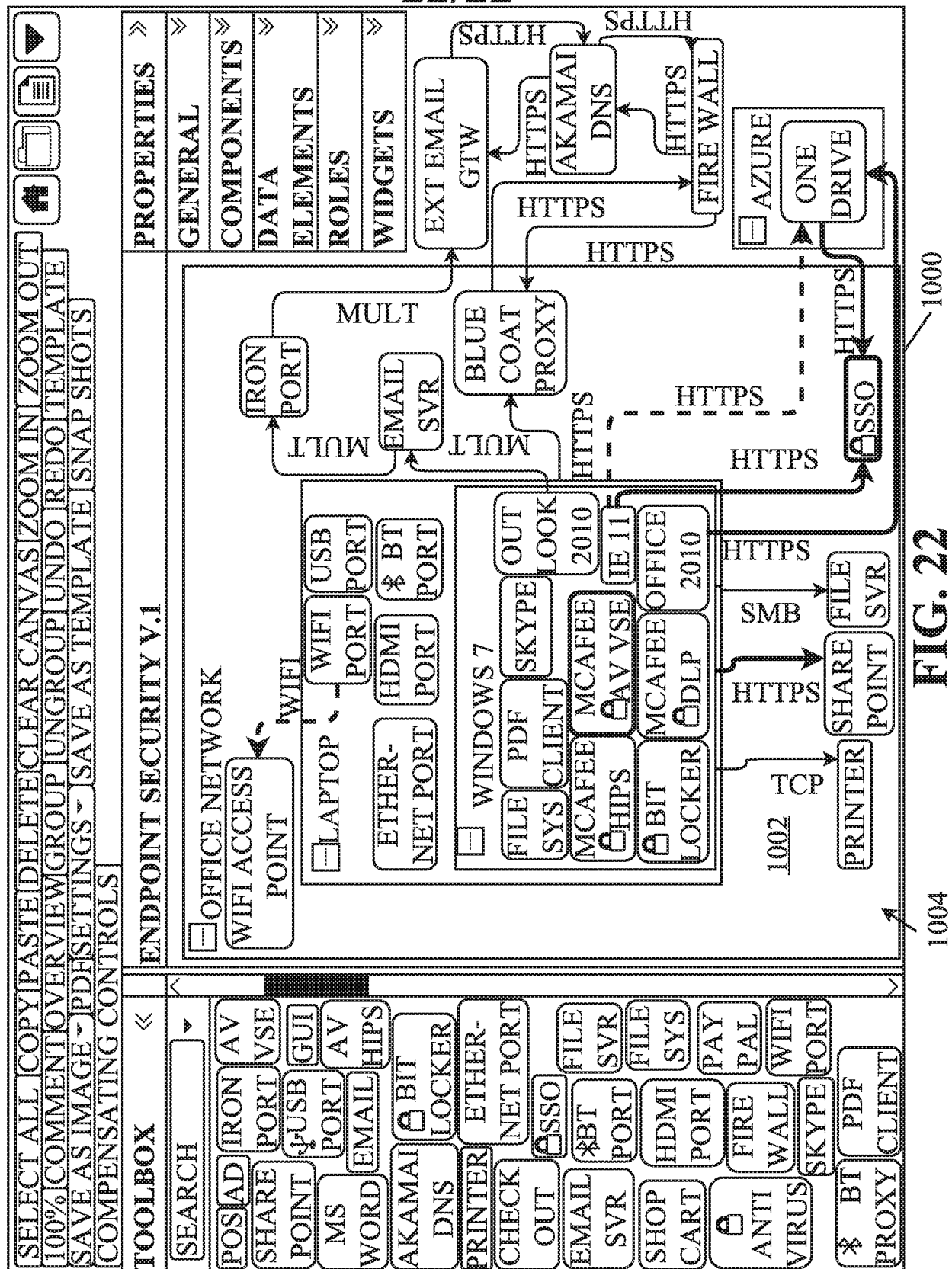


FIG. 22

ABSTRACT OF THE DISCLOSURE

Threat model chaining methods include providing one or more databases including a threat model components, threats, each threat associated with at least one of the threat model components, and compensating controls, each compensating control associate with one of the threats, providing a diagram interface configured to display a relational diagram defining a first threat model, and configuring the diagram interface to add a component group to the first threat model include in it a second threat model. Attack simulation methods include providing the one or more databases and diagram interface and configuring the diagram interface to visually display attack paths of threats associated with diagrammed threat model components which compromise a selected threat model component. Attack simulation systems include one or more computing devices coupled with one or more databases configured to store and interrelate threats, threat model components, and compensating controls, and allow diagramming and defining of threat models.

CLAIMS

What is claimed is:

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.
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.
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.

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.
5. 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 one or more attack paths which pass through multiple diagrammed threat model components of the first threat model.
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.
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.

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.

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.

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.

11. The attack simulation method of claim 3, further comprising configuring the diagram interface to receive one or more user inputs to add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.

12. An attack simulation system, comprising:
- one or more computing devices communicatively coupled with one or more databases,
 - the one or more computing devices displaying, on one or more displays of the one or more computing devices:
 - one or more input interfaces configured to, in response to receiving one or more user inputs, store a plurality of user-defined threat model components in the one or more databases, store a plurality of threats in the one or more databases, associate each of the threats with at least one of the threat model components through the one or more databases, store a plurality of compensating controls in the one or more databases, and associate each compensating control with at least one of the threats through the one or more databases, and;
 - a diagram interface configured to, in response to receiving one or more user inputs, diagram one of a system, an application, and a process, the diagram including one or more of the threat model components and one or more of the compensating controls, to define a first threat model, the first threat model including all threats associated through the one or more databases with the diagrammed threat model components;
 - wherein the diagram interface is configured to, in response to receiving a selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.
13. The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving a user input to toggle one of the diagrammed compensating controls (hereinafter “first control”) to an on state, toggle all attack paths mitigatable by the first control to a mitigated display state.
14. The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to receiving a user input to toggle the first control to an off state, toggle all attack paths mitigatable by the first control to an unmitigated display state.
15. The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to receiving one or more user inputs removing the first control from the first

threat model, toggle all attack paths mitigatable by the first control to an unmitigated display state.

16. The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.

17. The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, alter a profile of an attacking component, wherein the alteration alters the visually displayed attack paths.

18. The attack simulation system of claim 12, wherein the one of a system, an application, and a process comprises a computing network.

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.

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.

THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This document is a continuation-in-part application of U.S. Patent App. Ser. No. 15/922,856 titled “Threat Model Chaining and Attack Simulation Systems and Methods,” naming as first inventor Anurag Agarwal, filed Mar. 15, 2018, now pending, which in turn is a continuation-in-part application of U.S. Patent App. Ser. No. 15/888,021 titled “Threat Modeling Systems and Related Methods Including Compensating Controls,” naming as first inventor Anurag Agarwal, filed Feb. 3, 2018, now pending (hereinafter the ‘021 Application), which in turn claims the benefit of the filing date of U.S. Provisional Pat. App. Ser. No. 62/507,691 titled “System and Method of Including Compensating Controls in a Threat Modeling Process,” naming as first inventor Anurag Agarwal, filed May 17, 2017, now expired, and which ‘021 Application also claims the benefit of the filing date of U.S. Provisional Pat. App. Ser. No. 62/527,671 titled “System and Method for Identifying and Analyzing the Potential Attack Surface of a Complex System,” naming first inventor Anurag Agarwal, filed June 30, 2017, now expired, and which ‘021 Application also claims the benefit of the filing date of U.S. Provisional Pat. App. Ser. No. 62/530,295 titled “Method and Apparatus for Early Implementation of Enterprise DevSecOps,” naming first inventor Anurag Agarwal, filed July 10, 2017, now expired, and which ‘021 Application also claims the benefit of the filing date of U.S. Provisional Pat. App. Ser. No. 62/520,954 titled “System and Method for Identifying Potential Threats to a Complex System,” naming first inventor Anurag Agarwal, filed June 16, 2017, now expired, the disclosures of each of which are hereby incorporated entirely herein by reference.

BACKGROUND

1. Technical Field

[0002] Aspects of this document relate generally to threat modeling processes and systems.

2. Background Art

[0003] 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, WA. 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.

[0004] With regards to modeling computing networks, traditional threat modeling systems and methods exist for assessing risk from potential cyber threats at an individual application level without fully accounting for application-application interactions, thereby miscalculating organizational risk. Other systems and methods exist for discovering vulnerabilities to applications deployed in cyber environments by surveying applications. These rely on recognizing previously identified and cataloged vulnerability signatures and are not designed to survey non-application items included in an organization's cyber environment, nor can these systems recognize which threats newly introduced to a cyber system are relevant to security, nor can these systems perform "what-if" scenarios as part of an organization's risk management analysis. Existing methodologies also do not provide for communicating the risks associated with identified threats in a way that non-security experts easily appreciate or understand.

[0005] Accordingly, traditional threat modeling methodologies have the following weaknesses: (1) they are effective in analyzing only single applications operating in isolation on a predetermined infrastructure; (2) they require security subject-matter experts for their creation, use, and maintenance; (3) they are resource-intensive to build and maintain, and; (4) they cannot be effectively used to scale a threat modeling practice to meet the needs of enterprises generating tens of software applications per year. Traditional threat modeling methodologies also cannot be easily integrated into existing agile software development approaches or with DevOps practices, and so are often rejected by agile developers and operational teams as non-productive.

[0006] Existing threat modeling methodologies also do not help organizations understand: (1) the nature of application interactions; (2) the user of shared components; (3) the effect of including third-party elements within the IT ecosystem; (4) the downstream impact should potential threats be realized; (5) the nature of the organization's comprehensive attack surface; (6) the explicit nature of the organization's attacker population; (7) the effectiveness of deployed or contemplated compensating controls; or (8) a means to communicate the potential impact should threats be realized without communicating confidential information or security details which could further expose the organization to risk from potential threats.

SUMMARY

[0007] Embodiments of threat model chaining methods may include: providing one or more databases, the one or more databases including: 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 includes a predefined interrelated group of two or more of the threat model components.

[0008] Embodiments of threat model chaining methods may include one or more or all of the following:

[0009] 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.

[0010] 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.

[0011] Embodiments of attack simulation methods may include: providing one or more databases, the one or more databases including: 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.

[0012] Embodiments of attack simulation methods may include one or more or all of the following:

[0013] Configuring the diagram interface to, in response to receiving one or more user inputs through the one or more interfaces, visually display one or more attack paths which pass through multiple diagrammed threat model components of the first threat model.

[0014] 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.

[0015] 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.

[0016] 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.

[0017] 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.

[0018] 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.

[0019] Configuring the diagram interface to receive one or more user inputs to add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group includes a predefined interrelated group of two or more of the threat model components.

[0020] Embodiments of attack simulation systems may include: one or more computing devices communicatively coupled with one or more databases, the one or more computing devices displaying, on one or more displays of the one or more computing devices: one or more input interfaces configured to, in response to receiving one or more user inputs, store a plurality of user-defined threat model components in the one or more databases, store a plurality of threats in the one or more databases, associate each of the threats with at least one of the threat model components through the one or more databases, store a plurality of compensating controls in the one or more databases, and associate each compensating control with at least one of the threats through the one or more databases, and; a diagram interface configured to, in response to receiving one or more user inputs, diagram one of a system, an application, and a process, the diagram including one or more of the threat model components and one or more of the compensating controls, to define a first threat model, the first threat model including all threats associated through the one or more databases with the diagrammed threat model components; wherein the diagram interface is configured to, in response to receiving a selection of one of the diagrammed threat model components of the first threat model, visually display attack paths of all threats associated with the diagrammed threat model components which compromise the selected threat model component.

[0021] Embodiments of attack simulation systems may include one or more or all of the following:

[0022] The diagram interface may be configured to, in response to receiving a user input to toggle one of the diagrammed compensating controls (hereinafter “first control”) to an on state, toggle all attack paths mitigatable by the first control to a mitigated display state.

[0023] The diagram interface may be configured to, in response to receiving a user input to toggle the first control to an off state, toggle all attack paths mitigatable by the first control to an unmitigated display state.

[0024] The diagram interface may be configured to, in response to receiving one or more user inputs removing the first control from the first threat model, toggle all attack paths mitigatable by the first control to an unmitigated display state.

[0025] The diagram interface may be configured to, in response to receiving one or more user inputs, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.

[0026] The diagram interface may be configured to, in response to receiving one or more user inputs, alter a profile of an attacking component, wherein the alteration alters the visually displayed attack paths.

[0027] The one of a system, an application, and a process may be a computing network.

[0028] The diagram interface may be 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.

[0029] The diagram interface may be 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 includes a predefined interrelated group of two or more of the threat model components.

[0030] General details of the above-described embodiments, and other embodiments, are given below in the DESCRIPTION, the DRAWINGS, and the CLAIMS.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] Embodiments will be discussed hereafter using reference to the included drawings, briefly described below, wherein like designations refer to like elements:

[0032] FIG. 1 is a diagram representatively illustrating an implementation of a threat modeling system (threat model chaining system) (attack simulation system) (system);

[0033] FIG. 2 is a block diagram representatively illustrating an implementation of a threat modeling method;

[0034] FIG. 3 is a block diagram representatively illustrating an implementation of a threat modeling method;

[0035] FIG. 4 is a flowchart representatively illustrating an implementation of a threat modeling method;

[0036] FIG. 5 is a flowchart representatively illustrating an implementation of a threat modeling method;

[0037] FIG. 6 is an implementation of an interface of the system of FIG. 1;

[0038] FIG. 7 is an implementation of an interface of the system of FIG. 1;

[0039] FIG. 8 is an implementation of an interface of the system of FIG. 1;

[0040] FIG. 9 is an implementation of an interface of the system of FIG. 1;

[0041] FIG. 10 is an implementation of an interface of the system of FIG. 1;

[0042] FIG. 11 is an implementation of an interface of the system of FIG. 1;

[0043] FIG. 12 is an implementation of an interface of the system of FIG. 1;

[0044] FIG. 13 is an implementation of an interface of the system of FIG. 1;

[0045] FIG. 14 is a block diagram representatively illustrating an implementation of an attack simulation method;

[0046] FIG. 15 is an implementation of an interface of the system of FIG. 1;

[0047] FIG. 16 is a flowchart representatively illustrating an implementation of a threat modeling method;

[0048] FIG. 17 is an attack tree diagram representatively illustrating an attack path of a threat of a threat model;

[0049] FIG. 18 is a block diagram representatively illustrating attack paths of multiple threats of a threat model;

[0050] FIG. 19 is the block diagram of FIG. 18 with compensated controls added to the diagram;

[0051] FIG. 20 is a block diagram of an asset classification method of an attack simulation method;

[0052] FIG. 21 is an implementation of an interface of the system of FIG. 1, and;

[0053] FIG. 22 is an implementation of an interface of the system of FIG. 1.

DESCRIPTION

[0054] Implementations/embodiments disclosed herein (including those not expressly discussed in detail) are not limited to the particular components or procedures described herein. Additional or alternative components, assembly procedures, and/or methods of use consistent with the intended system and method of including compensating controls in a threat modeling process may be utilized in any implementation. This may include any materials, components, sub-components, methods, sub-methods, steps, and so forth.

[0055] As used herein, the term “input field” includes a “selector.” For example, a button or space on a user interface in which a user may move a cursor to and click to make a selection, and a checkbox field, and other similar fields, as well as alphanumeric input fields, are all “input fields” as used herein.

[0056] The term “compensating control” in implementations herein may be an alternative mechanism to a security requirement or standard issued by a standards-issuing body that is allowed by the standards-issuing body when the security requirement or standard as stated cannot be met by a party due to legitimate technical or documented business constraints.

[0057] In the payment card industry (PCI), as a non-limiting example, compensating controls were introduced in Payment Card Industry Data Security Standard (PCI DSS) 1.0 to give organizations an alternative to security requirements that could not be met due to legitimate technological or business constraints. According to the PCI Council, which was the standards-issuing body issuing the standard (jointly created by the four major credit-card companies VISA, MASTERCARD, DISCOVER, and AMERICAN EXPRESS), compensatory controls in that industry must: (1) meet the intent and rigor of the original stated requirement; (2) provide a similar level of defense as the original stated requirement; (3) be “above and beyond” other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and (4) be commensurate with the additional risk imposed by not adhering to the original stated requirement. Examples of compensating controls for information technology may include: using audit trails and logs for payroll management instead of segregation of duties (having two individuals responsible for separate parts of payroll management); the use of database security applications and services, network access control (NAC), data leak prevention strategies, and e-mail encryption in lieu of comprehensive encryption (i.e., in lieu of converting all electronic data into ciphertext and changing cryptographic keys periodically); two-factor authentication with a change of password every 60 days in lieu of long complex passwords; and so forth.

[0058] Notwithstanding the above, in implementations herein “compensating control” may have a more general definition. For example, in implementations a “security requirement” may be defined as a mechanism for stopping or closing a threat at the source of the threat, and a “compensating control” may be defined as a mechanism for stopping or closing a threat not at the source, but between the source and some protected component (i.e., preventing a threat emanating from a source from reaching a protected component). In other implementations a “security requirement” may be defined as a hardware solution and a “compensating control” may be defined as a software solution, such as a change in the code or software added to a system. In still other implementations a “security requirement” may be generally defined as any solution which is costlier or more time consuming and a “compensating control” may be defined as a solution which is not as secure or sure-proof as the relevant security requirement but which is less cost-prohibitive or time-prohibitive.

[0059] The threat modeling system and related methods discussed herein are implemented using computing devices and/or networks. Referring to FIG. 1, an implementation of a threat modeling system (threat model chaining system) (attack simulation system) (system) 100 is shown. FIG. 1 only shows a representative example, and there are many other contemplated systems that could be used to implement the threat modeling processes. System 100 includes a computing device 102 having a display 104. While the computing device is drawn as a desktop computer it could be a laptop, a mobile phone or tablet, or any other type of computing device. The same goes for all other computing devices shown in the drawings.

[0060] Device 102 is shown communicatively coupled with server 106 which is communicatively coupled with a database (DB) 108. The coupling may be direct, such as through a wired connection, or through a local area network (LAN), or remotely through telecommunication network 110 (which may be the Internet). In some systems the server and database could be housed on the same machine as the computing device 102 using virtualization. In implementations device 102 could be accessed by an administrator of the system to choose settings, add or remove users, add or remove items from the database, and so forth. System 100 only shows one computing device 102, though in implementations the number of computing devices 102 may be scaled up to any number. Likewise, only one server and database are shown, but these also may be scaled up to any number as needed.

[0061] Other computing devices may be included in system 100. Computing device 112 includes display 114 and is an example of a computing device which is communicatively coupled with device 102 both directly (such as through a hardwired or wireless LAN), and coupled

directly with the server (such as through a hardwired or wireless LAN), and also may be coupled with the server and/or the device 102 through telecommunication network 110. System 100 is shown with only one device 112 but in implementations it could be scaled up to any number of devices 112.

[0062] Computing device (device) 116 is an example of a computing device that is not directly coupled with either device 102 or the server but is only coupled thereto through the telecommunications network 110. Nevertheless, device 116 may access the server and database through the telecommunications network. Although only one device 116 is shown, this may be scaled up to any number. Device 116 has a display 118, as shown.

[0063] Also shown are a web server 120 and a remote server (server) 122, each of which may be included in implementations of system 100. By non-limiting example, device 116 may access the server 106 and database through the web server 120, such as by navigating to a uniform resource locator (URL) and providing login credentials. Computing devices 102 and 112 could do the same. Although only one web server is shown, this may be scaled up to any number as needed.

[0064] None of the computing devices shown in FIG. 1 are directly coupled with remote server 122, which may by non-limiting example be a third-party server, or multiple servers (such as a portion of a server rack) or any portion thereof. System 100 could, for example, exclude server 106, and utilize only remote servers 122 which have access to the database 108 (which may be stored on the remote servers), and each of the computing devices may access the database through the remote servers and through one or more described web servers such as through one or more user interfaces displayed on the displays of the computing devices when accessing correlated URLs.

[0065] In other implementations one or more application servers could be included in the system, the application server(s) positioned relationship-wise between an end-user device and the database(s) to facilitate operation of the methods that will be later described.

[0066] As indicated, these are only examples of how to implement a threat modeling system, and many other layouts are possible. System 100 may also include many other elements which are not shown for brevity. In a small business or organization wherein only one computing device may be needed to do threat modeling, system 100 could be implemented using a single computing device 102 with a database 108 stored thereon, or with one computing device 102 coupled with a server 106 and database 108 through a local connection (wired or hardwired), or using a cloud-stored database that the user access through user interfaces through remote

servers 122 and/or web servers 120. In an organization in which multiple computing devices may need to do threat modeling the system 100 could be implemented using a computing device 102 having the database stored thereon, or coupled through a local or Internet connection to a database 108 stored elsewhere within the organization's computing devices such as on a server 106 or remotely on remote servers 122 accessed via a web server 120, with other computing devices 112 and/or 116 coupled either directly with device 102 and/or 106 and/or through the telecommunication network 110. In implementations in which remote servers are utilized these may be scaled up to any needed number.

[0067] The threat modeling system and methods include the modeling of threats utilizing software which users access and interact with through a variety of user interfaces, some examples of which will be described hereafter, but a brief description of the processes facilitated by the software will now be discussed.

[0068] Referring to FIG. 2, a representative example of a threat modeling process (process) (method) 200 includes generating a threat model (model) 208 for any application, process, or system under consideration. By non-limiting example, this 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). Model 208 is used to generate an original threat report (report) 214 which in implementations includes identified threats, the status of identified threats (threat status), and the source(s) of identified threats, among other things.

[0069] As illustrated in FIG. 2, process 200 may include storing a plurality of threats 202 and threat model components (components) 204 in a data store 206. This may include, by non-limiting example, storing titles, definitions or descriptions, and/or associated images in the database 108 for each component and/or threat. The threats and components are used to create threat model 208.

[0070] Process 200 in implementations includes a user selecting from among the available components those components which are relevant to any given system, process or application. This is represented by the arrow between "components" and "relevant sources." The relevant sources 212 are relevant sources of threats that are determined by the system 100 either after, or while, the user is selecting the components that are involved in the specific application, system or process and defining relationships between and among the relevant components. The system also retrieves from the database relevant threats 210 that were previously correlated with the chosen components or combinations of components through the database,

to form the threat model 208 (this is representatively illustrated by the arrow between “threats” and “relevant threats”). The threat model thus includes relevant threats and the relevant sources of those threats. The threat model is used to generate a threat report 214.

[0071] There may be some components with which no threat is associated (and they are therefore not relevant sources of threats), and there may be some threats that are dependent on one or more relationships between components. For example, when modeling a computing network some components may communicate with one another using a hypertext transfer protocol secure (HTTPS) protocol or instead with a transmission control protocol (TCP), and this relationship may determine whether there is a relevant threat to include in the model (or which relevant threat to include in the model). Although these relationships between components are communicative couplings and/or protocols in some instances, the relationships themselves may be considered “components” in a broad sense so that, in FIG. 2, the potential relationship types between components would themselves be considered components 204 that are stored in the data store and which the user utilizes to build a diagram of the system, application or process. Communication protocols may use conductive wires (electric signals), optic fibers (optic signals), wireless technologies (electromagnetic signals), and so forth.

[0072] FIG. 2 is a simplified diagram. Each component and each plurality of components is a potential relevant source for one or more threats. For example, one threat may be “Bluejacking” and one component, which would be correlated to this threat through the database, could be “BLUETOOTH port.” Accordingly, if a user includes a BLUETOOTH port in a diagram of a computing system, the system 100 will identify that port as a relevant source for bluejacking in the associated threat model and threat report. The component in this example is a physical component of a computing device or system/network. In other implementations components/sources may not be physical components. For example, if one is modeling the threats involved in commuting to work safely one threat may be “freeway collision” and one component, which would be correlated with this threat through the database, would be “merging onto freeway.” Thus, in this latter example “merging onto freeway” would be a relevant source for “freeway collision.” In this example the component (and relevant source) is defined as an action or step, and not as a physical component.

[0073] Regardless of whether the threats and components/sources are physical elements or steps, actions, etc., the database allows for the correlation of any threat to any number of components and likewise, the correlation of any component to any number of threats. Accordingly, using the above example, the BLUETOOTH port may be defined as a relevant

source for a Bluejacking threat, but it may not be the only relevant source (another source may be a BLUETOOTH device wirelessly connected with the system being analyzed). Similarly, Bluejacking may be defined as one threat that may occur due to vulnerabilities of the BLUETOOTH port, but there may be other vulnerabilities or threats that are present in the system due to the BLUETOOTH port.

[0074] Referring to FIG. 3, another implementation of a threat modeling process (process) (method) 300 is shown. Method 300 includes the steps described above with respect to FIG. 2 but also includes additional steps. A modified data store 302 includes data store 206 but also includes compensating controls 304 stored in the database. The stored compensating controls include, by non-limiting example, a title, definition, image, and/or other items for each compensating control. Each compensating control may be associated with one or more threats and/or with one or more components and/or with one or more security requirements through the database (security requirements may in turn be associated with one or more components and/or one or more threats through the database). Method 300 includes user selection of one or more compensating controls (relevant compensating controls 308) from among all compensating controls 304 stored in the database, and the relevant compensating controls together with the threat model 208 previously discussed (in other words the relevant threats 210 and relevant sources 212) are included in the modified threat model 306. Modified threat model is used to generate modified threat report 310.

[0075] Referring now to FIG. 4, method 300 may include other steps and may be shown by threat modeling process (process) (method) 400 which includes creating a threat model of the application, system or process of interest (step 402), generating a threat report based on the threat model identifying relevant threats (step 404), generating a modified threat model with the status of one or more threats changed to “mitigated” using one or more of the relevant compensating controls (step 406), and generating a modified threat report and/or a change log including the threats designated as “mitigated” by the one or more relevant compensating controls (step 408).

[0076] Referring now to FIG. 5, another implementation of a threat modeling process (process) (method) 500 is representatively illustrated. Method 500 includes cycling through the process of selecting/deselecting a compensating control (i.e., adding it to the threat model, or removing it) as often as the user chooses. After the threat model is initially built and the initial threat report is generated (step 502) the user may define a compensating control (step 504) (this step may also be done before the threat model has been built or the threat report generated). The

user may select the threats mapped to the compensating control and/or deselect threats mapped to the compensating control (step 506).

[0077] The user may add the compensating control to the threat model and thereby modify the model (step 508). System 100 matches threats identified in the original threat model with those mapped to the selected compensating control (step 510). The user at this point may be able to further modify the threats mapped to the compensating control. The status of every matched threat may be changed to “mitigated” or some other status by the user (step 512). A modified threat report may then be generated (step 514). The user is then brought to a point at which he/she may select whether to revert the model to its previous state (step 516). If the user selects to not revert the model, the process skips to step 522, otherwise the compensating control is removed from the model (step 518) and the status of matched threats are reverted to their pre-matched values (step 520). The user then determines whether to add another compensating control (step 522) and if so the process cycles to step 504 again, otherwise the process ends.

[0078] Reference will now be made to several example user interfaces which may be utilized to accomplish the above general processes and other processes as will be described. It should be stressed that these are only examples, and that other user interfaces could be used to accomplish the methods. Similarly, although specific user interfaces are described with respect to specific functionalities (dropdown menus, buttons, fields, tags, text prediction, etc.), the practitioner of ordinary skill in the art will be able to mix and match these functionalities and/or use other functionalities with the user interfaces to make the user experience intuitive and easy. For example, in instances where a dropdown menu is present this could be replaced by a search field, or a radio button selection, and so forth. Nevertheless, the user interfaces implementations as depicted in the drawings are useful for a variety of reasons, as will be understood.

[0079] Referring now to FIG. 6, a representative example of a user interface (interface) 600 is shown. This interface is titled the “knowledge base” page and may be displayed on any of the displays of system 100 shown in FIG. 1, depending on the particular system setup. Interface 600 has a number of selectors or menu items near the top of the screen such as, by non-limiting example, a three-bar menu selector, a “select all” selector, a “new” selector, an “edit” selector, a “delete” selector, a “copy to library” selector, a “select library” dropdown selector, a “home” selector, a “knowledge base” selector, a “templates” selector, a “profile” selector, a “change password” selector, and a “sign out” selector. In implementations some of these selectors may

be further organized into dropdowns so as to take up less space on the interface. Additionally, in implementations of system 100 some or all of the menu items may be present on other interfaces, such that they are permanent menu items at the top of those other interfaces as the user navigates from one interface/page to another.

[0080] This “knowledge base” interface is an interface where the user may view and edit “components” that are stored in the database. The title “components” is thus present at the left near the top of the screen, and below this are three columns for “name,” “type,” and “labels.” Below the column titles are search boxes where a user may begin typing and predictive text will bring up a list of items that begin with the letters typed so far. Each row shows one component type, name, and labels (if any). The list is scrollable as indicated by the scroll bar, and only a small number of components are listed here. For example, the topmost item is a WiFi router (named WIFI RTR in shorthand, and this and any other text used in the system may be in some type of shorthand or may be spelled out in its entirety in various implementations), its type is “Device,” and no labels are applied. Shown in FIG. 6 are the following types: device, IoT device (which represents “internet of things” device), communication protocols (such as HTTPS), generic data store, database, application component, and deployment component. Other available types not shown may include, by non-limiting example: cloud, external system, FTP server, generic external interactor, generic process, generic trust boundary, Modbus, perimeter control, third party software, third party library, transaction, WINDOWS application, WINDOWS OS, and so forth. These are only representative examples, and the user may define new types as desired and apply those types to a new component (or existing component), which will associate the type with the component name through the database. The rows may be organized in alphabetical order by any of the columns (name, type, labels) by clicking on the title of the column and may be organized in reverse alphabetical order by again clicking on the same column header (and toggled with continued clicking). The labels column may be useful for, among other things, searching for components that have a label applied. For example, if the user is looking for embedded system components, the user may search in the labels column for “embedded system” (or a shortened version if the system uses a shortened version) to find all components that have the embedded system tag applied.

[0081] A user may select any row by clicking anywhere in that row. The selected row will be highlighted, as representatively illustrated in FIG. 6 wherein the “login” row is highlighted. Once a row is highlighted any data associated with the component through the database is

shown to the right. For example, in the middle of the screen the component name “login” and its type “application component” are shown. Below this the tags applied to this component are shown, which in this case include: web, application, feature, authentication, password. A description can be associated with the component through the database – in this case no description has been provided. If a user desires to edit the name, type, labels, or description the above “edit” selector may be selected and the user will be able to input new information for any of these fields, which upon pressing a “cancel” button will revert to the prior data or upon pressing a “save” button will write the new data to the database.

[0082] Interface 600 also shows a “properties” section to the right, which shows the threats and security requirements associated with this component through the database. The user may press the plus icons to add new threats or security requirements, as desired, or may use the “X” icons to remove threats and/or security requirements associated with the component through the database. In this example the login component has the following threats associated with it: inducing account lockout; session hijacking; and clickjacking. The security requirements associated with the component in this example are: parameterized queries – dynamic SQL; breach – randomizing secrets per request; and encryption algorithm (the first two only show a short description on the interface screen for ease of viewing).

[0083] The threats and security requirements associated with the component through the database will at least partially facilitate the later threat modeling when a user is depicting a specific system layout. For example, if a user is depicting a computer system layout and adds the “login” component to the system layout then one or more or all of the associated threats may become “relevant threats” to the overall system as previously described. In some systems 100 all the threats associated with this element would become “relevant threats” to the specific application, process, or system being modeled, and in other systems 100 some of these threats may be automatically dropped from “relevant threats” for the specific application, process or system being modeled if other components added to the system would inherently mitigate those threats (such as an HTTPS protocol instead of HTTP protocol being used between two components).

[0084] With regards to the other selectors, a user may select the “select all” option to select all components then listed (if the user has done a search this would limit to selecting all those components populated by the search), and the user may then press the delete selector to delete all of these components and their relationships (associated threats, security requirements, tags, descriptions, etc.) from the database. The user may instead, once all are

selected, press the “copy to library” selector to copy the selected items to a default library set up by the user previously through another interface. The user may similarly select only one or a few components to delete or copy to the default library. The “select library” selector allows a user to display various libraries, here the “ThreatModeler” library is displayed but the user may create his/her own libraries, may view other built-in libraries or third-party libraries accessible through the interface through a web server or other server which communicates with another third-party database, and so forth.

[0085] The user may select the “new” icon to bring up a popup interface in which the user may define a new component, giving it a name, selecting the component type from a dropdown menu, adding an image to be displayed to represent the component (such as a lock for a security feature, a USB indicator for a USB device, etc.), labels, and a description, and may then select a “cancel” selector to cancel the new component or may select a “save” selector to write the new component information and relationships to the database, and selecting either save or cancel will also remove the popup interface and revert back to interface 600.

[0086] The home menu item at the top right of the screen will navigate the user to a home screen. The knowledge base icon will navigate to interface 600. The templates selector navigates to an interface similar to interface 1000 of FIG. 10 (hereinafter described) but with a blank canvas 1002 for creating a new template which may be used later for creating other relational diagrams (diagrams) 1004 (also described hereafter). The profile selector brings up a popup window which displays the current user’s name, email, department, role (admin, etc.), and last login date/time as stored in the database, and a close button to close the window. The change password selector brings up a popup window to change the user’s password with a “close” selector to cancel the change and a “save” selector to write the new data to the database. In implementations the home, templates, and knowledge base icons are permanently displayed at the top of all interfaces of system 100 and the profile, change password, and sign out selectors are available from a dropdown icon which is also displayed at the top of all interfaces of system 100. The sign out selector allows the user to log out of the system. Interface 600, as well as other interfaces of the system, may also include a refresh selector to refresh the page and a help icon to bring up a help menu. An icon displaying a title and/or logo of the software may also be displayed at the top of the screen (such as the top left) which when selected may navigate to the home screen.

[0087] When the triple-bar menu icon is selected it brings up a popup expandable menu which, when all items are fully expanded, appears as interface 700 of FIG. 7. The “threat library” menu

item includes the sub-menu items “threats,” “test cases,” and “threat agents,” the “security requirements” menu item includes the sub-menu items shown, the “threat patterns” menu item includes the sub-menu items shown, and the “enterprise” menu item includes the sub-menu item “users.” When any of the sub-menu items are selected an interface very similar to interface 600 is displayed.

[0088] For example, FIG. 8 shows interface 800 which is accessed by selecting the “threats” sub-menu item. The title “threats” is shown near the top of a list of threats which are organized into rows and columns showing each threat’s name, risk level, and attached labels. Several threats are shown, and any column may be searched using the search box directly below the name, risk, or labels headers, which behaves similarly as described for FIG. 6, and the data may be organized alphabetically (or reverse alphabetically) by any column as described with respect to interface 600. The selected threat is highlighted, and its information is displayed to the right including the name, risk level, labels, and a description, which in this case includes a URL. The properties section includes threat agents which may be added, though none are added to this threat—but examples include things like “insider,” “black hat,” “hactivist,” “cyber terrorists,” “authorized external user,” and so forth which are threat agents that had previously been identified by the user. Threat agents may be added and removed. Test cases may also be added and removed, this threat has three test cases added which were previously entered into the database by the user. Security requirements may also be added by the user and, in this way, compensating controls may be associated with specific threats through the database—this is one of the ways the system facilitates step 506 of FIG. 5. Security requirements may be added to the database originally through another interface, described hereafter, and identified there as a compensating control, then added to a specific threat from interface 800. Such an association through the database facilitates the system displaying various compensating controls in a diagrammed system, method or application and the threats those compensating controls can mitigate.

[0089] The menu items at the top of FIG. 8 are the same commands/links as those shown in FIG. 6 but are shown here in icon format to give another representative example, where the select all selector is represented by a checkmark, the new selector is represented by a plus icon, the edit selector is represented by a pencil icon, the delete selector is represented by an “X” icon, the copy to library selector is represented by an icon of two documents, the home selector is represented by a home icon, the knowledge base selector is represented by a file folder icon, the templates selector is represented by a document icon, and the profile, change password,

and sign out selectors are available by selecting a dropdown menu represented by a downward facing triangle icon.

[0090] Referring back to FIG. 7, if the “test cases” sub-menu item is selected an interface similar to interfaces 600/800 is displayed, but showing test cases, and allowing the user to add, edit, delete, copy, add labels, and so forth, similarly as previously described with respect to the “threats” sub-menu item. The threat agents, security requirements, code snippets, code reviews, components (already described with respect to interface 600 since the components interface is set as the default interface when the “knowledge base” selector is selected), data elements, roles, widgets, component types, attributes, and user sub-menu items all have similar functionality and bring up similar interfaces when selected. Data elements, which represent data elements that may be captured by any diagrammed system, application or process (such as credit card numbers, billing addresses, pins, phone numbers, email addresses, order history, birth date, medical history, insurance history, and so forth) may be associated with specific threats and with specific security requirements in the same way as those associations may be made for components.

[0091] If a user selects the security requirements sub-menu item an interface similar to interfaces 600/800 will be shown similar to interface 900 of FIG. 9, which allows the user to order security requirements alphabetically (or reverse) by name or label and search for specific security requirements. Selecting any security requirement will highlight it and display its name, description, labels, an indicator to indicate whether the security requirement is a compensating control, and any code snippets or code reviews (under a “properties” header) that have been associated with the security requirement (which may be added or removed from that interface similar to what is described with respect to the “properties” elements of interfaces 600/800).

[0092] Interface 900 is actually the interface visible when the user selects the “new” selector to create a new security requirement. From this window the user may add a name, add a description, check a box (or leave it blank) to indicate whether the security requirement is a compensating control, add any labels (which are previously input into the database by the user), and press cancel to abort the addition or press save to write the data to the database.

[0093] From any of the previously mentioned interfaces, if the user presses the home selector an interface similar to interface 1300 of FIG. 13 will be displayed, which lists all previously stored threat models by name and showing their version. Either column may be organized alphabetically or in reverse, and the PDF button will export the list to PDF. If any specific threat model is selected it will be highlighted and its associated threat report (threat report interface)

1302 will be displayed, which will be discussed hereafter. From the top menu items the user may select the new selector to create a new threat model, the edit selector to edit the name, version, risk level, an “internal” toggle, and labels associated with the selected threat model, a delete selector to delete the selected threat model, a diagram selector to view the diagram for the selected threat model, a report selector to export to PDF the threat report (which for each threat the threat name, source, risk level, status, and creation date), a threat tree selector to view a diagrammed threat tree, showing threats of the threat model, and other selectors already described.

[0094] If the threat tree selector is selected a threat tree is displayed in which threats are organized as sub-elements of data elements and/or components, and also displayed are mitigating security requirements or compensating controls that may be implemented to mitigate the threats and an indicator of whether each threat has been mitigated. Portions of the tree may be collapsed, expanded, or viewed in vertical tree or horizontal tree format. The interface showing the tree diagram has selectors to zoom in, zoom out, revert to 100% zoom, toggle on/off a thumbnail overview image in a corner of the display, save an image of the tree, open a legends window which shows the colors in which various elements are diagrammed (threat agent, widget, component, role, data element, security requirement, threat, protocol, node, and project), and a filter selector which allows the user to remove and add back in any of the aforementioned items from the tree. The tree may be dragged and moved in any direction for viewing any portion of it easier.

[0095] Continuing with FIG. 13, if the new selector is selected (which, as with all other selectors, could be implemented as an icon or logo absent any wording), a popup window appears allowing the user to enter a name, version, toggle an “internal” indicator, select a risk level from a dropdown (from among previously determined risk levels stored in the database), apply labels (which allow the user to type and populate a list of already entered labels stored in the database to select one, or to add a new label by typing a new item and selecting “add new”), or the user may select a “new from template” button to begin a new diagram from an existing diagram template, or a “new from features” button to begin a new diagram from user-selected features, or the user may select “import” to begin a diagram from a previously stored diagram (such as from an older version of the software), or the user may select “empty” to begin a diagram with a blank canvas.

[0096] If the user selects “new from features” the diagram interface of FIG. 15 displays with a blank canvas 1002, and a popup selector (not shown) allowing the user to select “business

requirement” features which are desired to be included in the model such as, by non-limiting example, authentication, funds transfer, credit verification, bill pay, or other features already stored in the database previously by the user, and after selecting the desired features, the blank canvas will populate with a node for each feature. The user can then modify and/or add components to the diagram as desired. In implementations each of these added “business requirements” will add a “component group” to the diagram and threat model, as will be described hereafter.

[0097] If the user selects “empty” the diagram interface (interface) 1000 of FIG. 15 will appear, showing the blank canvas 1002 as shown. To the left of the canvas is a toolbox module which may be minimized using the left facing double arrows and re-expanded by selecting the same arrows which will then be right facing. To the right of the canvas is a properties module which also may be minimized and expanded in similar fashion, along with sub-menu items “general,” “components,” “data elements,” “roles,” and “widgets” each of which may be expanded downward or minimized upward using the double arrows (in FIG. 15 they are all minimized).

[0098] The toolbox module is searchable, with the user able to begin typing and the system suggesting through a list populated just below the search box components which begin with the letters (or include the letters) typed by the user. The dropdown to the right of the search box may be used to allow the user to search from among all components or a subset such as one or more specific component libraries as previously discussed, with ThreatModeler being an example component library) and/or one or more specific component types as stored in the database (and previously discussed with respect to FIG. 6). The user may also scroll down through the components using the scrollbar function.

[0099] In the example of FIG. 10 the components in the toolbox are of varying sizes, but in implementations they may all be of similar sizes and shapes (or identical sizes and shapes). In implementations in which the system is deployed within a single organization with only a local library of components the components listed in the toolbox will be those that have been input by the user or that were previously loaded into the database during software installation. In implementations in which the system includes some remote communication with other libraries the toolbox may display components available from other parties, such as through a cloud computing services, e.g., MICROSOFT AZURE or the like (in implementations the entire system and methods could be implemented using cloud computing in instances where a local software installation or local database are not desired).

[0100] The toolbox, as can be seen, includes components that were previously entered into the database through interface 600 as previously described. From interface 1000 the user may select a desired component and drag it to a desired location on the canvas, and by dragging multiple items the user may begin to add the components of a system, application 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. The user dragging components to the canvas is one way in which the user selects relevant components or relevant sources as described with respect to FIG. 2, and it is from these relevant components (relevant sources) that the system identifies relevant threats by identifying the threats that are associated through the database with those components.

[0101] In implementations a communication protocol (protocol) can be defined between components by clicking on a component and dragging the cursor to a second component. This will create an arrow, such as those shown on FIG. 10 between components on the canvas, and will display a default protocol (here the default protocol is HTTPS), but a user may right click the arrow to display a popup selector allowing the user to deselect HTTPS and/or select one or more other protocols (such as TCP, SMB, WiFi, 3G, 4G, AJAX, binary, BLUETOOTH, FTP, FTPS, HTTP, IMAP, MAPIRPC, SMTP, SMTPS, USB, etc.), and when any protocol is selected that protocol name will be displayed (or if multiple are selected then “multiple” or some term/icon meaning “multiple” will be displayed - in the image this is shown as “MULT” for short)—these protocol arrows will also be color coded by type (such as green for HTTPS, red for multiple, and so forth). Protocol arrows may also be deleted as desired. The alphanumeric descriptions are shown here next to the link arrows, but in implementations the wording may be superimposed over the link arrows. They are shown here next to the arrows for easier readability.

[0102] The components displayed in the toolbox of FIG. 10 are generally shown without icons. The USB Port, SSO (single sign on), BLUETOOTH PORT, and BLUETOOTH PROXY components are shown with icons as an example that all components may be shown in the toolbox with an icon if desired. It may also be seen that the user may input components that constitute branded software elements, such as PAY PAL, AKAMAI DNS, SKYPE, etc. In implementations all compensating controls will be displayed in the toolbox with a similar icon, such as the padlock icon shown for the SSO component of FIG. 10.

[0103] As a user adds components and links them together, the threat model includes the threats that are associated with the components/protocols. As previously described, each

component, each protocol, and each data element may be directly associated with one or more threats through the database. Accordingly, each time a component is added to the diagram, or a new link drawn between components and protocol selected, if there are any threats associated through the database with the component and/or protocol those threats are then included in the threat model. A user may at any time right click on a blank area of the canvas when no component/link is selected and a “threat report” item will be selectable which, when clicked, will generate a popup threat which will include a list of all threats. In implementations this will look much like the threat report 1302 shown in FIG. 13, and will include a first “threats” tab list of all threats (and the number of threats), identifying the risk level of each threat, showing the threat status (open/mitigated), identifying the source of the threat (which is a component on the diagram), and having an actions column from which the user may display a description of the threat (previously associated with the threat through the database) (the description selector here shown with the letter “D” though the selector could instead show “description” or the like) and leave a comment to store to the database (the comment selector having the phrase “note” though in other implementations it could say “notes” or “comment” or the like). The user may organize the table by any column (alphabetically or reverse) and may also organize by column headers by dragging the column headers to the location indicated. For example, the user could drag the “status” header to the identified location and then drag the “risk” header to the right of it and the table would then be organized first by status and then by risk level. When this “dragging” is done a “ghost header” is dragged up to the identified location in the sense that the existing header remains in place. The organization may be reverted to an earlier state by deleting the ghost headers using an “x” icon.

[0104] The threat report displayed also includes a security requirement tab (showing number of security requirements) and displaying a table similar to the threats table. The security requirements table lists the security requirements that are associated with one or more of the identified threats in one column, lists a source in another column (which is the component associated with the threat), includes an “implemented” column indicating whether the security requirement has been implemented, an “optional” column indicating whether the security requirement is optional, and a similar “actions” column to the previously described actions column, this time the description giving a description of the security requirement and allowing the user to record a written note. This table may be organized similar to the previously described table.

[0105] With respect to the “implemented” column, in implementations this is a checkbox for each security requirement indicating whether the security requirement has been implemented. The user may manually check those security requirements that have been implemented and manually uncheck those that have not. This column may also have been previously populated with some “implemented” checkmarks based on mitigations that the user has selected for specific compensating controls, which will be discussed later with respect to FIG. 11. Further, the “optional” column may also include checkboxes which a user may manually toggle to indicate which security requirements are optional or not. This column also may be populated by the user selecting certain mitigations as will later be discussed with respect to FIG. 11—for example if there are two security requirements associated through the database with a specific threat, but only one needs to be implemented, then if the user selects one of those security measures as mitigating the threat the other security measure may populate on this list as being checked “optional.”

[0106] The threat report further includes a “test cases” tab (showing the number of test cases) and displays a table listing test cases associated with the threats through the database. As previously described with respect to FIG. 8, each threat may have test cases associated with it. An example test case would be, for example, a “dictionary-based password attack” for a password-related threat. The test case tab would list this test case and have an “actions” column which, when an icon is selected, pops up a description, which in this case states “use a password cracking tool what will leverage the dictionary to feed passwords to the system and see if they work” and further list techniques like setting the test to try all words in the dictionary, common misspellings, and combinations of words and common misspellings of combinations. The test case tab/table thus offers tests that the user may try to test against the threats both before and after security requirements are implemented. This table may be organized and sorted similar to the previously described tables.

[0107] The threat report further includes a “code reviews” tab (showing the number of code reviews) and displays a table listing the code reviews that are associated with the security requirements through the database (as previously shown with respect to FIG. 9). An example code review would be, for example, an “Authentication: Weak Password” code review. The code review table would list this code review and have an “actions” column which, when an icon is selected, pops up a description, which in this case states “Password strength should be enforced upon a user setting/selecting one’s password” and gives examples of code that may be used to set up such an enforcement. The code review tab thus offers sample code that the user

may use to implement measures against threats which may complement or work together with implemented security requirements. This table may be organized and sorted similar to the previously described tables.

[0108] Multiple selectors are shown at the top of interface 1000 in addition to the permanent selectors that are available on several interfaces. The “select all” selector selects all components on the canvas (the user may then deselect some, if desired, for example for grouping some or all the components as later described). The “copy” selector copies selected components and the “paste” selector pastes the copy onto the canvas (this may also be done with keyboard shortcuts, and shortcuts may in implementations be used for all other selectors described herein for system 100). The “delete” selector deletes the selected components from the canvas and the “clear canvas” selector deletes all components from the canvas. The “zoom in” and “zoom out” and “100%” zoom in and out of the canvas and revert to a 100% zoom, respectively. The “comment” selector populates an empty comment box on the canvas in which the user may type a comment which will remain on the canvas until later removed (though it may appear in minimized or icon format until hovered over or opened). The “overview” selector displays a thumbnail overview of the entire diagram in a corner of the canvas.

[0109] The “undo” selector undoes the last action (or multiple last actions if selected multiple times) and the “redo” selector does the opposite. The leftmost “templates” selector pops up a menu from which one or more previously saved business requirement “features” may be selected to add to the canvas (these may be nodes and/or component groups, for example, and may be the same nodes/component groups that are described above when the user uses the “new from features” function when generating a new model). The “save as image” selector has a dropdown and allows the user to save an image of the diagram as then displayed in one of various formats such as PNG, SVG, etc., or to take a “snapshot” which saves the diagram at the present state to the database. The “PDF” selector generates a PDF of the threat report based on the current configuration of the diagram components (the threat report described to some extent above). The “settings” dropdown selector allows the user to toggle between straight or curved link lines (protocol lines/arrows), showing or hiding the link wording (in FIG. 10 the lines are curved and the link wording is shown), making the diagram public or non-public, and showing or hiding comments (the comment function described above).

[0110] The “save as template” selector allows a user to save the entire diagram as either a threat model or a business requirement “feature” (in other words saving it as a component

group) and in either case the user may give the feature a name, add labels, and select the type as either threat model or business requirement, then press cancel to cancel or save to store the new template to the database. The “snapshots” selector populates a list of previously saved snapshots, any one of which may be opened from the list or deleted.

[0111] The “group” and “ungroup” selectors allow the user to create a group containing multiple components or to delete a group (but not the included components). As seen in FIG. 10 for example, there is a “WINDOWS 7” group which includes file system, PDF client, SKYPE, OUTLOOK 2010, MCAFEE HIPS, MCAFEE AV VSE, IE11, BIT LOCKER, MCAFEE DLP, and OFFICE 2010 components. There is also a Laptop group containing the WINDOWS 7 group and further containing WiFi port, USB port, ethernet port, HDMI port, and BLUETHOOTH port components. Finally, there is an Office Network group which includes the Laptop group and also includes file server, SHAREPOINT, printer, WiFi access point, IRONPORT, email server, BLUECOAT proxy, and SSO (single sign on) components. Then there are other components (external email gateway, AKAMAI DNS) which are not part of any group. A group may be formed from any one or more components, and the AZURE group is seen containing only a single component: ONEDRIVE.

[0112] When a group is formed the user may, using the right-side “general” dropdown, add a custom display name, select a container type (from container, trust boundary, collection, or some other option stored in the database previously by the user), select a component (for example for the WINDOWS 7 the component “WINDOWS machine” is selected, which shows that some components stored in the database may include other components), select other display choices such title and background/border color, and select a Common Platform Enumeration (CPE) identification from among a list previously stored in the database (for example in this case ID a version of WINDOWS 7 is selected) (the list of CPE IDs may be searched using filters to easily find the appropriate one), and the user may also add notes.

[0113] As further examples, the WINDOWS 7 group is identified as a container group, a WINDOWS machine, and a specific WINDOWS 7 operating system version is identified. The Laptop group shown in FIG. 10 is listed as a container group and no CPE ID is selected. The Office Network group is identified as a trust boundary group type and no CPE ID is selectable. The AZURE group is identified as a trust boundary group type and no CPE ID is selectable.

[0114] Each grouping of components, however, could be diagrammed separately as an independent threat model and then saved as a component so that it may be imported into another threat model/diagram. When a user adds any of these component groups to a blank or existing diagram/threat model the threat model of the component group is added to (and/or

nested within) the threat model of the existing diagram/threat model. In this way the user can modify a threat model by incorporating previously defined threat models. This ability is generally termed “threat model chaining” herein and is a useful mechanism for allowing a user to diagram complex systems/processes without having to repeatedly build common elements among the systems/processes.

[0115] 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.

[0116] Referring back to FIG. 10, the “compensating controls” selector may be selected to display a popup similar to compensating control report (report) 1200 of FIG. 12. This report is populated from previous relations stored in the relational database. As indicated previously with respect to FIG. 6, each component may be associated with one or more threats and one or more security requirements through the database using interface 600, and as described with respect to FIG. 8 each threat may be associated with one or more 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.

[0117] By non-limiting example, the threat of “physical theft” is associated with the component “laptop” through the database, but no security requirements are directly associated with the laptop component. Nevertheless, the “physical theft” threat is associated with the security

requirements “MCAFEЕ FRP” and “BITLOCKER” through the database, both of which security requirements are identified through the database as compensating controls (MCAFEЕ FRP being a USB encryption tool and BITLOCKER being a disk encryption tool). Accordingly, when a user adds the laptop component to a diagram, if the user selects the “compensating controls” selector this list will then include both MCAFEЕ FRP and BITLOCKER as compensating controls for the physical theft threat. If the user removes the laptop component from the diagram (deletes it) then the MCAFEЕ FRP and BITLOCKER compensating controls will no longer appear in the list (unless they are also associated as compensating controls for some other threat present in the diagram). In implementations the list populated will also show compensating controls which are directly associated with a component that is added to the diagram. In other words, in the above example there are no security requirements directly associated with the laptop component, but if a third security requirement were directly associated with the component through interface 600, and if the third security requirement was identified through the database as a compensating control, then that third compensating control would also populate in the list of interface 1200.

[0118] Referring again to FIG. 10, it may be seen that this diagram includes the MCAFEЕ DLP, BITLOCKER, MCAFEЕ HIPS, and MCAFEЕ AV VSE components grouped in the WINDOWS 7 group. The user may, for example have modeled the WINDOWS 7 group, then used the compensating controls selector at the top of interface 1000 to identify that there are certain threats that these components would mitigate. The user may then add those components to the WINDOWS 7 group by dragging them from the toolbox to a location within the group outline to add them to that group. Then, upon right clicking on any specific security requirement component, the user may select a “mitigations” selector which pops up mitigations interface (interface) 1100 as shown in FIG. 11. The user could add one of these components at a time and model the mitigations, generate a new threat report, then either remove that component or add another compensating control, and in this way test out various compensating controls. This is one way in which the system facilitates steps 512, 514, 518, 518, 522, and 522, among other steps, of FIG. 5.

[0119] Interface 1100 displays a table which lists all threats and their associated sources (component associated with the threat), risk levels, and status, and highlights the listed threats which the security requirement is configured to mitigate as identified previously through the database through interface 800 (these threats are “mitigatable” by the selected security requirement). The user may deselect highlighted threats and/or may highlight other threats,

then may select “close” to cancel or may select “mitigate” to toggle those threats to mitigated through the database. Once this is done, for example, the threat report as seen in FIG. 13 (or popup shown from the diagram interface) will list the mitigated threats as “mitigated” and the compensating controls list shown in FIG. 12 will also show the mitigated risks as mitigated.

[0120] The threat report of FIG. 13 allows a user to manually change the risk level and threat status directly from the home menu using the “change risk” and “change threat status” drop downs once a threat is selected by clicking on any row. Changing the risk level of a threat from this interface will only change the risk level for this specific threat model. Threat statuses that may be used include, by non-limiting examples: open, closed, mitigated, fixed, not applicable, needs more details, not tested, secure usage practice, and so forth.

[0121] The systems and methods described herein may also be used for analyzing an attack surface of a complex system or process, which will be described now. In implementations the attack surface of a system or process is comprised of the sum of all open and unmitigated potential threats to an “asset” identified through threat modeling.

[0122] As described herein, a modeled system or process may include a modeled deployed or contemplated computing network, which could include by non-limiting example: one or more applications; one or more on-premises infrastructures; one or more cloud-based infrastructures; one or more hybrid infrastructures; serverless architectures; microservices; one or more embedded devices; one or more IoT devices; one or more mobile devices; one or more Industrial Control Systems (ICS); one or more cyber-physical systems (CPS); one or more third party systems; one or more organizational networks or intranets; non-cyber elements interacting with a cyber system such as, by non-limiting example tangible assets, intangible assets, property(ies), plant(s), equipment, liquid assets, brands, reputation, residential structures, real property, utility services, unattached removable items and assets; an infrastructure system, such as a transportation infrastructure, an electrical grid, a telecommunications network, and so forth, all in implementations accessible and utilized through a highly interconnected network of intranets, wireless networks, and the Internet.

[0123] All such components of a modeled process or system may include potential threats which, if discovered and exploited by an adversary, may yield one or more attack vectors to one or more assets of the system or process. The “asset” may be any item selected by a user to be identified as an asset. The modeled “attackers” included in any threat model may be actually modeled as a person in implementations, though in other implementations may be simply

modeled as an entry point or device included in the process or system which an attacking person may use to cause harm.

[0124] It may be pointed out that increased interconnectivity of a computing system with other systems (such as the Internet, third party systems, end user systems, etc.) may increase economic value and efficiency though these may also increase organizational risk due to the increase in adversarial actors and a constantly evolving threat landscape. The threat modeling chaining and attack simulation systems and methods described herein allow organizations to manage threats at a comprehensive organizational level notwithstanding an ever-changing threat landscape.

[0125] A modeled “attack” as used herein is a modeled attempt by an adversarial entity to transverse the modeled system or process from an attack surface to one or more assets within the system or process. The routes from all potential attackers to a selected asset are the “attack vectors” or attack paths to that asset.

[0126] Referring now to FIG. 14, a block flow diagram illustrating steps that may be included in a general attack surface analysis. Step 1402 includes user generation of a diagram of a system or process, as has been described previously with respect to FIG. 10. Step 1404 includes system generation of a threat report for each component or component group and step 1406 includes system combination of the individual threat reports into a comprehensive threat report for the overall diagrammed system/process (this would include, for example, including threat report elements for nested or chained threat models, as has been explained above), and then steps 1408-1414 include steps which may occur in any 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).

[0127] FIG. 16 further breaks down step 1402. At step 1602 the user identifies the components of the system or process and chooses their relative placement within the diagram, at step 1604 the user identifies the type and placement of any communication protocols between

components, and at step 1606 any other attributes of components (including protocols) may be further designated (this step may be excluded in some methods, and these steps may be done in any order in implementations).

[0128] FIG. 17 shows a tree diagram that representatively illustrates a method of determining an attack vector for a selected asset. After a system or process is modeled using the diagram interface, described above, then in the diagram interface or in another interface either an asset is selected or an associated component is selected and relevant threat attack paths illustrated. For example, in the topmost node of FIG. 17 an asset 1702 is shown, and the attack tree or threat tree shows that the asset is associated through the database with four components. Components 1704, 1706, 1708, and 1710 are each associated with threats (i.e., the threats that are associated with each component through the database). Accordingly, threats 1712, 1714, 1716, 1718, 1720, 1722, and 1724 are shown. It may be seen that the system then determines that threat 1722, through component 1708, is a threat to asset 1702, and thus attack vector 1726 (shown by lines of heavier weight) is shown between threat 1722 to asset 1702. The diagram of FIG. 17 may be shown on an interface of the system, though in implementations FIG. 17 simply models the method the system is utilizing behind the scenes to show the attack vector(s) in the diagram interface, as in some implementations (such as those shown in the drawings) the threats are not explicitly shown on the diagram interface(s). FIG. 17 shows an attack vector by which an adversarial entity may target the asset, i.e., by exploiting threat 1722 of component 1708. It should be noted that the asset may be some sub-component within a diagrammed component, or it may be some element that is somehow associated with the component (for example the component may be a database, and the asset may be sensitive client information stored within the database—in that instance the asset could be defined broadly as the database, or it could be defined narrowly as the sensitive information within the database, other information in the database not being included in the definition).

[0129] It is noted that each asset could have any number of threats that could threaten to compromise it. Accordingly, the system identifies all threats which may compromise the asset in order to visually diagram attack vectors for the user. Some assets may be threatened by only a single threat, some may be threatened by two or three threats, or more, and so forth. Along these same lines, it is pointed out (as has been discussed to some extent above) that each individual component (or grouped set of components) of a threat model could, itself, be associated with its own threat model through the database. Because of this, the overall threat model that is shown (for instance in FIG. 13) in implementations could be called a threat model

portfolio as it includes all sub-threat models and nested threat models. For example, an overall threat model A could include components B, C, and D. Component B could be a single component, component C could be a previously modeled group of components having its own threat model, and 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. Accordingly, the threat model A would include all threat models associated with components and component groups B, C, D, and E, including all nested threat models. As described above, this “threat model chaining” may allow for quick and simple building of process/system models without having to recreate commonly included system/process elements.

[0130] In implementations one or more interfaces of system 100 may be utilized to list the top potential threats (such as the top ten potential threats), the top most vulnerable components, the composition of threats by risk type, the composition of threats by status (mitigated, unmitigated, open, etc.), and so forth. The data may of course be organized and displayed in many other ways. In implementations an interface could list each threat, list each threat risk level, and list the source(s) for each threat. In implementations each threat source listing may include a component and an underlying source, so for example one component may be associated with multiple sources of a threat. An example would be an online banking interface which is shown on a diagrammed threat model as a component, and a threat may be a virus being introduced to the bank’s environment through a breach in the banking interface, and one source of the threat may be a legitimate user who unwarily exposes the ATM to a virus on his/her computer, and another source of the threat may be an individual hacker seeking to introduce to the virus to the banking environment, and another source of the threat may be a state-sponsored entity with high end mechanisms to seek to introduce the virus to the banking environment.

[0131] In implementations an interface of the system may list the most vulnerable components in ascending/descending order, along with the risk level for each listed component, the number of total threats to that component, and the number of open or unmitigated threats for that component. In implementations an interface of the system may list multiple data elements associated with components (for example user names, social security numbers, financial info, credit card numbers, employee ages, etc.) (in this case the component likely being a database housing the data), a data classification for each data element (such as confidential, restricted, public, etc.) and an exposure level for each data element (such as very high, high, low, etc.). In implementations an interface of the system may break down the risk levels by percentage, such

as 45% very high risks, 25% high risks, 15% medium risks, and so forth. In implementations an interface of the system may break down risk status by percentage, such as 45% open threats, 25% closed threats, 30% mitigated threats, etc. In implementations an interface of the system may visually illustrate the number threat introductions plotted versus time, such as the number of threat introductions by month.

[0132] Any of the interfaces discussed herein may, as would be expected, change (and in implementations may change dynamically) as edits are made to the diagram (for example when a compensating control is toggled between ON/OFF states, this may change many or all of the interface displays accordingly by varying percentages, mitigating threats, etc. Thus when a compensating control is introduced and/or turned on or off, the threat model, threat report, mitigations interface, compensating control report, and so forth may all change accordingly to reflect the updated configuration.

[0133] It is pointed out that any threat model of the system may be subjected to an attack vector analysis. So, for example, an attack vector analysis may be performed on a simple two-component diagram, or an attack vector analysis may be performed on a hundred-component diagram that includes the two-component diagram as a nested sub-threat model.

[0134] In implementations an interface of the system may show a display similar to FIG. 17 except mapping all components/assets vulnerable from a single threat. In other implementations an interface of the system may show a display of all threats affecting a single component or asset. In the latter case the visual display may show attack vectors branching outwards from the asset, tracing communication protocols and extending through multiple components as far back as the locations/sources of the underlying threats. This is representatively illustrated in FIG. 18, which shows a type of display that may be shown on an interface of the system.

[0135] 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. The arrows in FIG. 18 are shown in different formats so that they can be distinguished from one another. In other implementations they may all have the same appearance. 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. It may be seen that a threat emanating from component G threatens to compromise component A (or the asset within or associated with component A), the attack vector 1802 passing through component F and component B to reach component A. A threat emanating from component E also threatens to

compromise component A, the attack vector 1806 passing through component B to reach component A. A threat emanating from component D also threatens to compromise the asset, the attack vector 1804 passing through component C and component B to reach component A.

[0136] The attack vector displays may be modified based on contemplated compensating controls. FIG. 19, for example, shows the diagram of FIG. 18 but modified to include six compensating controls (each labeled “CC”). These compensating controls may mitigate different threats emanating from different components. Compensating control 3 (CC3) may mitigate one or more threats from component D. CC2 may mitigate one or more threats from components C and/or D. CC5 and CC6 may each mitigate one or more threats from component E. CC4 may mitigate one or more threats from components F and/or G. CC1 may mitigate one or more threats from components B, C, D, E, F, and/or G. Using such a modeled attack vector diagram, the user may be able to alter compensating controls and make decisions about where in the system to deploy compensating controls. The user may determine, for example, that CC1 may mitigate many threats more efficiently than several compensating controls deployed elsewhere in the system. Or it may be determined that the asset is better protected by some other combination of compensating controls.

[0137] The elimination of any threat of course protects downstream components. Accordingly, for example, if CC3 eliminates or mitigates one threat emanating from component D, then the downstream effects of that threat to components C, B, and A are all mitigated. On the other hand, if CC1 eliminates or mitigates the same threat, it would only eliminate or mitigate the threat for component A, not for components B or C. Accordingly, there are security advantages to having compensating controls further upstream.

[0138] Changing the compensating controls in such a diagram could also change the other displays on other interfaces, for example the listing of top threats, listing of top ten most vulnerable components, other top ten listings, composition of threats by risk, composition of threats by status, composition of threats by source, composition of threats by other criteria, the overall threat model, the mitigations interface, the compensating control report, and so forth. This dynamic change of all interfaces allows the user to do “what if” analyses by adding/removing any compensating control and/or toggling any compensating control between ON/OFF states and then seeing how all the aforementioned displays/reports etc. change accordingly. The change may, for example, illustrate one or more threats as mitigated or closed instead of open or unmitigated, reduce the total number of open or unmitigated threats, reduce exposure levels of data elements, alter the percentages of threats by risk level (very

high, high, medium, low, very low, etc.), alter the percentages of treats by status (open, closed, unmitigated, mitigated), or the reverse of all these, on any of the interfaces, reports of the system.

[0139] The term “asset” as it is used herein may refer to anything that has value to a user or organization, and therefore requires security measures to protect it from theft, manipulation, destruction, compromise, or other forms of abuse. Attackers are an active population of computer environment users and vary in the skills, toolsets, opportunities, financial backing, and other attributes required for a successful attack on an asset. Most security measures to protect a computer system-related asset may be categorized into one of two categories: (1) defensive and/or monitoring mechanisms to inhibit attacks in progress or mitigate the effects thereafter, and; (2) reducing the number of potential threats through which attacks may be initiated to begin with. The latter can in many cases be less costly overall, and the ability of the systems and methods described herein to test and retest various configurations, including modeling the use of compensating controls, allows users to focus efforts on this method.

[0140] In implementations threat modeling and/or attack simulation methods may include the following steps: (1) generally defining a threat model (including model type, outputs to be generated, and overall objectives for different stakeholders); (2) visually diagramming a system/process using database-stored components (including communication protocols and compensating controls); (3) classifying one or more data elements within a component (or associated with a component, and/or one or more components themselves, as assets; (4) identifying and enumerating potential threats to the assets based on the diagrammed components; (5) analyzing the identified threats (threat analysis); (6) identifying and analyzing potential attackers based on the threat analysis; (7) analyze the effectiveness of deployed or contemplated compensating controls to mitigate the potential threats; (8) analyze a threat model and attack surface as modified by compensating controls; and (9) measure and quantify the effectiveness of the model and/or method relative to the desired outputs and objectives previously determined. This is just one example of steps included in such methods, and other methods may exclude some of these steps, or include other steps, and so forth. In an implementation of the above steps, step (6) interrupts step (5), and in an alternative implementation step (5) is allowed to be completed without interruption. Furthermore, in implementations steps (7) and (8) may be iteratively bounced between during any given implementation, so that a user adds a compensating control then checks the outcome, toggles the configuration of the compensating control then checks the outcome, removes a

compensating control then checks the outcome, moves a compensating control to a new location then checks the outcome, etc., before moving to step (9).

[0141] Referring to step (1), different stakeholders may have different threat model output needs, so different model types can be built using system 100 and the methods described herein. For examples, software application developers, operations teams, embedded system teams, IoT device teams, cloud deployment and architecture teams, ICS system or cyber-related system teams, and so forth, may create different threat model types. Architects may model threats to a residential structure, structural engineers may model threats to occupants, neighborhood planners may model supporting infrastructures needed for developments, and so forth. Home decorators may model occupant flow and so determine the most secure places for expensive home décor. In non-computing systems/process that are modeled, the protocols may represent things other than communication – for example in the home décor example the protocols may represent methods of moving an occupant between rooms. In implementations a user may select one of many model types to begin with (to populate the proper predefined components with which to diagram the model). This could be selecting, by example, from among examples such as the following: application threat model; operational threat model; cloud threat model; embedded threat model; IoT threat model; cyber-physical system threat model; and so forth. A user may still access all components in the diagram interface by searching for them but selecting the proper model may allow the most relevant components to populate at the top of the list.

[0142] Still referring to step (1), a user may in implementations also select role-based threat model outputs (such as with yes/no selectors) such as: secure coding requirements; operational checklists; executive metrics; executive reporting; security metrics; security reporting, and so forth, and these may also affect the position of components within the toolbox list on the diagram interface. In other implementations these selections (and the selections in the above paragraph) may only be used for record-keeping purposes. The input may also include the name of the model, the version, the name of the model creator, the date created, the update person, the update date, comments, desired objectives by development/operations/security/executives/business leaders, and others, and notes or toggle elements to indicate whether those objectives are met, in progress, or in some other state (and any or all of these features may be included on one or more of the already-described interfaces).

[0143] A representative example of the aforementioned step (3) is illustrated in FIG. 20, which may involve the classification of assets which may be associated with, located nearby or relevant to, or utilized by diagrammed components. In implementations the asset classification for each asset includes: an asset class; an asset, and; an associated component. In implementations the asset classification may be used as an input for analyzing potential attackers by providing insight to possible purposes attackers may have in targeting the asset. As an example, in implementations of cybersecurity modeling the assets may be classified as: non-confidential data; confidential consumer data; confidential corporate data; system capabilities (such as electronic funds transfers); non-digital assets (such as infrastructure or IT-system controlled equipment, and so forth. In a residential security model the classification could be: lightweight valuables; heavy weight valuables; personal information; life and health of occupants; residential structure/utilities; home security (entry keys/codes), etc.

[0144] Step (5) has already been described to some extent previously with respect to FIG. 17 with the creation of an attack tree (a partial attack tree is shown in FIG. 17 – a full attack tree would include all assets as topmost nodes, and in implementations the attack tree may be similar or identical to the “threat tree” shown in FIG. 14 of the ‘021 Application). Referring to FIG. 17, the attack vector connects the asset with the component from which the threat emanates, and this association was determined by the previous classification step. In implementations the attack/threat tree may be simplified by only showing one topmost node (one asset) and only its associated components and threats. In implementations the attack tree only shows three levels – the topmost level being the assets, the middle level being components, and the bottom level being threats. This model can be simplified further to have only two levels – the topmost level includes asset/component pairings, and the bottom level shows the threats. In this simplified model the attack tree may show the asset identified as being nested within a component or otherwise attached or coupled with it (in implementations the topmost level would then show, for example, component 1 including asset 1 in level 1, component 2 including asset 1 in level 1, component 3 including asset 1 in level 1, etc., with level two (the bottom level) showing the threats coupled with the components. As a representative example, the asset could be jewelry, the components could be a front door, a back door, and a window, and a threat to the front door could be a bump-key, and since an attacker may use a bump-key to enter the front door, the bump-key is a threat to the asset.

[0145] Step (5) includes a second part, which is analyzing the identified threats. In implementations this involves various stages. One stage includes creating a profile for each

threat. This may include utilizing real-world threat intelligence to provide attributes to said threats, and the attributes may include defined technical means to exploit the threat. A numerical value may be assigned to this means attribute (a high value indicating a higher level of technical means required to exploit the threat. This means attribute may also include the requisite skill, toolset, social network, financial backing, etc. the attacking entity would need to utilize the threat and transverse the corresponding attack vector. As examples, the technical means for the aforementioned bump-key against the front door is relatively low, whereas the technical means to alternatively burrow through the home's foundation to bypass other security controls is relatively high.

[0146] Another threat attribute is the access required to carry out the attack. A number is assigned to the access attribute, with a high number indicating a higher required level of access. A low access attribute may for example be attached to lower level employee's alphanumeric password (which may be known by an immediate supervisor), while a high access attribute may be attached to biometric signatures for key personnel (which may require high access levels such as a privileged system administrator).

[0147] Another threat attribute is a defensive distance, or number of security controls and their effectiveness, between a threat and the asset. A high numerical value indicates a greater number of effective security measures in between. Another threat attribute is the potential impact if the threat is realized – a high value indicates a high technological or business impact in the event the threat is realized.

[0148] The second stage involves analyzing the attacker population. Two methods are disclosed herein. In one method (the preferred method), potential attackers are analyzed based on the identified threats and identified associated assets. The other method allows users to adopt existing threat intelligence about known attackers who have utilized existing threats (for example data of a 30% chance of a home invasion in any given year compared with a 1 in 20 million chance of a terrorist attack at the home). In the preferred method objective attributes and characteristics of attackers are provided even where such intelligence is not known.

[0149] The third stage involves determining a likelihood of a threat being realized. When the above preferred method is utilized this includes three sub steps of determining a subset of the attacker population with the sufficient means, sufficient motivation, and sufficient opportunity to exploit the threat, to determine the probability of an attacker subset coming from the attacker population (this discards attackers who would be unable to exploit the threat for whatever reason) (if the other method is used the statistically-provided probability is used). A

determination is then made of whether the asset is attractive to the attacker, if not the likelihood of threat exploit is set to a minimum value, but if it is attractive the likelihood of threat exploit is the product of an attacker coming from the attacker population and the level of attraction. The next step calculates the product of the impact should the identified threats be realized and the likelihood of the threats being realized for each threat. Each threat is then prioritized according to some scheme (e.g., critical, high, moderate, etc.).

[0150] Step (6) involves analyzing attackers using means, motive, and opportunity (as identified above, in the preferred embodiment this occurs partway through step (5) – but if real world intelligence is used this step is obviated and skipped. If the attacker lacks either sufficient means, or sufficient motivation, or sufficient opportunity to conduct an attack, the attacker is disregarded, whereas if the attacker has all three the attacker is included in the organizational attacker population. These determinations could be done, for example, by any known or discovered method to assign a meaningful and relevant value to each category, and if the value of the attacker’s technical means meets or exceeds the above set technical means value (and similarly for a motivation value compared with the above identified access level value and an opportunity value compared with the above identified defensive distance value) then the attacker is included in the organizational attacker population, otherwise not.

[0151] Step (7) has previously been described with respect to FIG. 5.

[0152] Step (8) includes reviewing the threat report after all of the above steps have been done. Step (9) involves comparing the outputs obtained from the threat model and process relative to the desired outputs and desired objectives indicated in step (1). In implementations steps (1) and (9) may be done through system interfaces. In other implementations they may simply be done manually. In still other implementations they may both be excluded.

[0153] Referring now to FIG. 21, a representative example of attack simulation methods is shown. FIG. 21 shows the methods illustrated using the diagram interface 1000, though in other implementations the methods may be implemented using a separate interface that takes the components diagrammed in any given threat model and displays them in a separate interface just for the purpose of illustrating attack vectors. In FIG. 21 it is to be understood that the user has previously identified, through the database, the ONE DRIVE element as an asset. In other implementations the asset could be linked to the ONE DRIVE component but could be displayed as its own separate component – for example a “client info database file” shown next to or within the ONE DRIVE component (though in such a case the “asset” itself would be a

“component” as that term is used herein). In the shown implementation the ONE DRIVE component itself is identified as the asset.

[0154] A number of dashed protocol lines are shown in FIG. 21. These are shown in this fashion after the user has selected the ONE DRIVE component and made a selection to show all threats that could compromise the component. For example, this could be done in implementations by right-clicking on the ONE DRIVE component and selecting a selector such as “Show Attack Paths,” though the attack paths may be shown using other methods that the practitioner of ordinary skill in the art may determine. Once the selection is made, all threats reaching the ONE DRIVE component are highlighted in some manner. In the representative example they are highlighted by showing dashed and “moving” arrows, meaning an animation which shows the dashed portions of the lines as moving in one direction or another. In some implementations this animation could show the dashes moving in the direction towards the asset, which may assist the user to trace attack paths back to the outermost threats. In other implementations the arrows could be reoriented when the attack paths are shown so that the arrow tips all point downstream towards the asset, which may also assist the user to trace attack paths back to outermost threats. In implementations the attack paths are shown in a different color and/or using a greater line thickness than other protocol lines. In implementations the attack paths are shown in bright red and using thick lines while non-compromised paths are shown in thin black lines.

[0155] It can be seen that there are threats associated with the WIFI ACCESS POINT and with the SHARE POINT components, and that these threats reach the ONE DRIVE component through OFFICE 2010 and IE11 components. There are a number of potential compensating controls in the diagrammed system which may be utilized to mitigate these threats. For example, the laptop component group is shown including the MCAFEE HIPS, MCAFEE AV VSE, BIT LOCKER, and MCAFEE DLP compensating controls, and there is also an SSO compensating control diagrammed between the IE11 and ONE DRIVE components. All compensating controls in this diagram are shown as having an icon of a padlock on them so that the user can easily view the compensating controls to modify the threat model and the attack simulation (the compensating controls in implementations do not introduce any new threats but only mitigate threats).

[0156] Referring now to FIG. 22, in this screen the user has toggled the MCAFEE AV VSE and SSO elements to an ON configuration. In implementations this is done by right-clicking each component and selecting “BLOCK” from a menu, which then changes all attack paths that are mitigatable by the selected compensating control to a mitigated display state (in some

implementations the user may be able to select which attack paths are mitigatable from this interface). In FIG. 22 these compensating controls are highlighted by outlining them in a thicker line to show that they are turned on (though this display may be excluded in other implementations). The attack paths that are mitigated by the compensating controls that have been toggled to an ON state (or to a blocking state) are now shown as solid lines again, while those that are not mitigated are still shown in dashed format. In implementations the mitigated attack paths are shown in a thick green line. The user may reselect the compensating controls and select unblock to revert the threat model to the previous state. The user may also delete any given compensating control from the diagram altogether, and this will have the effect of changing any attack paths that were mitigated by that compensating control to an unmitigated display state.

[0157] While the mitigated display state for attack paths are described herein as green and bold and the unmitigated display state for attack paths are described as dashed, red, bold and animated, the practitioner of ordinary skill in the art could select other visual techniques to differentiate attack paths from non-attack paths and mitigated attack paths from non-mitigated attack paths. When a user toggles a compensating control to an ON state this may have the effect of dynamically changing the threat report, the compensating control report, the mitigations interface, and so forth by toggling relevant threats to mitigated (and toggling the same compensating control to the OFF state or removing it altogether from the diagram may have the opposite effect). In implementations one or more of the user interfaces (such as those of FIGS. 21-22) may allow user selection of certain threat sources and deselection of others, so as to only show attack paths of threats associated with a selected subset of the diagrammed components. The threats are shown in FIGS. 21-22 as emanating from outermost components (and the system/method may default to checking for threats at all outermost nodes), but in implementations they could emanate from internal sources (such as a USB port in an internal system administrator computer being a threat source for a virus). An attacker could be visually displayed at each threatened component, for example an “attacker” component could be placed on the diagram coupled with the WIFI ACCESS POINT and SHAREPOINT components to indicate the presence of an attacker. In other implementations the attacker need not be displayed in this way, but the user may understand that an attacker is reaching for the asset through the end points from where the threats are shown emanating on the diagram. From these end point components, or from an actual “attacker” component, the user may edit an attack profile (such as to indicate along a spectrum from a low funded individual hacker all the

way to a state sponsored team of skilled and well-funded hackers) and this may modify the attack paths. For example, if the latter profile is identified then certain compensating controls may not mitigate the threats (for example the SSO element may not be effective, and another compensating control would be needed instead), and accordingly when the profile is changed one or more of the attack paths may change to a mitigated or unmitigated display state in response. The identification of hacker type may be done, for example, through dropdown lists, checkmark items, and so forth that had been previously set through the database by the user, and the ability of a compensating control to mitigate threats by lower-end attackers but not higher-end attackers may also be defined/set through the database in the input interfaces previously described (though using selectors not shown—but which the practitioner of ordinary skill in the art will know how to implement).

[0158] In implementations another interface may allow the user to get a list of all threats which may compromise the asset and all attack paths associated with those threats. The asset has been described above as being anything of value to the user, it could for example be a database, a financial asset, a trade secret (or files related to trade secrets), and so forth.

[0159] One more comment is made here with respect to threat model chaining. The user may select a sub-component or component group (for example the user could right click the WINDOWS 7 component in FIG. 22) and select an “open in new window” selector to open a new diagram interface showing the diagram just for that component group. The user may then view just the threats associated with the component group, using previously identified methods, and/or may identify assets within the component group (for example OUTLOOK 2010) to show attack paths related just to this component. In implementations a user may right click or otherwise select a component group on an existing threat model by selecting a box outlining the component group and then select a “show threats” or other menu item to treat the entire component group as an asset and to show all attack paths thereto.

[0160] In implementations the designation of a component as an asset is done as simply as clicking on any component and selecting a “show threats” or similar menu item from a list. In other implementations a component may be designated as an asset by another mechanism and/or using another interface. The asset may be selected and its features edited, as well, as detailed to some extent above (for example some of the asset classification may be done here, though this may alternatively be done using one or more other interfaces). The attack simulation systems and methods herein allow a user to obtain a thorough understanding of

threats and risks to multi-faceted systems/processes, and the impact to relevant assets, should potential threats be realized.

[0161] Although the examples of computing system models have been described in detail, system 100 may be utilized to model other threats. For example, referring to a disease epidemic threat model, the threats may be sources or ways the disease may spread, the security requirements may be methods or elements to reduce the effects of those sources, such as sterilizing surgery instruments, washing hands, using air filters, breathing masks, gloves, and the components may be steps or interactions that occur with respect to persons who may be infected, such as admitting them, dealing with infected clothing, performing medical operations on them, etc. In such a scenario the threat model may have no components, threats, or security requirements that relate directly to computing devices or systems, though the threat may be modeled on system 100 which utilizes computing devices. The same may be said for the aforementioned threat model of commuting to work. Numerous other threat models, involving any of myriad types of threats, could be modeled using system 100. Other types of threat models could include: modeling physical and technology threats to airplanes, smart homes, smart TVs, an electric grid, and so forth.

[0162] Accordingly, the system and interfaces described herein allow a user to model a variety of systems, applications, and processes to determine threats and to mitigate those threats. The user may, at any time, delete any security requirement component (which may be a compensating control component) from a diagram and then generate the threat report again to revert to the threat statuses prior to mitigation by any particular component. This is one way in which step 518 of FIG. 5 may be accomplished, since removing the mitigating component will revert the mitigated threats back to the open status (except for threats which are also mitigated by another mitigating component). In implementations there may be other ways to “roll back” the threat report to an earlier status, such as with one or more selectors on the threat report itself to revert to an earlier configuration, or one or more “back” selectors on the diagram interface, and so forth.

[0163] Utilizing the methods and systems described herein an organization or individual can quickly and efficiently model deployed or contemplated systems, applications and/or processes and assess relevant threats to determine a mitigation strategy. The user may assess new threats to the entire attack surface of a system, application or process as the new threats arise and accordingly develop modified mitigation strategies with minimal disruption to existing operations. Additionally, the methods and systems described herein allow users to study the

ability of a compensating control to block new or existing threats without penetration testing (pen-testing), which can be resource-intensive, slow, and not as thorough as desired. The systems and methods also allow assessment of future compensating controls which have not yet been implemented (and accordingly where penetration testing is not yet an option). Any of the threat modeling described herein may utilize existing threat modeling methodologies including STRIDE, P.A.S.T.A., TRIKE, OCATAVE, and/or VAST methodologies, which may include modeling the system, application or process as a data flow diagram (DFD) or a process flow diagram (PFD). The methods and systems herein integrate well with agile and DevOps development environments, and allows a threat modeling process which is simple enough to allow non-security experts to participate in the threat modeling process and to benefit from the outputs of the system/method.

[0164] In implementations a compensating control record in the database may include a definition or details which include: an articulation of the rigor and intent of a prescribed security requirement which the compensating control is meant to satisfy; a defensive level of the compensating control; security and defensive capabilities of the compensating control, and; additional risk imposed by not adhering to the prescribed security requirement.

[0165] Systems and methods described herein may have other features that have not been described in detail. Users may be able to access the interfaces of the system through a web page, as described, and may be able to register using user accounts, with login credentials, functionality for retrieving lost passwords etc. Individual users may be able to import custom libraries and other elements into the database including custom components, threats, threat agents, test cases, security requirements, code snippets, code reviews, data elements, roles (developer, customer, user, admin, etc.), widgets, component types, attributes, templates, threat models, and the like. In implementations widgets may be a subset of components and may include reusable modular components that may be included in some components. Some examples of widgets may be, by non-limiting example: forms, cookies, banners, embedded video, RSS feeds, SMS functionality, SILVERLIGHT, secure hardware token, file upload, XML parser, and so forth. Widgets may be associated with threats through the database, using an interface similar to interface 600 (but accessible by selecting “widgets” from interface 700), and may be added to any diagram in the same way that components are added, which may include defining communication protocols between the widget and other components/widgets. Widgets may in implementations comprise identifying information about a component, user

roles which can interact with a component, and the means by which the component receives, transmits, or stores data elements.

[0166] In implementations a software installation on one or more computing device to implement the systems and methods may include storing in the database default libraries, such as over 650 threats, and a number of standard or default definitions for components, default risk levels to choose from, though the user may set up custom threats and associations through the database (which essentially sets up custom risk algorithms), custom risk levels to choose from, and so forth, as described above. The ability of the user to diagram a system, application or process visually allows for non-security experts to analyze threats using a threat model. In implementations, previously generated diagrams may be able to be imported into the system using a PDF or VIZIO drawing.

[0167] In implementations the system is configured to interface with third-party software applications and libraries (including software as a service (SAAS)) services, by communicating with the third-party software/library using its application programming interface (API). This may be used, for example, to store standards from standards-issuing bodies in the database and to associate them with security requirements and/or compensating controls through the database. This may assist a user to determine when a component added to a diagrammed threat model would qualify as a compensating control as defined by the standards issuing body. The system may be said to include a “contextual threat engine,” which is the underlying database relations allowing the system to dynamically update the threat model each time a component is mapped onto the canvas, or connected with another component using a communication protocol, or when a protocol is changed or deleted, or a component removed, etc. The systems and methods described herein facilitate comprehensive enterprise-level attack surface analysis. Different users may use different interfaces within an organization in some implementations. Information technology (IT) professionals may define the actors, threats, components, etc. specific to an organization, non-IT professionals may map out systems using the canvas, executives may review the high-level threat details included in the home page or threat model, and so forth (though in other organizations any user may use any interface).

[0168] In implementations one or more user inputs may be used using one or more user interfaces to import a threat model from a third-party software or database into the system. When this is done an administrator may map components or elements of the imported threat model to stored components of the system so that the relevant threats and etc. will be included in the imported threat model. Along these lines, it is pointed out here that both end users and

administrators are “users” of the system as that term is used herein. Accordingly, when the claims refer to “one or more user inputs” these inputs may be carried out by an end user and/or they may be carried out by an administrator, such as an administrator maintaining a cloud database which several different end users are accessing to implement different deployments of the method/system.

[0169] It is further pointed out that systems and methods disclosed herein may use multiple computing devices, interfaces, displays, databases, and so forth. For example, any attack simulation system disclosed herein could include multiple computing devices (each having at least one display) and multiple databases in which data is stored, accessed, and manipulated using multiple interfaces displayed on the displays of the computing devices. The computing devices may be remote from one another and coupled with the database(s) through the Internet and/or locally. Any attack simulation methods and/or threat model chaining methods disclosed herein may include receiving user inputs at multiple interfaces displayed on displays of multiple computing devices coupled with multiple databases to accomplish the method(s) at least in part by storing, accessing and manipulating data in the databases. By non-limiting example, in implementations an administrator could access the one or more databases using an administrator computer to input threat model components, threats, compensating controls, and the like, and associate these elements with one another (and also may create some default threat models which the user may use or manipulate – for example an “ATM” threat model by non-limiting example which an end user could use or include in his/her own diagrammed system, application or process), while an end user could access the one or more databases using a separate remote computer to diagram a system, process or application and thereby generate a threat model to be displayed on the end user computer.

[0170] In places where the description above refers to specific embodiments of system and method of including compensating controls in a threat modeling process, one or more or many modifications may be made without departing from the spirit and scope thereof. Details of any specific embodiment/implementation described herein may, wherever possible, be applied to any other specific implementation/embodiment described herein.

PATENT ASSIGNMENT COVER SHEET

Electronic Version v1.1
 Stylesheet Version v1.2

EPAS ID: PAT5295727

SUBMISSION TYPE:	NEW ASSIGNMENT	
NATURE OF CONVEYANCE:	ASSIGNMENT	
CONVEYING PARTY DATA		
	Name	Execution Date
	ANURAG AGARWAL	12/16/2018
RECEIVING PARTY DATA		
Name:	THREATMODELER SOFTWARE INC.	
Street Address:	101 HUDSON ST., STE. 2100	
City:	JERSEY CITY	
State/Country:	NEW JERSEY	
Postal Code:	07302	
PROPERTY NUMBERS Total: 1		
	Property Type	Number
	Application Number:	16228738
CORRESPONDENCE DATA		
Fax Number:	(801)317-8889	
<i>Correspondence will be sent to the e-mail address first; if that is unsuccessful, it will be sent using a fax number, if provided; if that is unsuccessful, it will be sent via US Mail.</i>		
Phone:	8017195229	
Email:	paul@pauljohnsonlaw.com	
Correspondent Name:	PAUL B. JOHNSON	
Address Line 1:	8483 S 1275 E	
Address Line 4:	SANDY, UTAH 84094	
ATTORNEY DOCKET NUMBER:	THREATM008	
NAME OF SUBMITTER:	PAUL B. JOHNSON	
SIGNATURE:	/Paul B. Johnson/	
DATE SIGNED:	12/20/2018	
	This document serves as an Oath/Declaration (37 CFR 1.63).	
Total Attachments: 4		
source=PATAssign3#page1.tif		
source=PATAssign3#page2.tif		
source=PATAssign3#page3.tif		
source=PATAssign3#page4.tif		

PATENT ASSIGNMENT

This Assignment is made and executed by Anurag Agarwal having an address of 149 Essex Street, #4B, Jersey City, NJ 07302 (hereinafter "Assignor"), to and in favor of ThreatModeler Software Inc., a New Jersey corporation having an address of 101 Hudson St., Ste. 2100, Jersey City, NJ 07302 (hereinafter "Assignee").

Whereas Assignor desires to assign his/her/its entire right, title and interest in and to the invention(s) and subject matter described in the United States nonprovisional utility patent application titled "Threat Model Chaining and Attack Simulation Systems and Related Methods" which was filed on Dec. 20, 2018 and assigned Application Serial No. 16/228,738 (hereinafter the "Patent Application") and all patents, patent applications and the like on the invention(s) or the subject matter of the Patent Application to Assignee for the territory of the United States of America (hereinafter "U.S.") and all foreign countries, for valuable consideration, and whereas Assignee has provided such good and valuable consideration to Assignor, the receipt and sufficiency of which Assignor hereby acknowledges; accordingly, Assignor hereby warrants, covenants, and agrees as follows:

1. Assignor hereby sells, assigns, conveys, transfers, and sets over to Assignee, its successors, legal representatives and assigns his/her/its entire right, title and interest in and to: (a) the Patent Application itself; (b) every U.S. patent that has issued or that issues and that is based in whole or in part on the Patent Application or the subject matter thereof, including every non-provisional, divisional, continuation, continuation-in-part, reissue, reexamination, substitution, extension, counterpart and the like; (c) every U.S. patent application, already filed or to be filed, that is based in whole or in part on the Patent Application or the subject matter thereof, including every counterpart, divisional, continuation, continuation-in-part, provisional, non-provisional, reissue, reexamination, extension, substitution and the like; (d) every non-U.S. patent, inventor's certificate, utility model, design and every like property or right that has issued or that issues and that is based in whole or in part on the Patent Application or the subject matter thereof, including every provisional, non-provisional, divisional, continuation, continuation-in-part, substitution and the like; (e) every non-U.S. application for a patent, inventor's certificate, utility model, design or like property or right, filed or to be filed, that is based in whole or in part on the Patent Application or the subject matter thereof, including every divisional, continuation, continuation-in-part, non-provisional, provisional, substitution and the like, and; (f) all priority rights, Convention rights and like benefits in the U.S. and every foreign country related to the Patent Application, the subject matter thereof, or any application or issued or granted property or right described in this section 1, including but not limited to any and all rights under the Paris Convention, the Patent Cooperation Treaty and any other international agreements to which the U.S. adheres.

2. Assignor agrees that Assignee may apply for patents, utility models, designs, inventor's certificates and the like, in the U.S. and in all foreign countries, based in whole or in part on the invention(s) or the subject matter described in the Patent Application or any other application or issued or granted property or right described in section 1 above. Assignor hereby grants to

Assignee the sole and exclusive right to prosecute the Patent Application and every application described in section 1 above as well as any and all opposition proceedings, reissue applications, reexaminations, supplemental examinations, nullity proceedings, invalidity proceedings, pre-grant opposition proceedings, and the like. Assignor authorizes all U.S. and foreign governmental bodies, including the U.S. Patent and Trademark Office (hereinafter "USPTO"), having the power and/or authority to issue patents, inventor's certificates, designs, utility models, or the like based in whole or in part on the Patent Application or the subject matter thereof, or any application or issued or granted property or right described in section 1 above, to issue such in the name of Assignee or, as the case may be, Assignee's successors, legal representatives or assigns.

3. Assignor grants to Assignee, its successors, legal representatives, and assigns, the exclusive right to sue third parties for present and past damages related to the invention(s) and the subject matter described in the Patent Application and any application or issued or granted registration or like property or right described in section 1 above.

4. Assignor warrants and covenants that he/she/it has the full and unencumbered right to sell, assign, convey, transfer and set over the interests hereby sold, assigned, conveyed, transferred and set over, and that he/she/it has not executed and will not execute any document or instrument in conflict with this Assignment.

5. Assignor further covenants and agrees that, upon request and without further consideration, but at the expense of Assignee, he/she/it will: (a) assist Assignee in prosecuting the Patent Application and each application described in section 1 above as well as opposition proceedings, reissue applications, reexaminations, supplemental examinations, nullity proceedings, invalidity proceedings, pre-grant opposition proceedings and the like; (b) provide Assignee with information concerning the invention(s) and the subject matter described in the Patent Application and each application and issued or granted property or right described in section 1 above; (c) execute, sign and deliver papers, make all rightful oaths and testify in any legal proceedings related to the Patent Application or any application or issued or granted property or right described in section 1 above; (d) execute additional assignment documents in favor of Assignee, similar to this Assignment, for each application and each issued or granted property or right described in section 1 above, and; (e) perform all other reasonably necessary acts; to enable Assignee to obtain, secure, maintain, perfect, protect and enforce all of the rights, title and interest sold, assigned, conveyed, transferred and set over under this Assignment and to file and issue the Patent Application and each application and issued or granted property or right described in section 1 above in the name of Assignee as applicant and owner.

6. Assignee may assign any right, title and interest sold, assigned, conveyed, transferred and set over under this Assignment, in whole or in part, to any party.

7. All references herein to Assignee include any successors, legal representatives or assigns of Assignee.

8. The above-identified Patent Application was made or authorized to be made by Assignor. Assignor believes that he/she is the original inventor or an original joint inventor of a claimed invention in the Patent Application. Assignor acknowledges that any willful false statement made in this paragraph is punishable under 18 U.S.C. 1001 by fine or imprisonment of not more than five (5) years, or both.
9. Assignor hereby authorizes and requests any attorney of the Law Office of Paul B. Johnson, Customer number 145042, to insert, after execution of this Assignment, the above filing date and application number of the Patent Application and any further information necessary or desirable for purposes of recording this Assignment with the USPTO.
10. This Assignment shall be binding upon any and all successors, legal representatives, and assigns of Assignor.

Executed this 16 day of December, 2019 at Jersey City, NJ by:
(City and State)

Legal Name: Anurag Agarwal
Print or Type

Signature: 

Mailing Address: 101 Hudson St Ste 2100
Jersey City NJ 07302

Residence: ☐ Same as mailing address, or:
105 Greene St Unit 1801
Jersey City NJ 07302

CD Submission Review Results

Internal Worksheet Only - Do Not Scan

Application Number Receipt Date

☒ New Application ☐ Response To Notice Date Of Response

☐ Jumbo – Large tables are included on the CD

☒ **There are no problems with the CDs in the submission.**

Items checked below are to be selected in the PALM Pre-Exam CD problem list.

Omitted Items

☐	Files on compact disc are unreadable:
☐	Disc(s) of either set not readable:
☐	Disc(s) do not contain file names listed:
☐	Amended CD missing unamended files
☐	Missing compact discs

Missing Parts

☐	Disc(s) do not contain file names listed
☐	Discs contains files that are non-ASCII files:
☐	Only one copy of the CD, no duplicate:
☐	Wrong media type, e.g., CD-RW:
☐	The transmittal letter and specification do not list information:
☐	Both disc(s) contain unreadable files:
☐	One disc(s) contain unreadable files:
☐	Compact disc(s) contain viruses, but are still readable:
☐	EFS/Paper Submission:
☐	Table does not maintain data in proper alignment:
☐	Not proper subject matter for CD's:

Informality

☐	No statement in transmittal letter that CD's are the same:
☐	No incorporation by reference statement for the CD's:
☐	CD's not labeled "Copy 1" and "Copy 2":
☐	Deficient CD packaging:
☐	Deficient Labeling on CD's:
☐	The transmittal letter does not list information:
☐	The specification does not list information:
☐	Table less than 51 pages submitted on CD:

File Directory Attachment

☐	Copy of file directory listing is attached and should be mailed to applicant
☐	Copy of file directory listing is not attached
☐	Copy of file directory listing is not attached because it is over one page long

Additional Comments

Internal Worksheet Only - Do Not Scan

SCORE Placeholder Sheet for IFW Content

Application Number: 16228738

Document Date: 12/20/2018

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

- Drawing

At the time of document entry (noted above):

- USPTO employees may access SCORE content via eDAN using the Supplemental Content tab, or via the SCORE web page.
- External customers may access SCORE content via PAIR using the Supplemental Content tab.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY. DOCKET NO	TOT CLAIMS	IND CLAIMS
16/228,738	12/20/2018	2491	785	ThreatM008	20	3

CONFIRMATION NO. 3702

FILING RECEIPT

145042

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363



00000000103601242

Date Mailed: 02/06/2019

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Inventor(s)

Anurag Agarwal, Jersey City, NJ;

Applicant(s)

ThreatModeler Software Inc., Jersey City, NJ;

Assignment For Published Patent Application

ThreatModeler Software Inc., Jersey City, NJ

Power of Attorney: The patent practitioners associated with Customer Number 145042

Domestic Priority data as claimed by applicant

This application is a CIP of 15/922,856 03/15/2018 PAT 10200399
which is a CIP of 15/888,021 02/03/2018
which claims benefit of 62/507,691 05/17/2017
and claims benefit of 62/527,671 06/30/2017
and claims benefit of 62/530,295 07/10/2017
and claims benefit of 62/520,954 06/16/2017

Foreign Applications for which priority is claimed (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see <http://www.uspto.gov> for more information.) - None.

Foreign application information must be provided in an Application Data Sheet in order to constitute a claim to foreign priority. See 37 CFR 1.55 and 1.76.

Permission to Access Application via Priority Document Exchange: Yes

Permission to Access Search Results: Yes

Applicant may provide or rescind an authorization for access using Form PTO/SB/39 or Form PTO/SB/69 as appropriate.

If Required, Foreign Filing License Granted: 02/04/2019

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 16/228,738**

Projected Publication Date: 05/16/2019

Non-Publication Request: No

Early Publication Request: No

**** SMALL ENTITY ****

Title

Threat Model Chaining and Attack Simulation Systems and Related Methods

Preliminary Class

726

Statement under 37 CFR 1.55 or 1.78 for AIA (First Inventor to File) Transition Applications: No

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific

countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4258).

LICENSE FOR FOREIGN FILING UNDER
Title 35, United States Code, Section 184
Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The U.S. offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to promote and facilitate business investment. SelectUSA provides information assistance to the international investor community; serves as an ombudsman for existing and potential investors; advocates on behalf of U.S. cities, states, and regions competing for global investment; and counsels U.S. economic development organizations on investment attraction best practices. To learn more about why the United States is the best country in the world to develop

technology, manufacture products, deliver services, and grow your business, visit <http://www.SelectUSA.gov> or call +1-202-482-6800.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875						Application or Docket Number 16/228,738		
APPLICATION AS FILED - PART I								
(Column 1)		(Column 2)		SMALL ENTITY		OTHER THAN SMALL ENTITY		
FOR	NUMBER FILED	NUMBER EXTRA	RATE(\$)	FEE(\$)		RATE(\$)	FEE(\$)	
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	75		N/A		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))	N/A	N/A	N/A	330		N/A		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	380		N/A		
TOTAL CLAIMS (37 CFR 1.16(j))	20	minus 20 = *	x 50 =	0.00	OR			
INDEPENDENT CLAIMS (37 CFR 1.16(h))	3	minus 3 = *	x 230 =	0.00				
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00				
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00				
			TOTAL	785		TOTAL		
* If the difference in column 1 is less than zero, enter "0" in column 2.								
APPLICATION AS AMENDED - PART II								
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	x =	OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =	OR	x =	
	Application Size Fee (37 CFR 1.16(s))					OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR		
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
(Column 1)		(Column 2)		(Column 3)		SMALL ENTITY		
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE(\$)	ADDITIONAL FEE(\$)		RATE(\$)	ADDITIONAL FEE(\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	x =	OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	x =	OR	x =	
	Application Size Fee (37 CFR 1.16(s))					OR		
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					OR		
				TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3. ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20". *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3". The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.								

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

Feb 06, 2019 04:35:23 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	APP.FILE.REC	02/06/2019	ThreatM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://sportal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

Electronic Acknowledgement Receipt

EFS ID:	35849950
Application Number:	16228738
International Application Number:	
Confirmation Number:	3702
Title of Invention:	Threat Model Chaining and Attack Simulation Systems and Related Methods
First Named Inventor/Applicant Name:	Anurag Agarwal
Customer Number:	145042
Filer:	Paul B. Johnson
Filer Authorized By:	
Attorney Docket Number:	ThreatM008
Receipt Date:	26-APR-2019
Filing Date:	20-DEC-2018
Time Stamp:	18:35:24
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Preliminary Amendment	PreliminaryAmendment.pdf	137118	no	24
			4a69d4061add56db9fb85d143def3f23e5a a9141		

Warnings:

IriusRisk

Information:	
Total Files Size (in bytes):	137118
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

AMENDMENT/REPLY

Applicant: ThreatModeler Software Inc.

Docket No: THREATM008

Examiner: Ashokkumar B. Patel

Ser. No: 16228738

Filed: December 20, 2018

Group Art Unit: 2491

Title: Threat Model Chaining and Attack Simulation Systems and Related Methods

PRELIMINARY AMENDMENT UNDER 37 C.F.R. 1.115

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner:

This is a preliminary amendment under 37 C.F.R. 1.115.

Specification Amendments begin on page 2.

Remarks begin on page 24.

AMENDMENTS TO THE SPECIFICATION

Please make the following amendments to the specification, which amendments introduce no new matter.

Please replace paragraphs [0066], [0078], [0093], [0112], [0118], [0125], [0126], [0130], [0131], [0135], [0138], [0140], [0141], [0144], [0145], [0146], [0147], [0150], [0163], [0166], and [0170] with the following paragraphs:

[0066] As indicated, these are only examples of how to implement a threat modeling system, and many other layouts are possible. System 100 may also include many other elements which are not shown for brevity. In a small business or organization wherein only one computing device may be needed to do threat modeling, system 100 could be implemented using a single computing device 102 with a database 108 stored thereon, or with one computing device 102 coupled with a server 106 and database 108 through a local connection (wired or hardwired), or using a cloud-stored database that the users access through user interfaces through remote servers 122 and/or web servers 120. In an organization in which multiple computing devices may need to do threat modeling the system 100 could be implemented using a computing device 102 having the database stored thereon, or coupled through a local or Internet connection to a database 108 stored elsewhere within the organization's computing devices such as on a server 106 or remotely on remote servers 122 accessed via a web server 120, with other computing devices 112 and/or 116 coupled either directly with device 102 and/or 106 and/or through the telecommunication network 110. In implementations in which remote servers are utilized these may be scaled up to any needed number.

[0078] Reference will now be made to several example user interfaces which may be utilized to accomplish the above general processes and other processes as will be described. It

should be stressed that these are only examples, and that other user interfaces could be used to accomplish the methods. Similarly, although specific user interfaces are described with respect to specific functionalities (dropdown menus, buttons, fields, tags, text prediction, etc.), the practitioner of ordinary skill in the art will be able to mix and match these functionalities and/or use other functionalities with the user interfaces to make the user experience intuitive and easy. For example, in instances where a dropdown menu is present this could be replaced by a search field, or a radio button selection, and so forth. Nevertheless, the user interface implementations as depicted in the drawings are useful for a variety of reasons, as will be understood.

[0093] From any of the previously mentioned interfaces, if the user presses the home selector an interface similar to interface 1300 of FIG. 13 will be displayed, which lists all previously stored threat models by name and showing their version. Either column may be organized alphabetically or in reverse, and the PDF button will export the list to PDF. If any specific threat model is selected it will be highlighted and its associated threat report (threat report interface) 1302 will be displayed, which will be discussed hereafter. From the top menu items the user may select the new selector to create a new threat model, the edit selector to edit the name, version, risk level, an “internal” toggle, and labels associated with the selected threat model, a delete selector to delete the selected threat model, a diagram selector to view the diagram for the selected threat model, a report selector to export to PDF the threat report (which shows for each threat the threat name, source, risk level, status, and creation date), a threat tree selector to view a diagrammed threat tree, showing threats of the threat model, and other selectors already described.

[0112] When a group is formed the user may, using the right-side “general” dropdown, add a custom display name, select a container type (from container, trust boundary, collection, or some other option stored in the database previously by the user), select a component (for

example for the WINDOWS 7 the component “WINDOWS machine” is selected, which shows that some components stored in the database may include other components), select other display choices such as title and background/border color, and select a Common Platform Enumeration (CPE) identification from among a list previously stored in the database (for example in this case ID a version of WINDOWS 7 is selected) (the list of CPE IDs may be searched using filters to easily find the appropriate one), and the user may also add notes.

[0118] Referring again to FIG. 10, it may be seen that this diagram includes the MCAFEE DLP, BITLOCKER, MCAFEE HIPS, and MCAFEE AV VSE components grouped in the WINDOWS 7 group. The user may, for example have modeled the WINDOWS 7 group, then used the compensating controls selector at the top of interface 1000 to identify that there are certain threats that these components would mitigate. The user may then add those components to the WINDOWS 7 group by dragging them from the toolbox to a location within the group outline to add them to that group. Then, upon right clicking on any specific security requirement component, the user may select a “mitigations” selector which pops up mitigations interface (interface) 1100 as shown in FIG. 11. The user could add one of these components at a time and model the mitigations, generate a new threat report, then either remove that component or add another compensating control, and in this way test out various compensating controls. This is one way in which the system facilitates steps 512, 514, 516, 518, 520, and 522, among other steps, of FIG. 5.

[0125] A modeled “attack” as used herein is a modeled attempt by an adversarial entity to traverse the modeled system or process from an attack surface to one or more assets within the system or process. The routes from all potential attackers to a selected asset are the “attack vectors” or attack paths to that asset.

[0126] Referring now to FIG. 14, a block flow diagram illustrates steps that may be included in a general attack surface analysis. Step 1402 includes user generation of a diagram of a system or process, as has been described previously with respect to FIG. 10. Step 1404 includes system generation of a threat report for each component or component group and step 1406 includes system combination of the individual threat reports into a comprehensive threat report for the overall diagrammed system/process (this would include, for example, including threat report elements for nested or chained threat models, as has been explained above), and then steps 1408-1414 include steps which may occur in any 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).

[0130] In implementations one or more interfaces of system 100 may be utilized to list the top potential threats (such as the top ten potential threats), the top most vulnerable components, the composition of threats by risk type, the composition of threats by status (mitigated, unmitigated, open, etc.), and so forth. The data may of course be organized and displayed in many other ways. In implementations an interface could list each threat, list each threat risk level, and list the source(s) for each threat. In implementations each threat source listing may include a component and an underlying source, so for example one component may be associated with multiple sources of a threat. An example would be an online banking interface which is shown on a diagrammed threat model as a component, and

a threat may be a virus being introduced to the bank's environment through a breach in the banking interface, and one source of the threat may be a legitimate user who unwarily exposes the ATM to a virus on his/her computer, and another source of the threat may be an individual hacker seeking to introduce the virus to the banking environment, and another source of the threat may be a state-sponsored entity with high end mechanisms to seek to introduce the virus to the banking environment.

[0131] In implementations an interface of the system may list the most vulnerable components in ascending/descending order, along with the risk level for each listed component, the number of total threats to that component, and the number of open or unmitigated threats for that component. In implementations an interface of the system may list multiple data elements associated with components (for example user names, social security numbers, financial info, credit card numbers, employee ages, etc.) (in this case the component likely being a database housing the data), a data classification for each data element (such as confidential, restricted, public, etc.) and an exposure level for each data element (such as very high, high, low, etc.). In implementations an interface of the system may break down the risk levels by percentage, such as 45% very high risks, 25% high risks, 15% medium risks, and so forth. In implementations an interface of the system may break down risk status by percentage, such as 45% open threats, 25% closed threats, 30% mitigated threats, etc. In implementations an interface of the system may visually illustrate the number of threat introductions plotted versus time, such as the number of threat introductions by month.

[0135] 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. The arrows in FIG. 18 are shown in different formats so that they can be distinguished from one another. In other implementations they may all have the same

appearance. 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. It may be seen that a threat emanating from component G threatens to compromise component A (or the asset within or associated with component A), the attack vector 1802 passing through component F and component B to reach component A. A threat emanating from component E also threatens to compromise component A, the attack vector 1806 passing through component B to reach component A. A threat emanating from component D also threatens to compromise the asset, the attack vector 1804 passing through component C and component B to reach component A.

[0138] Changing the compensating controls in such a diagram could also change the other displays on other interfaces, for example the listing of top threats, listing of top ten most vulnerable components, other top ten listings, composition of threats by risk, composition of threats by status, composition of threats by source, composition of threats by other criteria, the overall threat model, the mitigations interface, the compensating control report, and so forth. This dynamic change of all interfaces allows the user to do “what if” analyses by adding/removing any compensating control and/or toggling any compensating control between ON/OFF states and then seeing how all the aforementioned displays/reports etc. change accordingly. The change may, for example, illustrate one or more threats as mitigated or closed instead of open or unmitigated, reduce the total number of open or unmitigated threats, reduce exposure levels of data elements, alter the percentages of threats by risk level (very high, high, medium, low, very low, etc.), alter the percentages of threats by status (open, closed, unmitigated, mitigated), or the reverse of all these, on any of the interfaces or reports of the system.

[0140] In implementations threat modeling and/or attack simulation methods may include the following steps: (1) generally defining a threat model (including model type, outputs to

be generated, and overall objectives for different stakeholders); (2) visually diagramming a system/process using database-stored components (including communication protocols and compensating controls); (3) classifying one or more data elements within a component (or associated with a component), and/or one or more components themselves, as assets; (4) identifying and enumerating potential threats to the assets based on the diagrammed components; (5) analyzing the identified threats (threat analysis); (6) identifying and analyzing potential attackers based on the threat analysis; (7) analyze the effectiveness of deployed or contemplated compensating controls to mitigate the potential threats; (8) analyze a threat model and attack surface as modified by compensating controls; and (9) measure and quantify the effectiveness of the model and/or method relative to the desired outputs and objectives previously determined. This is just one example of steps included in such methods, and other methods may exclude some of these steps, or include other steps, and so forth. In an implementation of the above steps, step (6) interrupts step (5), and in an alternative implementation step (5) is allowed to be completed without interruption. Furthermore, in implementations steps (7) and (8) may be iteratively bounced between during any given implementation, so that a user adds a compensating control then checks the outcome, toggles the configuration of the compensating control then checks the outcome, removes a compensating control then checks the outcome, moves a compensating control to a new location then checks the outcome, etc., before moving to step (9).

[0141] Referring to step (1), different stakeholders may have different threat model output needs, so different model types can be built using system 100 and the methods described herein. For example, software application developers, operations teams, embedded system teams, IoT device teams, cloud deployment and architecture teams, ICS system or cyber-related system teams, and so forth, may create different threat model types. Architects may model threats to a residential structure, structural engineers may model threats to occupants, neighborhood planners may model supporting infrastructures needed for

developments, and so forth. Home decorators may model occupant flow and so determine the most secure places for expensive home décor. In non-computing systems/process that are modeled, the protocols may represent things other than communication – for example in the home décor example the protocols may represent methods of moving an occupant between rooms. In implementations a user may select one of many model types to begin with (to populate the proper predefined components with which to diagram the model). This could be selecting, by example, from among examples such as the following: application threat model; operational threat model; cloud threat model; embedded threat model; IoT threat model; cyber-physical system threat model; and so forth. A user may still access all components in the diagram interface by searching for them but selecting the proper model may allow the most relevant components to populate at the top of the list.

[0144] Step (5) has already been described to some extent previously with respect to FIG. 17 with the creation of an attack tree (a partial attack tree is shown in FIG. 17 – a full attack tree would include all assets as topmost nodes, and in implementations the attack tree may be similar or identical to the “threat tree” shown in FIG. 14 of the ‘021 Application). Referring to FIG. 17, the attack vector connects the asset with the component from which the threat emanates, and this association was determined by the previous classification step. In implementations the attack/threat tree may be simplified by only showing one topmost node (one asset) and only its associated components and threats. In implementations the attack tree only shows three levels – the topmost level being the assets, the middle level being components, and the bottom level being threats. This model can be simplified further to have only two levels – the topmost level includes asset/component pairings, and the bottom level shows the threats. In this simplified model the attack tree may show the asset identified as being nested within a component or otherwise attached or coupled with it (in implementations the topmost level would then show, for example, component 1 including asset 1 in level 1, component 2 including asset 1 in level 1, component 3 including asset 1 in

level 1, etc., with level two (the bottom level) showing the threats coupled with the components). As a representative example, the asset could be jewelry, the components could be a front door, a back door, and a window, and a threat to the front door could be a bump-key, and since an attacker may use a bump-key to enter the front door, the bump-key is a threat to the asset.

[0145] Step (5) includes a second part, which is analyzing the identified threats. In implementations this involves various stages. One stage includes creating a profile for each threat. This may include utilizing real-world threat intelligence to provide attributes to said threats, and the attributes may include defined technical means to exploit the threat. A numerical value may be assigned to this means attribute (a high value indicating a higher level of technical means required to exploit the threat. This means attribute may also include the requisite skill, toolset, social network, financial backing, etc. the attacking entity would need to utilize the threat and traverse the corresponding attack vector. As examples, the technical means for the aforementioned bump-key against the front door is relatively low, whereas the technical means to alternatively burrow through the home's foundation to bypass other security controls is relatively high.

[0146] Another threat attribute is the access required to carry out the attack. A number is assigned to the access attribute, with a high number indicating a higher required level of access. A low access attribute may for example be attached to a lower level employee's alphanumeric password (which may be known by an immediate supervisor), while a high access attribute may be attached to biometric signatures for key personnel (which may require high access levels such as a privileged system administrator).

[0147] Another threat attribute is a defensive distance, or number of security controls and their effectiveness, between a threat and the asset. A high numerical value indicates a

greater number of effective security measures in between. Another threat attribute is the potential impact if the threat is realized – a high value indicates a high technological or business impact in the event the threat is realized.

[0150] Step (6) involves analyzing attackers using means, motive, and opportunity (as identified above, in the preferred embodiment this occurs partway through step (5) – but if real world intelligence is used this step is obviated and skipped). If the attacker lacks either sufficient means, or sufficient motivation, or sufficient opportunity to conduct an attack, the attacker is disregarded, whereas if the attacker has all three the attacker is included in the organizational attacker population. These determinations could be done, for example, by any known or discovered method to assign a meaningful and relevant value to each category, and if the value of the attacker's technical means meets or exceeds the above set technical means value (and similarly for a motivation value compared with the above identified access level value and an opportunity value compared with the above identified defensive distance value) then the attacker is included in the organizational attacker population, otherwise not.

[0163] Utilizing the methods and systems described herein an organization or individual can quickly and efficiently model deployed or contemplated systems, applications and/or processes and assess relevant threats to determine a mitigation strategy. The user may assess new threats to the entire attack surface of a system, application or process as the new threats arise and accordingly develop modified mitigation strategies with minimal disruption to existing operations. Additionally, the methods and systems described herein allow users to study the ability of a compensating control to block new or existing threats without penetration testing (pen-testing), which can be resource-intensive, slow, and not as thorough as desired. The systems and methods also allow assessment of future compensating controls which have not yet been implemented (and accordingly where

penetration testing is not yet an option). Any of the threat modeling described herein may utilize existing threat modeling methodologies including STRIDE, P.A.S.T.A., TRIKE, OCTAVE, and/or VAST methodologies, which may include modeling the system, application or process as a data flow diagram (DFD) or a process flow diagram (PFD). The methods and systems herein integrate well with agile and DevOps development environments, and allow a threat modeling process which is simple enough to allow non-security experts to participate in the threat modeling process and to benefit from the outputs of the system/method.

[0166] In implementations a software installation on one or more computing devices to implement the systems and methods may include storing in the database default libraries, such as over 650 threats, and a number of standard or default definitions for components, default risk levels to choose from, though the user may set up custom threats and associations through the database (which essentially sets up custom risk algorithms), custom risk levels to choose from, and so forth, as described above. The ability of the user to diagram a system, application or process visually allows for non-security experts to analyze threats using a threat model. In implementations, previously generated diagrams may be able to be imported into the system using a PDF or VIZIO drawing.

[0170] In places where the description above refers to specific embodiments of threat model chaining and attack simulation systems and related methods, one or more or many modifications may be made without departing from the spirit and scope thereof. Details of any specific embodiment/implementation described herein may, wherever possible, be applied to any other specific implementation/embodiment described herein.

Below please find the full text of the replacement paragraph(s) with markings to show all the changes relative to the previous versions:

[0066] As indicated, these are only examples of how to implement a threat modeling system, and many other layouts are possible. System 100 may also include many other elements which are not shown for brevity. In a small business or organization wherein only one computing device may be needed to do threat modeling, system 100 could be implemented using a single computing device 102 with a database 108 stored thereon, or with one computing device 102 coupled with a server 106 and database 108 through a local connection (wired or hardwired), or using a cloud-stored database that the ~~user~~ users access through user interfaces through remote servers 122 and/or web servers 120. In an organization in which multiple computing devices may need to do threat modeling the system 100 could be implemented using a computing device 102 having the database stored thereon, or coupled through a local or Internet connection to a database 108 stored elsewhere within the organization's computing devices such as on a server 106 or remotely on remote servers 122 accessed via a web server 120, with other computing devices 112 and/or 116 coupled either directly with device 102 and/or 106 and/or through the telecommunication network 110. In implementations in which remote servers are utilized these may be scaled up to any needed number.

[0078] Reference will now be made to several example user interfaces which may be utilized to accomplish the above general processes and other processes as will be described. It should be stressed that these are only examples, and that other user interfaces could be used to accomplish the methods. Similarly, although specific user interfaces are described with respect to specific functionalities (dropdown menus, buttons, fields, tags, text prediction, etc.), the practitioner of ordinary skill in the art will be able to mix and match these functionalities and/or use other functionalities with the user interfaces to make the user experience intuitive and easy. For example, in instances where a dropdown menu is present this could be replaced by a search field, or a radio button selection, and so forth.

Nevertheless, the user ~~interfaces~~ interface implementations as depicted in the drawings are useful for a variety of reasons, as will be understood.

[0093] From any of the previously mentioned interfaces, if the user presses the home selector an interface similar to interface 1300 of FIG. 13 will be displayed, which lists all previously stored threat models by name and showing their version. Either column may be organized alphabetically or in reverse, and the PDF button will export the list to PDF. If any specific threat model is selected it will be highlighted and its associated threat report (threat report interface) 1302 will be displayed, which will be discussed hereafter. From the top menu items the user may select the new selector to create a new threat model, the edit selector to edit the name, version, risk level, an “internal” toggle, and labels associated with the selected threat model, a delete selector to delete the selected threat model, a diagram selector to view the diagram for the selected threat model, a report selector to export to PDF the threat report (which shows for each threat the threat name, source, risk level, status, and creation date), a threat tree selector to view a diagrammed threat tree, showing threats of the threat model, and other selectors already described.

[0112] When a group is formed the user may, using the right-side “general” dropdown, add a custom display name, select a container type (from container, trust boundary, collection, or some other option stored in the database previously by the user), select a component (for example for the WINDOWS 7 the component “WINDOWS machine” is selected, which shows that some components stored in the database may include other components), select other display choices such as title and background/border color, and select a Common Platform Enumeration (CPE) identification from among a list previously stored in the database (for example in this case ID a version of WINDOWS 7 is selected) (the list of CPE IDs may be searched using filters to easily find the appropriate one), and the user may also add notes.

[0118] Referring again to FIG. 10, it may be seen that this diagram includes the MCAFEE DLP, BITLOCKER, MCAFEE HIPS, and MCAFEE AV VSE components grouped in the WINDOWS 7 group. The user may, for example have modeled the WINDOWS 7 group, then used the compensating controls selector at the top of interface 1000 to identify that there are certain threats that these components would mitigate. The user may then add those components to the WINDOWS 7 group by dragging them from the toolbox to a location within the group outline to add them to that group. Then, upon right clicking on any specific security requirement component, the user may select a “mitigations” selector which pops up mitigations interface (interface) 1100 as shown in FIG. 11. The user could add one of these components at a time and model the mitigations, generate a new threat report, then either remove that component or add another compensating control, and in this way test out various compensating controls. This is one way in which the system facilitates steps 512, 514, ~~518~~ 516, 518, ~~522~~ 520, and 522, among other steps, of FIG. 5.

[0125] A modeled “attack” as used herein is a modeled attempt by an adversarial entity to ~~transverse~~ traverse the modeled system or process from an attack surface to one or more assets within the system or process. The routes from all potential attackers to a selected asset are the “attack vectors” or attack paths to that asset.

[0126] Referring now to FIG. 14, a block flow diagram ~~illustrating~~ illustrates steps that may be included in a general attack surface analysis. Step 1402 includes user generation of a diagram of a system or process, as has been described previously with respect to FIG. 10. Step 1404 includes system generation of a threat report for each component or component group and step 1406 includes system combination of the individual threat reports into a comprehensive threat report for the overall diagrammed system/process (this would include, for example, including threat report elements for nested or chained threat models, as has been explained above), and then steps 1408-1414 include steps which may occur in

any 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).

[0130] In implementations one or more interfaces of system 100 may be utilized to list the top potential threats (such as the top ten potential threats), the top most vulnerable components, the composition of threats by risk type, the composition of threats by status (mitigated, unmitigated, open, etc.), and so forth. The data may of course be organized and displayed in many other ways. In implementations an interface could list each threat, list each threat risk level, and list the source(s) for each threat. In implementations each threat source listing may include a component and an underlying source, so for example one component may be associated with multiple sources of a threat. An example would be an online banking interface which is shown on a diagrammed threat model as a component, and a threat may be a virus being introduced to the bank's environment through a breach in the banking interface, and one source of the threat may be a legitimate user who unwarily exposes the ATM to a virus on his/her computer, and another source of the threat may be an individual hacker seeking to introduce [[to]] the virus to the banking environment, and another source of the threat may be a state-sponsored entity with high end mechanisms to seek to introduce the virus to the banking environment.

[0131] In implementations an interface of the system may list the most vulnerable components in ascending/descending order, along with the risk level for each listed component, the number of total threats to that component, and the number of open or unmitigated threats for that component. In implementations an interface of the system may list multiple data elements associated with components (for example user names, social security numbers, financial info, credit card numbers, employee ages, etc.) (in this case the component likely being a database housing the data), a data classification for each data element (such as confidential, restricted, public, etc.) and an exposure level for each data element (such as very high, high, low, etc.). In implementations an interface of the system may break down the risk levels by percentage, such as 45% very high risks, 25% high risks, 15% medium risks, and so forth. In implementations an interface of the system may break down risk status by percentage, such as 45% open threats, 25% closed threats, 30% mitigated threats, etc. In implementations an interface of the system may visually illustrate the number of threat introductions plotted versus time, such as the number of threat introductions by month.

[0135] 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. The arrows in FIG. 18 are shown in different formats so that they can be distinguished from one another. In other implementations they may all have the same appearance. 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. It may be seen that a threat emanating from component G threatens to compromise component A (or the asset within or associated with component A), the attack vector 1802 passing through component F and component B to reach component A. A threat emanating from component E also threatens to compromise component A, the attack vector 1806 passing through component B to reach component A. A threat emanating from

component D also threatens to compromise the asset, the attack vector 1804 passing through component C and component B to reach component A.

[0138] Changing the compensating controls in such a diagram could also change the other displays on other interfaces, for example the listing of top threats, listing of top ten most vulnerable components, other top ten listings, composition of threats by risk, composition of threats by status, composition of threats by source, composition of threats by other criteria, the overall threat model, the mitigations interface, the compensating control report, and so forth. This dynamic change of all interfaces allows the user to do “what if” analyses by adding/removing any compensating control and/or toggling any compensating control between ON/OFF states and then seeing how all the aforementioned displays/reports etc. change accordingly. The change may, for example, illustrate one or more threats as mitigated or closed instead of open or unmitigated, reduce the total number of open or unmitigated threats, reduce exposure levels of data elements, alter the percentages of threats by risk level (very high, high, medium, low, very low, etc.), alter the percentages of ~~treats~~ threats by status (open, closed, unmitigated, mitigated), or the reverse of all these, on any of the interfaces, ~~reports~~ or reports of the system.

[0140] In implementations threat modeling and/or attack simulation methods may include the following steps: (1) generally defining a threat model (including model type, outputs to be generated, and overall objectives for different stakeholders); (2) visually diagramming a system/process using database-stored components (including communication protocols and compensating controls); (3) classifying one or more data elements within a component (or associated with a ~~component~~ component), and/or one or more components themselves, as assets; (4) identifying and enumerating potential threats to the assets based on the diagrammed components; (5) analyzing the identified threats (threat analysis); (6) identifying and analyzing potential attackers based on the threat analysis; (7) analyze the effectiveness

of deployed or contemplated compensating controls to mitigate the potential threats; (8) analyze a threat model and attack surface as modified by compensating controls; and (9) measure and quantify the effectiveness of the model and/or method relative to the desired outputs and objectives previously determined. This is just one example of steps included in such methods, and other methods may exclude some of these steps, or include other steps, and so forth. In an implementation of the above steps, step (6) interrupts step (5), and in an alternative implementation step (5) is allowed to be completed without interruption. Furthermore, in implementations steps (7) and (8) may be iteratively bounced between during any given implementation, so that a user adds a compensating control then checks the outcome, toggles the configuration of the compensating control then checks the outcome, removes a compensating control then checks the outcome, moves a compensating control to a new location then checks the outcome, etc., before moving to step (9).

[0141] Referring to step (1), different stakeholders may have different threat model output needs, so different model types can be built using system 100 and the methods described herein. For ~~examples~~ example, software application developers, operations teams, embedded system teams, IoT device teams, cloud deployment and architecture teams, ICS system or cyber-related system teams, and so forth, may create different threat model types. Architects may model threats to a residential structure, structural engineers may model threats to occupants, neighborhood planners may model supporting infrastructures needed for developments, and so forth. Home decorators may model occupant flow and so determine the most secure places for expensive home décor. In non-computing systems/process that are modeled, the protocols may represent things other than communication – for example in the home décor example the protocols may represent methods of moving an occupant between rooms. In implementations a user may select one of many model types to begin with (to populate the proper predefined components with which to diagram the model). This could be selecting, by example, from among examples

such as the following: application threat model; operational threat model; cloud threat model; embedded threat model; IoT threat model; cyber-physical system threat model; and so forth. A user may still access all components in the diagram interface by searching for them but selecting the proper model may allow the most relevant components to populate at the top of the list.

[0144] Step (5) has already been described to some extent previously with respect to FIG. 17 with the creation of an attack tree (a partial attack tree is shown in FIG. 17 – a full attack tree would include all assets as topmost nodes, and in implementations the attack tree may be similar or identical to the “threat tree” shown in FIG. 14 of the ‘021 Application). Referring to FIG. 17, the attack vector connects the asset with the component from which the threat emanates, and this association was determined by the previous classification step. In implementations the attack/threat tree may be simplified by only showing one topmost node (one asset) and only its associated components and threats. In implementations the attack tree only shows three levels – the topmost level being the assets, the middle level being components, and the bottom level being threats. This model can be simplified further to have only two levels – the topmost level includes asset/component pairings, and the bottom level shows the threats. In this simplified model the attack tree may show the asset identified as being nested within a component or otherwise attached or coupled with it (in implementations the topmost level would then show, for example, component 1 including asset 1 in level 1, component 2 including asset 1 in level 1, component 3 including asset 1 in level 1, etc., with level two (the bottom level) showing the threats coupled with the ~~components~~ components). As a representative example, the asset could be jewelry, the components could be a front door, a back door, and a window, and a threat to the front door could be a bump-key, and since an attacker may use a bump-key to enter the front door, the bump-key is a threat to the asset.

[0145] Step (5) includes a second part, which is analyzing the identified threats. In implementations this involves various stages. One stage includes creating a profile for each threat. This may include utilizing real-world threat intelligence to provide attributes to said threats, and the attributes may include defined technical means to exploit the threat. A numerical value may be assigned to this means attribute (a high value indicating a higher level of technical means required to exploit the threat. This means attribute may also include the requisite skill, toolset, social network, financial backing, etc. the attacking entity would need to utilize the threat and ~~transverse~~ traverse the corresponding attack vector. As examples, the technical means for the aforementioned bump-key against the front door is relatively low, whereas the technical means to alternatively burrow through the home's foundation to bypass other security controls is relatively high.

[0146] Another threat attribute is the access required to carry out the attack. A number is assigned to the access attribute, with a high number indicating a higher required level of access. A low access attribute may for example be attached to a lower level employee's alphanumeric password (which may be known by an immediate supervisor), while a high access attribute may be attached to biometric signatures for key personnel (which may require high access levels such as a privileged system administrator).

[0147] Another threat attribute is a defensive distance, or number of security controls and their effectiveness, between a threat ~~and~~ and the asset. A high numerical value indicates a greater number of effective security measures in between. Another threat attribute is the potential impact if the threat is realized – a high value indicates a high technological or business impact in the event the threat is realized.

[0150] Step (6) involves analyzing attackers using means, motive, and opportunity (as identified above, in the preferred embodiment this occurs partway through step (5) – but if

real world intelligence is used this step is obviated and ~~skipped~~ skipped). If the attacker lacks either sufficient means, or sufficient motivation, or sufficient opportunity to conduct an attack, the attacker is disregarded, whereas if the attacker has all three the attacker is included in the organizational attacker population. These determinations could be done, for example, by any known or discovered method to assign a meaningful and relevant value to each category, and if the value of the attacker's technical means meets or exceeds the above set technical means value (and similarly for a motivation value compared with the above identified access level value and an opportunity value compared with the above identified defensive distance value) then the attacker is included in the organizational attacker population, otherwise not.

[0163] Utilizing the methods and systems described herein an organization or individual can quickly and efficiently model deployed or contemplated systems, applications and/or processes and assess relevant threats to determine a mitigation strategy. The user may assess new threats to the entire attack surface of a system, application or process as the new threats arise and accordingly develop modified mitigation strategies with minimal disruption to existing operations. Additionally, the methods and systems described herein allow users to study the ability of a compensating control to block new or existing threats without penetration testing (pen-testing), which can be resource-intensive, slow, and not as thorough as desired. The systems and methods also allow assessment of future compensating controls which have not yet been implemented (and accordingly where penetration testing is not yet an option). Any of the threat modeling described herein may utilize existing threat modeling methodologies including STRIDE, P.A.S.T.A., TRIKE, ~~OCATAVE~~ OCTAVE, and/or VAST methodologies, which may include modeling the system, application or process as a data flow diagram (DFD) or a process flow diagram (PFD). The methods and systems herein integrate well with agile and DevOps development environments, and allow ~~allows~~ a threat modeling process which is simple enough to allow non-security experts to

participate in the threat modeling process and to benefit from the outputs of the system/method.

[0166] In implementations a software installation on one or more computing ~~device~~ devices to implement the systems and methods may include storing in the database default libraries, such as over 650 threats, and a number of standard or default definitions for components, default risk levels to choose from, though the user may set up custom threats and associations through the database (which essentially sets up custom risk algorithms), custom risk levels to choose from, and so forth, as described above. The ability of the user to diagram a system, application or process visually allows for non-security experts to analyze threats using a threat model. In implementations, previously generated diagrams may be able to be imported into the system using a PDF or VIZIO drawing.

[0170] In places where the description above refers to specific embodiments of ~~system and method of including compensating controls in a threat modeling process~~ threat model chaining and attack simulation systems and related methods, one or more or many modifications may be made without departing from the spirit and scope thereof. Details of any specific embodiment/implementation described herein may, wherever possible, be applied to any other specific implementation/embodiment described herein.

CONCLUSION

If there are any questions, the Examiner is invited to contact an attorney of record using the contact information listed below.

Respectfully submitted,

Date: April 26, 2019 By: /Paul B. Johnson/
Paul B. Johnson
Reg. No. 59375

Law Office of Paul B. Johnson
8483 S 1275 E
Sandy, UT 84094-1363
Ph: 801.719.5229
Fax: 801.317.8889
paul@pauljohnsonlaw.com



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
16/228,738	12/20/2018	Anurag Agarwal	ThreatM008

CONFIRMATION NO. 3702

PUBLICATION NOTICE



OC000000108237643

145042
Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363

Title:Threat Model Chaining and Attack Simulation Systems and Related Methods

Publication No.US-2019-0147161-A1

Publication Date:05/16/2019

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Public Records Division. The Public Records Division can be reached by telephone at (571) 272-3150 or (800) 972-6382, by facsimile at (571) 273-3250, by mail addressed to the United States Patent and Trademark Office, Public Records Division, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <https://portal.uspto.gov/pair/PublicPair>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

May 17, 2019 03:38:00 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	NTC.PUB	05/16/2019	ThreatM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	12/20/2018	Anurag Agarwal	ThreatM008	3702
145042	7590	08/08/2019		
Law Office of Paul B. Johnson 8483 S. 1275 E. Sandy, UT 84094-1363			EXAMINER SONG, HOSUK	
			ART UNIT	PAPER NUMBER
			2435	
			NOTIFICATION DATE	DELIVERY MODE
			08/08/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

paul@pauljohnsonlaw.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(I)(1) - 706.02(I)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10200399. Although the claims at issue are not identical, they are not patentably distinct from each other (see table below).

<u>Instant Application</u>	<u>U.S. Patent No. 10200399</u>
Claim 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	Claim 1: A threat model chaining and system configuration method, comprising: In response to receiving one or more user inputs, using one or more interfaces displayed on a display of a computing device communicatively coupled with a database: storing a plurality of threat model components in the database; storing a plurality of threats in the database associating each threat with at least one of the threat model components through the database; storing a plurality of compensating controls in the database;

<p>with at least one of the threats through the one or more databases;</p> <p>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;</p> <p>configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representation of one or more of the threat model components and visual representation of one or more of the compensating controls, the relational diagram defining a first threat model, and;</p> <p>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.</p>	<p>associating each compensating control with at least one of the threats through the database;</p> <p>displaying , using a diagram interface, a relational diagram of a system, 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;</p> <p>adding a component group to the first threat model and thereby redefining 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, and;</p> <p><i>physically arranging tangible components matching the threat model components of the diagrammed system to form an actual system, the actual system mitigating actual threats corresponding with the threats of the first threat model.</i></p>
---	--

Although the conflicting claims are not identical, they are not patentably distinct from each other because both are directed to detecting threat using a plurality of threat model and configuring the diagram interface to display a relational diagram using one or more threat model; and only differing in that the claims of '399 patent explicitly recite physically arranging tangible components matching the threat model components of the diagrammed system to form an actual system, the actual system mitigating actual threats corresponding with the threats of the first threat model. Thus the claims of the '399 patent are rendered as obvious variants of the instant claims.

Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10255439. Although the claims at issue are not identical, they are not patentably distinct from each other (see table below).

<u>Instant Application</u>	<u>U.S. Patent No. 10200399</u>
Claim 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	Claim 1: A threat model and system configuration method, comprising: In response to receiving one or more user inputs, using one or more input interfaces displayed on a display of a computing device communicatively coupled with a database: storing a plurality of threats in the database; storing a plurality of threats in the database; associating each threat with at least one of the threat model components through the database; storing a plurality of security requirements in the database, including storing an indication of

<p>with at least one of the threats through the one or more databases;</p> <p>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;</p> <p>configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representation of one or more of the threat model components and visual representation of one or more of the compensating controls, the relational diagram defining a first threat model, and;</p> <p>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.</p>	<p>whether each security requirement is a compensating control;</p> <p>associating each compensating control with at least one of the threats through the database;</p> <p>displaying a relational diagram of a system, using visual representations of one or more of the threat model components, the diagram defining a threat model;</p> <p>generating and displaying a threat report displaying each threat that is associated through the databases with one of the threat model components included in the threat model, wherein the threat report displays a threat status for each threat indicating whether that threat has been mitigated, and wherein the threat report includes one or more input fields configured to manually change each threat status;</p> <p>generating and displaying a report displaying each compensating control that is associated through the database with one of the threats included in the threat report;</p> <p>removing one of the compensating controls from the diagram and automatically changing the threat status of at least one of the threats</p>
---	---

	<p>included in the threat report to an unmitigated status, and;</p> <p>physically arranging tangible components matching the threat model components of the diagrammed system to form an actual system, the actual system mitigating actual threats corresponding with the threats displayed in the threat report.</p>
--	--

Although the conflicting claims are not identical, they are not patentably distinct from each other because both are directed to detecting threat using a plurality of threat model and configuring the diagram interface to display a relational diagram using one or more threat model; and only differing in that the claims of '439 patent explicitly recite removing one of the compensating controls from the diagram and automatically changing the threat status of at least one of the threats included in the threat report to an unmitigated status, and physically arranging tangible components matching the threat model components of the diagrammed system to form an actual system, the actual system mitigating actual threats corresponding with the threats displayed in the threat report. Thus the claims of the '439 patent are rendered as obvious variants of the instant claims.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. Claim(s) 1-20 is/are directed to abstract idea. The claim(s) does/do not include additional elements that are sufficient to amount to significantly more than the

judicial exception because the claimed invention only appears to encompass various steps of organizing and manipulating information. The claimed concepts are not meaningfully different than those concepts found by the courts to be abstract ideas such as: comparing data to determine a risk level (*Perkin-Elmer*); collecting/analyzing information to detect misuse and notifying a user (*FairWarning v. Iatric*); collecting, displaying, and manipulating data (*Int. Ventures v. Cap One Financial*).

Independent claims 1,4,12 recites additional elements of computing device and system. These elements are recited at a high level of generality and are well-known components. These generic computer components are claimed to perform their basic functions of storing and processing data. Hence, these elements do not add significantly more to the abstract idea.

Dependent claims 2,3,5-11,13-20 incorporate such deficiencies and fail to remedy the findings stated herein, *supra*.

USPTO Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HOSUK SONG whose telephone number is (571)272-3857. The examiner can normally be reached on Mon-Fri: 7:30AM-5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on 571-272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available

Art Unit: 2435

through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/HOSUK SONG/

Primary Examiner, Art Unit 2435

<i>Notice of References Cited</i>	Application/Control No. 16/228,738		Applicant(s)/Patent Under Reexamination Agarwal, Anurag	
	Examiner HOSUK SONG		Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-10255439-B2	04-2019	Agarwal; Anurag	G06F16/904	1/1
*	B	US-10200399-B2	02-2019	Agarwal; Anurag	G06F21/577	1/1
*	C	US-9043924-B2	05-2015	Maor; Ofer	G06F11/3688	726/25
*	D	US-8413249-B1	04-2013	Chou; Andy C	G06F11/00	726/25
*	E	US-8407801-B2	03-2013	Ikegami; Michiyo	G06F21/577	726/25
*	F	US-6952779-B1	10-2005	Cohen; Gideon	G06F21/577	726/22
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

<i>Search Notes</i> 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/577; G06F21/552; G06F 21/554; G06FG06F 17/30283; H04L 63/1433; H04L 63/20	07/31/2019	HS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
EAST, foreign patent database, IBM TDB, USPGPUB, inventor name search	07/31/2019	HS
CPC search with keywords	07/31/2019	HS
NPL(IEEE) with keywords	07/31/2019	HS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
726	22-25	07/31/2019	HS

--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S75	2	((("10200399") or ("10255439")).PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2019/07/31 09:02
S76	16	("20060015941" "20060241991" "20110126111" "20110178942" "20140137257" "20180324207" "4959015" "7096502" "7433829" "7891003" "7900259" "8191139" "8255995" "8413237" "9497203" "9774613").PN.	US-PGPUB; USPAT	OR	OFF	2019/07/31 09:52
S77	16	("20060015941" "20060241991" "20110126111" "20110178942" "20140137257" "20180324207" "4959015" "7096502" "7433829" "7891003" "7900259" "8191139" "8255995" "8413237" "9497203" "9774613").PN.	US-PGPUB; USPAT	OR	OFF	2019/07/31 12:37
S78	539	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:41
S79	70367	(G06F21/577 OR G06F21/552 OR G06F21/554 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:49
S80	1	("agarwal, anurag").INV. and 726/\$.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:49
S81	6	(threats and database and diagram\$5 and model and control\$4 and (visual or display\$4)).CLM.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:51
S82	2691	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:53
S83	242	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record)	US-PGPUB; USPAT; FPRS;	OR	ON	2019/07/31 12:53

		and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	EPO; JPO; DERWENT; IBM_TDB			
S84	20	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/22.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:53
S85	49	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/23.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:54
S86	15	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/24.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:54
S87	78	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/25.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:55
S88	226	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 12:55
S89	144	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 13:21
S91	153	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 13:23
S92	127	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 13:23
S93	7	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 13:24

		packets) and 726/22.ccls.				
S95	4	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and 726/24.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 13:36
S96	18	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and 726/25.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 13:42
S97	168	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4 or NVIS or network adj3 visualization) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 13:43
S98	127	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4 or NVIS or network adj3 visualization) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 13:43
S99	18	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and 726/25.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 15:25
S100	127	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 15:26
S101	78	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/25.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 16:35
S102	11	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 18:39

		packets) and 726/23.ccls.				
S103	7	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and 726/22.ccls.	US-PGPUB; OR USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/07/31 18:42

8/ 1/ 2019 9:06:23 AM
C:\ Users\ hsong\ Documents\ EAST\ Workspaces\ 16228738.wsp

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number

Filing Date

First Named Inventor

Anurag Agarwal

Art Unit

Examiner Name

Attorney Docket Number

ThreatM008

U.S.PATENTS

[Remove](#)

Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
/H.S./	1	7891003	B2	2011-02-15	Mir	
/H.S./	2	7900259	B2	2011-03-01	Jeschke et al.	
/H.S./	3	9774613	B2	2017-09-26	Thomas et al.	
/H.S./	4	4959015		1990-09-25	Rasinski et al.	
/H.S./	5	7433829	B2	2008-10-07	Borgia et al.	
/H.S./	6	7096502	B1	2006-08-22	Fox et al.	
/H.S./	7	8191139	B2	2012-05-29	Heimerdinger et al.	
/H.S./	8	8255995	B2	2012-08-28	Kraemer et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		
First Named Inventor	Anurag Agarwal	
Art Unit		
Examiner Name		
Attorney Docket Number	ThreatM008	

/H.S/	9	8413237	B2	2013-04-02	O'Rourke et al.	
/H.S/	10	9497203	B2	2016-11-15	Honig et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS

Remove

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/H.S/	1	20060241991	A1	2006-10-26	Pudhukottai et al.	
/H.S/	2	20110178942	A1	2011-07-21	Watters et al.	
/H.S/	3	20140137257	A1	2014-05-15	Martinez et al.	
/H.S/	4	20110126111	A1	2011-05-26	Gill et al.	
/H.S/	5	20180324207	A1	2018-11-08	Reybok, Jr. et al.	
/H.S/	6	20060015941	A1	2006-01-19	McKenna	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS

Remove

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		
First Named Inventor	Anurag Agarwal	
Art Unit		
Examiner Name		
Attorney Docket Number	ThreatM008	

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
/H.S./	1	Threat Risk Modeling, published online at least as early as Feb. 3, 2018 by OWASP, available at https://www.owasp.org/index.php/Threat_Risk_Modeling .	
/H.S./	2	Threat Model, Wikipedia, published online at least as early as Feb. 3, 2018, available at https://en.wikipedia.org/wiki/Threat_model (note that some of the material in this Wikipedia article appears to be posted by one or more inventors of the present application or its parent provisional applications - some of the material appears to be posted by Brian Beyst, for example, who is an inventor on two of the parent provisional applications).	
/H.S./	3	Comparisons of Threat Model Modeling Methodologies, published online by ThreatModeler at least as early as Apr. 15, 2016, available at http://threatmodeler.com/comparison-threat-modeling-methodologies/ (note that this article appears to be affiliated with a business organization of, and may have been published under the direction of, one or more inventors of the present application or its parent provisional applications).	
/H.S./	4	Microsoft Threat Modeling Tool, published online by Microsoft, different sections published at different times from Aug. 22, 2017 to Jan. 24, 2018, available online at https://docs.microsoft.com/en-us/azure/opbuildpdf/security/TOC.pdf?branch=live	
/H.S./	5	A description of an on-sale version of systems and methods, on sale in the U.S. by applicants at least as early as 12/31/2011, which on-sale version disclosed some of the elements disclosed in the present application. The description includes a detailed discussion of which claim elements of the claims as originally filed in the present application were disclosed in the 2011 version and which were not, and includes screenshots of user interfaces used in the system/methods.	
/H.S./	6	Lockheed Martin Corporation, "Seven Ways to Apply the Cyber Kill Chain with a Threat Intelligence Platform," published at least as early as 2015.	

If you wish to add additional non-patent literature document citation information please click the Add button

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Anurag Agarwal
Art Unit	
Examiner Name	
Attorney Docket Number	ThreatM008

EXAMINER SIGNATURE

Examiner Signature	/HOSUK SONG/	Date Considered	07/31/2019
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	
Filing Date	
First Named Inventor	Anurag Agarwal
Art Unit	
Examiner Name	
Attorney Docket Number	ThreatM008

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Paul B. Johnson/	Date (YYYY-MM-DD)	2018-12-06
Name/Print	Paul B. Johnson	Registration Number	59375

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Access provided by:
United States Patent and
Trademark Office
Sign Out

Browse

My Settings

Get Help

Search within results 🔍

Download PDFs

Per Page: 17 Per Page 25

Export

Alert Set Search Alerts

Search History

Displaying results 1-25 of 3,347 for network threat model x

Conferences (2,756)

Journals (433)

Magazines (70)

Early Access Articles (52)

Courses (29)

Books (6)

Standards (1)

Filter:

Alert Set Search Alerts

sort: 17 Sort Relevance

Show

All Results

My Subscribed
Content

Open Access

Year

Single Year Range

1978 2019

From

To

1978

2019

Author

Affiliation

Publication Title

Publisher

Supplemental Items

Conference Location

Standard Status

Standard Type

Index Terms

Mathematical modelling of the spreading of software threats in computer network

Sergey Semenov ; Vyacheslav Davydov ; Sergey Engalichev

Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science

Year: 2012 | Conference Paper | Publisher: IEEE

Abstract

(101 Kb)

Mathematical modelling of the spreading of software threats in computer network

Sergey Semenov | Vyacheslav Davydov | Sergey Engalichev

Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science

Year: 2012 | Conference Paper | Publisher: IEEE

A threat risk estimation model for computer network security

Razieh Rezaee ; Abbas Ghaemi Bafghi ; Masoud Khosravi-Farmad

2016 6th International Conference on Computer and Knowledge Engineering (ICCCKE)

Year: 2016 | Conference Paper | Publisher: IEEE

Cited by: Papers (1)

Abstract

(2469 Kb)

A threat risk estimation model for computer network security

Razieh Rezaee | Abbas Ghaemi Bafghi | Masoud Khosravi-Farmad

2016 6th International Conference on Computer and Knowledge Engineering (ICCCKE)

Year: 2016 | Conference Paper | Publisher: IEEE

The Research on Fuzzy Bayesian Network Model for the Network Public Opinion Situation and Threat Assessment

Jiaoli Fang ; Jianming Huang ; Ming Liu

2012 Third International Conference on Networking and Distributed Computing

Year: 2012 | Conference Paper | Publisher: IEEE

Abstract

(162 Kb)

The Research on Fuzzy Bayesian Network Model for the Network Public Opinion Situation and Threat Assessment

Jiaoli Fang | Jianming Huang | Ming Liu

2012 Third International Conference on Networking and Distributed Computing

Year: 2012 | Conference Paper | Publisher: IEEE

Standard's Dictionary
Terms

- 0SE
- 0SF
- 0SI
- 1/0
- 1/0 task-structuring criteria
- 1GL
- 2GL
- 3G
- 4GL
- 5GL
- <Viewpoint>

Browse »

-  **Evaluating network cyber resiliency methods using cyber threat, Vulnerability and Defense Modeling and Simulation**
 Suzanne Hassell ; Paul Beraud ; Alen Cruz ; Gangadhar Ganga ; Steve Martin ; Justin Toennies ; Pablo Vazquez ; Gary Wright ; Daniel Gomez ; Frank Pietryka ; Niraj Srivastava ; Travis Hester ; David Hyde ; Brian Mastropietro
 MILCOM 2012 - 2012 IEEE Military Communications Conference
 Year: 2012 | Conference Paper | Publisher: IEEE
 Cited by: Papers (3)

Abstract (1320 Kb)

Evaluating network cyber resiliency methods using cyber threat, Vulnerability and Defense Modeling and Simulation

Suzanne Hassell | Paul Beraud | Alen Cruz | Gangadhar Ganga | Steve Martin | Justin Toennies | Pablo Vazquez | Gary Wright | Daniel Gomez | Frank Pietryka | Niraj Srivastava | Travis Hester | David Hyde | Brian Mastropietro
 MILCOM 2012 - 2012 IEEE Military Communications Conference
 Year: 2012 | Conference Paper | Publisher: IEEE

-  **The Hierarchical Threat Model of Routing Security for Wireless Ad Hoc Networks**

Guo Xian ; Feng Tao ; Yuan Zhan-Ting ; Ma Jian-Feng
 2010 First International Conference on Networking and Distributed Computing
 Year: 2010 | Conference Paper | Publisher: IEEE

Abstract (333 Kb)

The Hierarchical Threat Model of Routing Security for Wireless Ad Hoc Networks

Guo Xian | Feng Tao | Yuan Zhan-Ting | Ma Jian-Feng
 2010 First International Conference on Networking and Distributed Computing
 Year: 2010 | Conference Paper | Publisher: IEEE

-  **Overview of Research on Assessment Model of Radiant Threat Rank Based on Dynamic Bayesian Network**

Zheng Tang ; Xiao-guang Gao ; Ying Zhang
 2007 IEEE International Conference on Automation and Logistics
 Year: 2007 | Conference Paper | Publisher: IEEE
 Cited by: Papers (3)

Abstract (156 Kb)

Overview of Research on Assessment Model of Radiant Threat Rank Based on Dynamic Bayesian Network

Zheng Tang | Xiao-guang Gao | Ying Zhang
 2007 IEEE International Conference on Automation and Logistics
 Year: 2007 | Conference Paper | Publisher: IEEE

-  **Network Threat Behavior Detection and Trend Analysis Based on the Collaborative Model**

Dong Ma ; Yongjun Wang
 2012 Fourth International Conference on Multimedia Information Networking and Security
 Year: 2012 | Conference Paper | Publisher: IEEE

Abstract (874 Kb)

Network Threat Behavior Detection and Trend Analysis Based on the Collaborative Model

Dong Ma | Yongjun Wang
 2012 Fourth International Conference on Multimedia Information Networking and Security
 Year: 2012 | Conference Paper | Publisher: IEEE

-  **Network Survivability Analysis Based on Stochastic Game Model**
 Wang Chunlei ; Miao Qing ; Dai Yiqi
 2012 Fourth International Conference on Multimedia Information Networking
 and Security
 Year: 2012 | Conference Paper | Publisher: IEEE
 Cited by: Papers (2)
 Abstract (742 Kb)

Network Survivability Analysis Based on Stochastic Game Model

Wang Chunlei | Miao Qing | Dai Yiqi
 2012 Fourth International Conference on Multimedia Information Networking
 and Security
 Year: 2012 | Conference Paper | Publisher: IEEE

-
-  **Network security situation awareness based on intercepting the threat spread**
 Bo Zhou ; Lin-fei Zhong
 Proceedings of 2013 3rd International Conference on Computer Science and
 Network Technology
 Year: 2013 | Conference Paper | Publisher: IEEE
 Abstract (189 Kb)

Network security situation awareness based on intercepting the threat spread

Bo Zhou | Lin-fei Zhong
 Proceedings of 2013 3rd International Conference on Computer Science and
 Network Technology
 Year: 2013 | Conference Paper | Publisher: IEEE

-
-  **POLIoT : Internet Of Things Framework In Managing Network Threats At Metro Polytechnic Tasek Gelugor**
 Zulkarnain Md. Ali ; Mohamad Azuan Bin Mohamed Arshad ; Marini Abu Bakar
 2018 Cyber Resilience Conference (CRC)
 Year: 2018 | Conference Paper | Publisher: IEEE
 Abstract (225 Kb)

POLIoT : Internet Of Things Framework In Managing Network Threats At Metro Polytechnic Tasek Gelugor

Zulkarnain Md. Ali | Mohamad Azuan Bin Mohamed Arshad | Marini Abu Bakar
 2018 Cyber Resilience Conference (CRC)
 Year: 2018 | Conference Paper | Publisher: IEEE

-
-  **Mathematical Modeling and Analysis of Destabilization Threats in Computer Networks**
 Nataliia Ivanushchak ; Nataliia Kunanets ; Volodymyr Pasichnyk
 2018 International Scientific-Practical Conference Problems of
 Infocommunications. Science and Technology (PIC S&T)
 Year: 2018 | Conference Paper | Publisher: IEEE
 Abstract (250 Kb)

Mathematical Modeling and Analysis of Destabilization Threats in Computer Networks

Nataliia Ivanushchak | Nataliia Kunanets | Volodymyr Pasichnyk
 2018 International Scientific-Practical Conference Problems of
 Infocommunications. Science and Technology (PIC S&T)
 Year: 2018 | Conference Paper | Publisher: IEEE

-
-  **Conceptual Model for Security in Next Generation Network**
 Masoud Hayeri Khyavi ; Mina Rahimi
 2016 30th International Conference on Advanced Information Networking
 and Applications Workshops (WAINA)

Year: 2016 | Conference Paper | Publisher: IEEE

Cited by: Papers (2)

Abstract

(519 Kb)

Conceptual Model for Security in Next Generation Network

Masoud Hayeri Khyavi | Mina Rahimi

2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)

Year: 2016 | Conference Paper | Publisher: IEEE

■ A Model of Threat Assessment based on Discrete Hopfield Neural Network

Changqing Kang ; Lihong Guo

2006 6th World Congress on Intelligent Control and Automation

Year: 2006 | Volume: 1 | Conference Paper | Publisher: IEEE

Abstract

(195 Kb)

A Model of Threat Assessment based on Discrete Hopfield Neural Network

Changqing Kang | Lihong Guo

2006 6th World Congress on Intelligent Control and Automation

Year: 2006 | Volume: 1 | Conference Paper | Publisher: IEEE

■ Threat Situation Analysis of Local Area Network Based on the Network Graph Theory Model

Na Li ; Jingbo Xia ; Kuisheng Feng ; Rong Liu

2009 First International Conference on Information Science and Engineering

Year: 2009 | Conference Paper | Publisher: IEEE

Abstract

(385 Kb)

Threat Situation Analysis of Local Area Network Based on the Network Graph Theory Model

Na Li | Jingbo Xia | Kuisheng Feng | Rong Liu

2009 First International Conference on Information Science and Engineering

Year: 2009 | Conference Paper | Publisher: IEEE

■ Guiding Threat Analysis with Threat Source Models

K. Clark ; C. Lee ; S. Tyree ; J. Hale

2007 IEEE SMC Information Assurance and Security Workshop

Year: 2007 | Conference Paper | Publisher: IEEE

Cited by: Papers (5)

Abstract

(8533 Kb)

Guiding Threat Analysis with Threat Source Models

K. Clark | C. Lee | S. Tyree | J. Hale

2007 IEEE SMC Information Assurance and Security Workshop

Year: 2007 | Conference Paper | Publisher: IEEE

■ Optimal response to computer network threats

Farzaneh Abazari ; Afsaneh Madani ; Hossein Gharaee

2016 8th International Symposium on Telecommunications (IST)

Year: 2016 | Conference Paper | Publisher: IEEE

Cited by: Papers (1)

Abstract

(1055 Kb)

Optimal response to computer network threats

Farzaneh Abazari | Afsaneh Madani | Hossein Gharaee

2016 8th International Symposium on Telecommunications (IST)

Year: 2016 | Conference Paper | Publisher: IEEE

■ Privacy threat modeling framework for online social networks

Yong Wang ; Raj Kumar Nepali

2015 International Conference on Collaboration Technologies and Systems (CTS)

Year: 2015 | Conference Paper | Publisher: IEEE

Cited by: Papers (5)

Abstract

(339 Kb)

Privacy threat modeling framework for online social networks

Yong Wang | Raj Kumar Nepali

2015 International Conference on Collaboration Technologies and Systems (CTS)

Year: 2015 | Conference Paper | Publisher: IEEE

❏ **Threat Model Framework and Methodology for Personal Networks (PNs)**

Neeli Rashmi Prasad

2007 2nd International Conference on Communication Systems Software and Middleware

Year: 2007 | Conference Paper | Publisher: IEEE

Cited by: Papers (5)

Abstract

(5149 Kb)

Threat Model Framework and Methodology for Personal Networks (PNs)

Neeli Rashmi Prasad

2007 2nd International Conference on Communication Systems Software and Middleware

Year: 2007 | Conference Paper | Publisher: IEEE

❏ **Target Threat Assessment Based on Genetic Neural Network**

Hua Chen ; Ke Zhang

2012 International Conference on Industrial Control and Electronics Engineering

Year: 2012 | Conference Paper | Publisher: IEEE

Abstract

(301 Kb)

Target Threat Assessment Based on Genetic Neural Network

Hua Chen | Ke Zhang

2012 International Conference on Industrial Control and Electronics Engineering

Year: 2012 | Conference Paper | Publisher: IEEE

❏ **High Threat Alarms Mining for Effective Security Management: Modeling, Experiment and Application**

Yongwei Meng ; Tao Qin ; Yukun Liu ; Chao He

2018 IEEE Symposium on Computers and Communications (ISCC)

Year: 2018 | Conference Paper | Publisher: IEEE

Abstract

(168 Kb)

High Threat Alarms Mining for Effective Security Management: Modeling, Experiment and Application

Yongwei Meng | Tao Qin | Yukun Liu | Chao He

2018 IEEE Symposium on Computers and Communications (ISCC)

Year: 2018 | Conference Paper | Publisher: IEEE

❏ **Cyber threat trees for large system threat cataloging and analysis**

P. Ongsakom ; K. Turney ; M. Thornton ; S. Nair ; S. Szygenda ; T. Manikas

2010 IEEE International Systems Conference

Year: 2010 | Conference Paper | Publisher: IEEE

Cited by: Papers (7)

Abstract

(746 Kb)

Cyber threat trees for large system threat cataloging and analysis

P. Ongsakorn | K. Turney | M. Thornton | S. Nair | S. Szygenda | T. Manikas
 2010 IEEE International Systems Conference
 Year: 2010 | Conference Paper | Publisher: IEEE

-  **Intelligent Threat Hunting in Software-Defined Networking**
 Steven Schmitt | Farah I. Kandah | Dylan Brownell
 2019 IEEE International Conference on Consumer Electronics (ICCE)
 Year: 2019 | Conference Paper | Publisher: IEEE
 Abstract (235 Kb)

Intelligent Threat Hunting in Software-Defined Networking

Steven Schmitt | Farah I. Kandah | Dylan Brownell
 2019 IEEE International Conference on Consumer Electronics (ICCE)
 Year: 2019 | Conference Paper | Publisher: IEEE

-  **A model for classifying threats and framework association in wireless sensor networks**
 Adnan Ashraf | Abdul Rauf | Marvie Mussadiq | B.S. Chowdhry | Manzoor Hashmani
 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication
 Year: 2009 | Conference Paper | Publisher: IEEE
 Cited by: Papers (1)
 Abstract (256 Kb)

A model for classifying threats and framework association in wireless sensor networks

Adnan Ashraf | Abdul Rauf | Marvie Mussadiq | B.S. Chowdhry | Manzoor Hashmani
 2009 3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication
 Year: 2009 | Conference Paper | Publisher: IEEE

-  **Threat Analysis of the Security Credential Management System for Vehicular Communications**
 Matthew D. Furtado | Robert D. Mushrall | Hong Liu
 2018 IEEE International Symposium on Technologies for Homeland Security (HST)
 Year: 2018 | Conference Paper | Publisher: IEEE
 Abstract (224 Kb)

Threat Analysis of the Security Credential Management System for Vehicular Communications

Matthew D. Furtado | Robert D. Mushrall | Hong Liu
 2018 IEEE International Symposium on Technologies for Homeland Security (HST)
 Year: 2018 | Conference Paper | Publisher: IEEE

-  **Aviation Transportation, Cyber Threats, and Network-of-Networks: Modeling Perspectives for Translating Theory to Practice**
 Udit Bhatia | Samrat Chatterjee | Auroop Ratan Ganguly | Jianxi Gao | Mahantesh Halappanavar | Matthew Oster | Kevin Clark | Robert Briganfio | Ramakrishna Tipireddy
 2018 IEEE International Symposium on Technologies for Homeland Security (HST)
 Year: 2018 | Conference Paper | Publisher: IEEE
 Abstract (1874 Kb)

Aviation Transportation, Cyber Threats, and Network-of-Networks: Modeling Perspectives for Translating Theory to Practice

Udit Bhatia | Samrat Chatterjee | Auroop Ratan Ganguly | Jianxi Gao |
Mahantesh Halappanavar | Matthew Oster | Kevin Clark | Robert Briganfio |
Ramakrishna Tipireddy
2018 IEEE International Symposium on Technologies for Homeland Security
(HST)
Year: 2018 | Conference Paper | Publisher: IEEE

Load More

IEEE Account	▼
Profile Information	▼
Purchase Details	▼
Need Help?	▼
Other	▼

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2018 IEEE. All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

US & Canada: +1 800 678 4333
Worldwide: +1 732 981 0060

IEEE Account	Purchase Details	Profile Information	Need Help?
» Change Username/Password	» Payment Options	» Communications Preferences	» US & Canada: +1 800 678 4333
» Update Address	» Order History	» Profession and Education	» Worldwide: +1 732 981 0060
	» View Purchased Documents	» Technical Interests	» Contact & Support

About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.
© Copyright 2018 IEEE. All rights reserved. Use of this web site signifies your agreement to the terms and conditions.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 3702

SERIAL NUMBER	FILING or 371(c) DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
16/228,738	12/20/2018	726	2435	ThreatM008		
RULE						
APPLICANTS ThreatModeler Software Inc., Jersey City, NJ; INVENTORS Anurag Agarwal, Jersey City, NJ; ** CONTINUING DATA ***** This application is a CIP of 15/922,856 03/15/2018 PAT 10200399 which is a CIP of 15/888,021 02/03/2018 PAT 10255439 which claims benefit of 62/507,691 05/17/2017 and claims benefit of 62/527,671 06/30/2017 and claims benefit of 62/530,295 07/10/2017 and claims benefit of 62/520,954 06/16/2017 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY ** 02/04/2019						
Foreign Priority claimed ☐ Yes ☒ No 35 USC 119(a-d) conditions met ☐ Yes ☒ No Verified and Acknowledged <u>/Hosuk Song/</u> Examiner's Signature		☐ Met after Allowance Initials	STATE OR COUNTRY NJ	SHEETS DRAWINGS 22	TOTAL CLAIMS 20	INDEPENDENT CLAIMS 3
ADDRESS Law Office of Paul B. Johnson 8483 S. 1275 E. Sandy, UT 84094-1363 UNITED STATES						
TITLE Threat Model Chaining and Attack Simulation Systems and Related Methods						
FILING FEE RECEIVED 785	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit		

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

Aug 08, 2019 03:30:43 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	CTNF	08/08/2019	ThreatM008
	892	08/08/2019	ThreatM008
	1449	08/08/2019	ThreatM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://sportal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363



**Courtesy Reminder for
Application Serial No: 16/228,738**

Attorney Docket No: ThreatM008

Customer Number: 145042

Date of Electronic Notification: 08/08/2019

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

paul@pauljohnsonlaw.com

To view your correspondence online or update your email addresses, please visit us anytime at **<https://ppair-my.uspto.gov/pair/PrivatePair>**.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

Electronic Acknowledgement Receipt

EFS ID:	37570740
Application Number:	16228738
International Application Number:	
Confirmation Number:	3702
Title of Invention:	Threat Model Chaining and Attack Simulation Systems and Related Methods
First Named Inventor/Applicant Name:	Anurag Agarwal
Customer Number:	145042
Filer:	Paul B. Johnson
Filer Authorized By:	
Attorney Docket Number:	ThreatM008
Receipt Date:	25-OCT-2019
Filing Date:	20-DEC-2018
Time Stamp:	20:40:22
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	OAR1.pdf	196562	no	28
			801a816e6ae08385776e9ecf3206abf9630753a9		

Warnings:

IriusRisk

Information:	
Total Files Size (in bytes):	196562
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

AMENDMENT/REPLY

Applicant: ThreatModeler Software Inc.

Docket No: THREATM008

Examiner: Song, Hosuk

Ser. No: 16228738

Filed: December 20, 2018

Group Art Unit: 2435

Title: Threat Model Chaining and Attack Simulation Systems and Related Methods

**RESPONSE TO OFFICE ACTION
DATED AUGUST 8, 2019**

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner:

This is filed in response to the Office Action mailed August 8, 2019. This response is being filed within the shortened statutory period and therefore no extension of time fees are applicable. Reconsideration of the application is requested in view of the following:

The current Claims begin(s) on page 2.

Remarks/Arguments begin on page 8.

CLEAN VERSION OF CURRENT CLAIM STATUS

No amendments are made to the claims, but the current status of each is given below.

1. (Original) 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.
2. (Original) 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.

3. (Original) 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.

4. (Original) 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.

5. (Original) 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 one or more attack paths which pass through multiple diagrammed threat model components of the first threat model.

6. (Original) 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.

7. (Original) 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.

8. (Original) 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.

9. (Original) 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.

10. (Original) 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.

11. (Original) The attack simulation method of claim 3, further comprising configuring the diagram interface to receive one or more user inputs to add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.

12. (Original) An attack simulation system, comprising:
one or more computing devices communicatively coupled with one or more databases, the one or more computing devices displaying, on one or more displays of the one or more computing devices:

one or more input interfaces configured to, in response to receiving one or more user inputs, store a plurality of user-defined threat model components in the one or more databases, store a plurality of threats in the one or more databases, associate each of the threats with at least one of the threat model components through the one or more databases, store a plurality of compensating controls in the one or more databases, and associate each compensating control with at least one of the threats through the one or more databases, and;

a diagram interface configured to, in response to receiving one or more user inputs, diagram one of a system, an application, and a process, the diagram including one or more of the threat model components and one or more of the compensating

controls, to define a first threat model, the first threat model including all threats associated through the one or more databases with the diagrammed threat model components;

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

13. (Original) The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving a user input to toggle one of the diagrammed compensating controls (hereinafter “first control”) to an on state, toggle all attack paths mitigatable by the first control to a mitigated display state.

14. (Original) The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to receiving a user input to toggle the first control to an off state, toggle all attack paths mitigatable by the first control to an unmitigated display state.

15. (Original) The attack simulation system of claim 13, wherein the diagram interface is configured to, in response to receiving one or more user inputs removing the first control from the first threat model, toggle all attack paths mitigatable by the first control to an unmitigated display state.

16. (Original) The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, visually display only attack paths of all threats associated with a subset of the diagrammed threat model components.

17. (Original) The attack simulation system of claim 12, wherein the diagram interface is configured to, in response to receiving one or more user inputs, alter a profile of an attacking component, wherein the alteration alters the visually displayed attack paths.
18. (Original) The attack simulation system of claim 12, wherein the one of a system, an application, and a process comprises a computing network.
19. (Original) 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.
20. (Original) 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.

Remarks/Arguments

Claims 1-20 are pending. Reconsideration is requested in light of the following.

Nonstatutory Double Patenting Rejections

Claims 1-20 were rejected based on nonstatutory double patenting with regards to U.S. Patent No. 10200399 and U.S. Patent No. 10255439. The cited U.S. Patents are commonly owned with the examined application, and terminal disclaimers are being filed herewith to overcome these rejections. Accordingly, it is respectfully requested that the nonstatutory double patenting rejections be withdrawn.

Rejections under 35 U.S.C. 101

Summary of 101 Rejections

Claims 1-20 were rejected under 35 U.S.C. 101 as drawn to non-statutory subject matter for attempting to claim an abstract idea.

Legal Standard for 35 U.S.C. 101

35 U.S.C. 101 sets for a subject matter eligibility requirement: "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title." In expounding on section 101, MPEP 2104 indicates as follows:

(a) first, a claimed invention must fall within one of the four statutory categories of invention, i.e., process, machine, manufacture, or composition of matter; and (b) second, a claimed invention must be directed to patent-eligible subject matter and not a judicial exception (unless the claim as a whole includes additional limitations amounting to significantly more than the exception).

MPEP 2106.I. there are two criteria given for making the subject matter eligibility determination: (1) the “claimed invention must be to one of the four statutory categories” and (2) the “claimed invention also must qualify as patent-eligible subject matter, i.e., the claim must not be directed to a judicial exception unless the claim as a whole includes additional limitations amounting to significantly more than the exception.” The Examiner bears the initial burden of establishing a prima facie case of unpatentability under 101. MPEP 2106.07.

The First Step

The first step is to determine whether the invention is directed to one of the four statutory categories. The first listed category, a “process,” is synonymous with a “method” and is simply an invention that is claimed as an act, or a step, or a series of acts or steps. MPEP 2106.03.I., citing *Gottschalk v. Benson*, 409 U.S. 63, 70, 175 USPQ 673, 676 (1972). The second category is a “machine.” Something qualifies as a “machine” if it is “a concrete thing, consisting of parts, or of certain devices and combination of devices.” MPEP 2106.03.I., *Digitech Image Techs. V. Electronics for Imaging*, 758 F.3d 1344, 1348-49, 111 USPQ2d 1717, 1719 (Fed. Cir. 2017) (quoting *Burr v. Duryee*, 68 U.S. 531, 570, 17 L. Ed. 650, 657 (1863)). This “includes every mechanical device or combination of mechanical powers and devices to perform some function and produce a certain effect or result.” MPEP 2106.03.I., citing *In re Nuijten*, 500 F.3d 1346, 1355, 84 USPQ2d 1495, 1501 (Fed. Cir. 2007) (quoting *Corning v. Burden*, 56 U.S. 252, 267, 14 L. Ed. 683, 690 (1854)).

The Second Step

The second step is to determine whether the claim is wholly directed to subject matter encompassing a judicially recognized exception, and this step has been further delineated into two sub-steps.

Step 2A

First, one of the judicially recognized exceptions is a claim directed to nothing more than an “abstract idea.” *Diamond v. Diehr*, 450 U.S. 175, 185, 209 USPQ 1, 7 (1981); *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2354, 110 USPQ2d 1976, 1980 (2014) (citing *Association for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107, 2116, 106 USPQ2d 1972, 1979 (2013)); *Diamond v. Chakrabarty*, 447 U.S. 303, 309, 206 USPQ 193, 197 (1980); *Parker v. Flook*, 437 U.S. 584, 589, 198 USPQ 193, 197 (1978); *Gottschalk v. Benson*, 409 U.S. 63, 67-68, 175 USPQ 673, 675 (1972). See also *Bilski v. Kappos*, 561 U.S. 593, 601, 95 USPQ2d 1001, 1005-06 (2010). The first sub-step of Step 2, which has been called Step 2A by MPEP 2106.04.II (and which was superseded in part by the 2019 Revised Patent Subject Matter Eligibility Guidance (Federal Register Vol. 84, No. 4, p. 50-57, issued Jan. 7, 2019) (hereinafter “2019 Revised Guidance”), is to determine whether the claim is directed to an abstract idea. If the claim is not directed to an abstract idea, the claim is subject matter eligible and no further inquiry is required (in other words, the Examiner does not proceed to Step 2B). MPEP 2016.04.II; 2019 Revised Guidance, 57.

The 2019 Revised Guidance clarified that while, in the past, examiners have determined subject matter eligibility by describing subject matter claimed in the patent application and noting whether or not similar subject matter has been identified as an abstract idea in prior cases, this approach is no longer practical. “While that approach was effective soon after *Alice* was decided, it has since become impractical. The Federal Circuit has now issued numerous decisions identifying subject matter as abstract or non-abstract in the context of specific cases, and that number is continuously growing. In addition, similar subject matter has been described both as abstract and not abstract in different cases.” 2019 Revised Guidance, 51-52. The 2019 Revised Guidance points out, for instance, that:

claims in one application could be deemed to be abstract, whereas slightly different claims related to the same or similar subject matter could be determined to reflect a patent eligible “improvement.” Alternatively, claims in one application could be found to be abstract, whereas claims to the same or similar subject matter in another application, containing additional or different

embodiments in the specification, could be deemed eligible as not directed to an abstract idea. In other words, the finding that the subject matter claimed in a prior patent was “abstract” as claimed may not determine whether similar subject matter in another application, claimed somewhat differently or supported by a different disclosure, is directed to an abstract idea and therefore patent ineligible. *2019 Revised Guidance*, 52, citing *TLI Communications LLC v. A.V. Automotive, LLC*, 823 F.3d 607, 611 (Fed. Cir. 2016); *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1335 (Fed. Cir. 2016); *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1258 (Fed. Cir. 2017); *Credit Acceptance Corp. v. Westlake Servs.*, 859 F.3d 1044, 1056 (Fed. Cir. 2017); *Finjan, Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299, 1304 (Fed. Cir. 2018) (quoting *Enfish*, 822 F.3d at 1335).

Accordingly, the *2019 Revised Guidance* extracted and synthesized key concepts identified by the courts as abstract ideas to indicate that the abstract idea doctrine includes the following subject matter groupings when recited as claim limitations. The *2019 Revised Guidance* specifically indicates on p. 52 that “the abstract idea exception includes the following groupings of subject matter, when recited as such in a claim limitation(s) (that is, when recited on their own or per se).”

- (a) **Mathematical concepts—mathematical relationships, mathematical formulas or equations, mathematical calculations.** *Bilski v. Kappos*, 561 U.S. 593, 611 (2010) (“The concept of hedging . . . reduced to a mathematical formula . . . is an . . . abstract idea[.]”); *Diamond v. Diehr*, 450 U.S. 175, 191 (1981) (“A mathematical formula as such is not accorded the protection of our patent laws”) (citing *Benson*, 409 U.S. 63); *Parker v. Flook*, 437 U.S. 584, 594 (1978) (“[T]he discovery of [a mathematical formula] cannot support a patent”); *Benson*, 409 U.S. at 71–72 (concluding that permitting a patent on the claimed invention “would wholly preempt the mathematical formula and in practical effect would be a patent on the algorithm itself”); *Mackay Radio & Telegraph Co. v. Radio Corp. of Am.*, 306 U.S. 86, 94 (1939) (“[A] scientific truth, or the mathematical expression of it, is not patentable”); *SAP America, Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1163 (Fed. Cir. 2018) (claims to a “series of mathematical calculations based on selected information” are directed to abstract ideas); *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1350 (Fed. Cir. 2014) (claims to a “process of organizing information through mathematical correlations” are directed to an abstract idea); *Bancorp Servs., LLC v. Sun Life Assurance Co. of Can. (U.S.)*, 687 F.3d 1266, 1280 (Fed. Cir. 2012) (identifying the concept of “managing a stable value

protected life insurance policy by performing calculations and manipulating the results” as an abstract idea).

- (b) **Certain methods of organizing human activity—fundamental economic principles or practices (including hedging, insurance, mitigating risk); commercial or legal interactions (including agreements in the form of contracts; legal obligations; advertising, marketing or sales activities or behaviors; business relations); managing personal behavior or relationships or interactions between people (including social activities, teaching, and following rules or instructions).** *Alice*, 573 U.S. at 219–20 (concluding that use of a third party to mediate settlement risk is a “fundamental economic practice” and thus an abstract idea); *id.* (describing the concept of risk hedging identified as an abstract idea in *Bilski* as “a method of organizing human activity”); *Bilski*, 561 U.S. at 611–612 (concluding that hedging is a “fundamental economic practice” and therefore an abstract idea); *Bancorp*, 687 F.3d at 1280 (concluding that “managing a stable value protected life insurance policy by performing calculations and manipulating the results” is an abstract idea); *Inventor Holdings, LLC v. Bed Bath & Beyond, Inc.*, 876 F.3d 1372, 1378–79 (Fed. Cir. 2017) (holding that concept of “local processing of payments for remotely purchased goods” is a “fundamental economic practice, which Alice made clear is, without more, outside the patent system.”); *OIP Techs., Inc. v. Amazon.com, Inc.*, 788 F.3d 1359, 1362–63 (Fed. Cir. 2015) (concluding that claimed concept of “offer-based price optimization” is an abstract idea “similar to other ‘fundamental economic concepts’ found to be abstract ideas by the Supreme Court and this court”); *buySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014) (holding that concept of “creating a contractual relationship—a ‘transaction performance guaranty’ ” is an abstract idea); *In re Comiskey*, 554 F.3d 967, 981 (Fed. Cir. 2009) (claims directed to “resolving a legal dispute between two parties by the decision of a human arbitrator” are ineligible); *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 715 (Fed. Cir. 2014) (holding that claim “describe[ing] only the abstract idea of showing an advertisement before delivering free content” is patent ineligible); *In re Ferguson*, 558 F.3d 1359, 1364 (Fed. Cir. 2009) (holding methods “directed to organizing business or legal relationships in the structuring of a sales force (or marketing company)” to be ineligible); *Credit Acceptance*, 859 F.3d 1044 at 1054 (“The Board determined that the claims are directed to the abstract idea of ‘processing an application for financing a purchase.’ . . . We agree.”); *Interval Licensing*, 896 F.3d at 1344–45 (concluding that “[s]tanding alone, the act of providing someone an additional set of information without disrupting the ongoing provision of an initial set of information is an abstract idea,” observing that the district court “pointed to the nontechnical human activity of passing a note to a person who is in the middle of a meeting or conversation as further illustrating the basic, longstanding practice that is the focus of the [patent ineligible] claimed invention.”); *Voter Verified, Inc. v. Election Systems & Software, LLC*, 887 F.3d 1376,

1385 (Fed. Cir. 2018) (finding the concept of “voting, verifying the vote, and submitting the vote for tabulation,” a “fundamental activity” that humans have performed for hundreds of years, to be an abstract idea); *In re Smith*, 815 F.3d 816, 818 (Fed. Cir. 2016) (concluding that “[a]pplicants’ claims, directed to rules for conducting a wagering game” are abstract).

- (c) **Mental processes—concepts performed in the human mind (including an observation, evaluation, judgment, opinion).** If a claim, under its broadest reasonable interpretation, covers performance in the mind but for the recitation of generic computer components, then it is still in the mental processes category unless the claim cannot practically be performed in the mind. *See Intellectual Ventures I LLC v. Symantec Corp.*, 838 F.3d 1307, 1318 (Fed. Cir. 2016) (“[W]ith the exception of generic computer implemented steps, there is nothing in the claims themselves that foreclose them from being performed by a human, mentally or with pen and paper.”); *Mortg. Grader, Inc. v. First Choice Loan Servs. Inc.*, 811 F.3d 1314, 1324 (Fed. Cir. 2016) (holding that computer-implemented method for “anonymous loan shopping” was an abstract idea because it could be “performed by humans without a computer”); *Versata Dev. Grp. v. SAP Am., Inc.*, 793 F.3d 1306, 1335 (Fed. Cir. 2015) (“Courts have examined claims that required the use of a computer and still found that the underlying, patent-ineligible invention could be performed via pen and paper or in a person’s mind.”); *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366, 1375, 1372 (Fed. Cir. 2011) (holding that the incidental use of “computer” or “computer readable medium” does not make a claim otherwise directed to process that “can be performed in the human mind, or by a human using a pen and paper” patent eligible); *id.* at 1376 (distinguishing *Research Corp. Techs. v. Microsoft Corp.*, 627 F.3d 859 (Fed. Cir. 2010), and *SIRF Tech., Inc. v. Int’l Trade Comm’n*, 601 F.3d 1319 (Fed. Cir. 2010), as directed to inventions that “could not, as a practical matter, be performed entirely in a human’s mind”). Likewise, performance of a claim limitation using generic computer components does not necessarily preclude the claim limitation from being in the mathematical concepts grouping, *Benson*, 409 U.S. at 67, or the certain methods of organizing human activity grouping, *Alice*, 573 U.S. at 219–20. 15 *Mayo*, 566 U.S. at 71 (“[M]ental processes[] and abstract intellectual concepts are not patentable, as they are the basic tools of scientific and technological work” (quoting *Benson*, 409 U.S. at 67)); *Flook*, 437 U.S. at 589 (same); *Benson*, 409 U.S. at 67, 65 (noting that the claimed “conversion of [binary-coded decimal] numerals to pure binary numerals can be done mentally,” i.e., “as a person would do it by head and hand.”); *Synopsys, Inc. v. Mentor Graphics Corp.*, 839 F.3d 1138, 1139, (Fed. Cir. 2016) (holding that claims to the mental process of “translating a functional description of a logic circuit into a hardware component description of the logic circuit” are directed to an abstract idea, because the claims “read on an individual performing the claimed steps mentally or with pencil and paper”); *Mortg. Grader*,

811 F.3d. at 1324 (concluding that concept of “anonymous loan shopping” is an abstract idea because it could be “performed by humans without a computer”); *In re BRCA1 & BRCA2-Based Hereditary Cancer Test Patent Litig.*, 774 F.3d 755, 763 (Fed. Cir. 2014) (concluding that concept of “comparing BRCA sequences and determining the existence of alterations” is an “abstract mental process”); *In re Brown*, 645 F. App’x. 1014, 1017 (Fed. Cir. 2016) (non-precedential) (claim limitations “encompass the mere idea of applying different known hair styles to balance one’s head. Identifying head shape and applying hair designs accordingly is an abstract idea capable, as the Board notes, of being performed entirely in one’s mind”). *2019 Revised Guidelines*, 52-53.

The *2019 Revised Guidance* indicates that “[c]laims that do not recite matter that falls within these [three] enumerated groupings of abstract ideas should not be treated as reciting abstract ideas.” P. 53. The *2019 Revised Guidance* further that even if a claim falls within one of these three groupings, such a claim “is not directed to a judicial exception (Step 2A: NO) and is eligible (thus concluding the eligibility analysis) if “the claim as a whole integrates the recited tentative abstract idea into a practical application.” P. 53, 57. The *2019 Revised Guidance* goes on to give a non-exhaustive list of examples where the courts have found such practical applications:

- An additional element reflects an improvement in the functioning of a computer, or an improvement to other technology or technical field. *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1258–59.
- An additional element that applies or uses a judicial exception to effect a particular treatment or prophylaxis for a disease or medical condition. *See, e.g., Classen Immunotherapies, Inc. v. Biogen IDEC*, 659 F.3d 1057, 1066–68 (Fed. Cir. 2011). *See also Vanda Pharm. Inc. v. West-Ward Pharm. Int’l Ltd.*, 887 F.3d 1117, 1135 (Fed. Cir. 2018).
- An additional element implements a judicial exception with, or uses a judicial exception in conjunction with, a particular machine or manufacture that is integral to the claim. *Eibel Process Co. v. Minnesota & Ontario Paper Co.*, 261 U.S. 45, 64–65 (1923).
- An additional element effects a transformation or reduction of a particular article to a different state or thing. *Diehr*, 450 U.S. at 184.

- An additional element applies or uses the judicial exception in some other meaningful way beyond generally linking the use of the judicial exception to a particular technological environment, such that the claim as a whole is more than a drafting effort designed to monopolize the exception. *Diehr*, 450 U.S. at 184, 187.

In short, in almost all cases, if a claim does not fall within the three groupings of abstract ideas, the claim is not “directed” to an abstract idea—the analysis then stops at 2A and the claim is subject matter eligible. But even if the claim falls within the three groupings, if the claim as a whole recites a practical application of the abstract idea, then the analysis again stops at 2A and the claim is subject matter eligible.

Step 2B

If the claim is directed to an abstract idea so that, under Step 2A, the claim falls within one of the three enumerated groupings and additionally the claim as a whole does not recite a practical application of the abstract idea, then the Examiner proceeds to Step 2B, which is to determine whether the claim recites additional elements that amount to “significantly more” than the recited judicial exception. MPEP 2106.05. “For example, the claim may recite additional elements that render the claim patent eligible even though a judicial exception is recited in a separate claim element.” *2019 Revised Guidance*, 56, citing *Diehr*, 450 U.S. at 185, 187. The Federal Circuit has found claims eligible at Step 2B because, for example, the additional elements were unconventional in combination. *2019 Revised Guidance*, 56, citing *Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F. 3d 1288, 1300, 1303 (Fed. Cir. 2016); *BASCOM Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349-52 (Fed. Cir. 2016); *DDR Holdings*, 773 F.3d at 1257-59. “[I]f a claim has been determined to be directed to a judicial exception under revised Step 2A, examiners should then evaluate the additional elements individually and in combination under Step 2B to determine whether they provide an inventive concept.” *2019 Revised Guidance*, 56. If the additional elements individually or in combination provide an inventive concept (Step 3B: YES) then the claim is subject matter eligible.

While not all elements of Step 2A need to be reevaluated in Step 2B, this step should nevertheless include a consideration of whether an additional element or combination of elements: “[a]dds a specific limitation or combination of limitations that are not well-understood, routine, conventional activity in the field, which is indicative that an inventive concept may be present; or simply appends well-understood, routine, conventional activities previously known to the industry specified at a high level of generality, to the judicial exception, which is indicative that an inventive concept may not be present.” *2019 Revised Guidance*, 56. Additionally, under step 2B a consideration (or reconsideration) of the following can determine whether a claim is subject matter eligible:

- Whether the claim “purport(s) to improve the functioning of the computer itself” or “any other technology or technical field. MPEP 2106.05(a), citing *Alice Corp. Pty. Ltd. v. CLS Bank Int’l*, 134 S. Ct. 2347, 2359, 110 USPQ2d 1976, 1984 (2014).
- Whether the judicial exception is applied with, or by use of, a particular machine. MPEP 2106.05(b), citing *Bilski v. Kappos*, 561 U.S. 593, 604, 95 USPQ2d 1001, 1007 (2010).
- Whether the claim effects a transformation or reduction of a particular article to a “different state or thing.” MPEP 2106.05(c), citing *Bilski v. Kappos*, 561 U.S. 593, 658, 95 USPQ2d 1001, 1007 (2010) (quoting *Gottschalk v. Benson*, 409 U.S. 63, 70, 175 USPQ 673, 676 (1972)).
- Whether the additional element(s) are well-understood, routine, conventional activities previously known to the industry. MPEP 2106.05(d), citing *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 113 USPQ2d 1097 (Fed. Cir. 2014).

Summary

The *2019 Revised Guidance* is an accurate summary of caselaw surrounding judicial exceptions to subject matter eligibility. The above cited cases indicate that claims should generally only fail Step 2A if they are mathematical concepts, certain methods of organizing human activity, or mental processes and even then only if the claims as a whole do not recite a practical application of the judicial exception. In the rare exception in which a claim is considered abstract notwithstanding its not being in one of these categories, it cannot be

rejected based on subject matter eligibility unless approved by the Technology Center Director, whose approval must be indicated in the file record, along with a justification of why the claim is being treated as reciting an abstract idea notwithstanding its not falling into one of the three enumerated categories. *2019 Revised Guidance*, p. 57.

Arguments

Claims 1-20

The Examiner has not established a prima facie case of subject matter ineligibility of claims 1-20 under 35 U.S.C. 101 by failing to show under Step 2A that the claims, as a whole, in light of the specification, are “directed” to an abstract idea.

In particular, in making the rejection of claims 1-20 the Examiner has taken an approach that the *2019 Revised Guidance* calls “impractical” by simply describing subject matter claimed in the patent application and noting whether or not similar subject matter has been identified as an abstract idea in prior cases. The *2019 Revised Guidance* summarizes, as detailed above, that “the finding that the subject matter claimed in a prior patent was ‘abstract’ as claimed may not determine whether similar subject matter in another application, claimed somewhat differently or supported by a different disclosure, is directed to an abstract idea and therefore patent ineligible.” *2019 Revised Guidance*, 52. In the instant case, the examiner did not focus on how the claims of the instant application are similar or different from the claims of the applications in the cited cases (*Perkin-Elmer, FairWarning v. Iatric, Int. Ventures v. Cap One Financial*), nor how the disclosures of the application and the cited references are similar or different. Rather, the examiner simply focused on the subject matter very broadly.

For example, the examiner states that the claims “only appear to encompass various steps of organizing and manipulating information,” but the examiner made this statement without reciting any language of any of the instant claims. Similarly, in reciting that the

claimed concepts are “not meaningfully different than . . . comparing data to determine a risk level (*Perkin-Elmer*); collecting/analyzing information to detect misuse and notifying a user (*FairWarning v. Iatric*); collecting, displaying, and manipulating data (*Int. Ventures v. Cap. One Financial*),” the Examiner similarly recites no claim language from any of the applications of those cases. Accordingly, the examiner is not making a rejection based on the claim language of the instant application as compared with the claim language of the prior cases, but rather is making a broad rejection based on similar subject matter. But, as the *2019 Revised Guidance* correctly indicates, simply relying on similarities of subject matter is “impractical” and inappropriate because even the courts have found different patent applications, with the same subject matter, to be either subject matter eligible or not subject matter eligible, depending on the specific claim language and the written description. Accordingly, in the first place, the Examiner’s rejection, by focusing broadly on the subject matter of the present application and prior applications alone, instead of specific claim language, cannot properly establish a *prima facie* case of lack of subject matter eligibility.

Additionally, the caselaw that is cited against Applicant’s claims actually speak in favor of the claims not being abstract. The *Intellectual Ventures I v. Capital One* case that the Examiner cites was found to have claims that were drawn to an abstract idea because they recited only the “idea” of a solution (collecting, displaying, and manipulating data) without reciting details of “how” a solution was to be accomplished. MPEP 2106.05(f), citing *Intellectual Ventures I v. Capital One Fin. Corp.*, 850 F.3d 1332, 121 USPQ2d 1940 (Fed. Cir. 2017). For example, the entire “display” clause of the claim at issue in *Intellectual Ventures* stated “display of an instance of a management record type through a user interface.” *Intellectual Ventures*, 850 F.3d 1339. As can be seen, there are no details about the display of the “instance of a management record type,” only that it is somehow displayed. This, accordingly, fails to indicate “how” it is displayed.

In the instant case, however, applicant’s claims include very specific details of “how” to display the elements being displayed on the user interfaces, i.e., a relational diagram is

displayed on a diagram interface, using visual representations of threat model components and visual representations of compensating controls (Independent Claims 1, 4, 12), visual representations of component “groups” are included on the diagram, the component groups each including multiple threat model components (Independent Claim 1, Dependent Claim 20), visual representations of attack paths are displayed on the diagram (Dependent Claim 2, Independent Claim 4, Independent Claim 12), the diagram displays attack paths passing through multiple threat model components (Dependent Claim 5), “mitigatable” attack paths are toggled to a mitigated display state in response to toggling a displayed compensating control to an “on” state (Dependent Claims 6, 13) mitigatable attack paths are toggled to an unmitigated display state in response to toggling a displayed compensating control to an “off” state (Dependent Claims 7, 14), all attack paths mitigatable by a compensating control are toggled to an unmitigated display state in response to removing the compensating control from the diagram (Dependent Claims 8, 15), only the attack paths of a subset of selected diagrammed threat model components are displayed in response to user input (Dependent Claims 9, 16), the displayed attack paths are altered in response to altering a profile of an attacking component (Dependent Claims 10, 17), additional threat model components/threats/compensating controls are stored in the database(s) and associated with one another through user interfaces (Dependent Claim 3), the diagram is in implementations a diagram of a computer network (Dependent Claim 18), and communication protocols are included on the diagram in the form of alphanumeric indicators (Dependent Claim 19). In other words, there is a great level of detail of “how” the information is displayed on the user interface(s) in the claims of the instant application, and this is in stark contrast to the very broad language of the *Intellectual Ventures* claim at issue, which did not include any details in the claims about “how” to display the information.

With regards to the *PerkinElmer* case, in that case the applicant was attempting to patent an algorithm/natural law *per se*, by claiming “comparing the measured level” of a “screening marker” taken from pregnant woman with “observed relative frequency

distributions of marker levels in Down's syndrome pregnancies" and using a "cut-off level" to simply indicate whether the pregnancy was "screen-positive or screen-negative."

PerkinElmer, Inc. v. Intema Ltd., 496 Fed. App'x 65, 68-69, 105 USPQ2d 1960, 1963-94 (Fed. Cir. 2012). Whether a certain level indicated negative for Down's syndrome or not was, of course, a natural law, and the claims only applied this natural law, using an algorithm, by gathering data of one patient and comparing it to past patients. The district court had held that "the claims recite an ineligible algorithm" but had decided they were patent eligible because they "focus on a data-gathering method" and the holding of the Federal Circuit was that the mere gathering of data, and applying it to a mathematical algorithm, was not enough to make the claims subject matter eligible, but that the claims still recited "an ineligible mental step and natural law." *PerkinElmer*, 71, 81. The MPEP interprets the holding as indicating that "mere data gathering," in addition to reciting a natural law or algorithm, is not enough to convert the claim into subject eligible matter. MPEP 2106.05(g).

The *PerkinElmer* case is, generally, not on point, because Applicant's claims do not attempt to claim any specific algorithm or law of nature. If the *PerkinElmer* claims had been allowed then, potentially, the claimant would have been able to prevent all others from diagnosing Down's syndrome pregnancies based on a natural law because all persons doing such diagnoses would, by default, have to gather some data from the pregnant woman to compare with past data using the algorithm. The claims therefore, because they only recited gathering the data in addition to the algorithm/natural law, effectively attempted to patent the algorithm/natural law itself, and this is what was impermissible. In the instant case, the claims recite no natural law or algorithm that Applicant would be tying up or preventing others from using, so *PerkinElmer* is not on point and does not necessitate a finding of subject matter ineligibility of the instant claims.

In the *FairWarning* case the court highlighted the fact that claims can be ineligible if they are the mere "collecting and analyzing information, without more (such as identifying a particular tool for presentation)" because such claims can be done in the mind, i.e., they can

be “mental processes.” *FairWarning v. Iatric Sys.*, 839 F.3d 1089, 1095, 120 USPQ2d 1293 (Fed. Cir. 2016). For example, the entire portion of the claim that could be construed to include a “display” of information in that case said only “providing information if the event has occurred,” and the rest of the steps were all steps that could be done entirely in the mind of a person, including things such as “generating a rule . . . applying the rule . . . storing, in a memory, a hit if the event has occurred . . .” and attempted to claim these steps, all of which could be done in a person’s mind, by simply indicating that the processes occurred in a “computer environment.” *FairWarning*, 839 F. 3d at 92. Courts have indeed found that processes which can be done entirely in the mind are not made patent eligible by simply indicating that they are done on a computer, but it is very instructive that the court in this case highlighted the idea of the claims lacking a “particular tool for presentation,” as indicated above.

The claims in *FairWarning* of course did not include such a particular tool, simply stating “providing information if the event has occurred.” In the claims of the instant application, however, Applicant has gone to great lengths to detail a “particular tool for presentation,” including a specific diagram interface shown on a display that shows visual representations of threat model components, visual representations of compensating controls, visual representations of attack paths (in some cases passing through multiple visual representations of threat model components), specific methods of toggling attack paths on/off in response to turning compensating controls on/off and/or removing compensating controls from the diagram, and so forth. *Claims 1-20*. In other words, Applicant’s claims do recite a “particular tool for presentation” which takes the claim elements quite a ways out of the realm of a simple “mental process.” The *FairWarning* case accordingly does not speak against the instant claims, but instead in favor of finding them subject matter eligible.

It is further pointed out that, in making the rejection of claims 1-20, the Examiner has not indicated how the claims fall into one of the three subject matter groupings generally considered abstract: mathematical concepts, methods of organizing human activity, or

mental processes. The Examiner argues that the claims appear to encompass “various steps of organizing and manipulating information” but that, by itself, is not a category of abstract ideas. As indicated in the *2019 Revised Guidance*, the categories are mathematical concepts, certain methods of organizing human activity, and mental processes.

Applicant’s claims do not recite any mathematical algorithm, nor even any mathematical steps at all in the claimed systems and methods. While it is true that any computer implementing the methods or systems are going to be using logic and, therefore, some underlying math while performing the steps, Applicant’s claims do not recite any of that math or any of those algorithms. As pointed out in the *2019 Revised Guidance*, claims only fall within one of the abstract idea groupings if the abstract idea is “recited as such in a claim limitation(s), that is, when recited on their own or per se.” *2019 Revised Guidance*, 52. As Applicant’s claims do not recite on their own, or per se, any mathematical calculations, operations, or algorithms, they cannot be categorized as falling within the “mathematical concepts” group, and none of the cases regarding mathematical concepts that are cited in the *2019 Revised Guidance* appear to indicate that Applicant’s claims would fall into that category.

Applicant’s claims similarly do not recite any method of organizing human activity, any fundamental principle or practice, any commercial or legal interaction (including agreements in the form of contracts, legal obligations, advertising, marketing or sales activities or behaviors, or business relations), or managing personal behavior or relationships or interactions between people (including social activities, teaching, and following rules or instructions). Indeed, none of the cases regarding methods of organizing human activity that are cited in the *2019 Revised Guidance* appear to indicate that Applicant’s claims would fall into that category.

Applicant’s claims similarly do not fall into the category of mental processes because they do not cover “performance in the mind but for the recitation of generic computer

components.” *2019 Revised Guidance*, 52-53. As the caselaw indicates, and as has been described to some extent above, while some computer-implemented claims are subject matter ineligible as being capable of being performed entirely in the mind, the inclusion in the claims of specific user interface details takes claims out of the realm of “mental processes.” As indicated previously with respect to the *FairWarning* case, when the claims include specific user interface details, this is one way to claim a “particular tool for presentation” which takes the claim out of the realm of a mental process. With respect to the instant claims, the diagram interface that is shown on a computing device’s display—including the visual representations of threat model components, visual representations of compensating controls, visual representations of attack paths, the automatic modification of attack paths between mitigated/unmitigated display states based on removing a threat model component from the diagram or toggling the threat model component between on/off states or modifying an attacking component profile, user interfaces for storing threat model components and threats and compensating controls in the database(s) and associating them with one another, the display of only attack paths of threats associated with a subset of diagrammed threat model components, the diagrammed alphanumeric indicators of communication protocols and of a computing network, and the automated editing of a threat model by adding or removing components from a diagram—takes the claims quite far from the realm of “mental only” processes. *Claims 1-20*. As indicated by the cases discussed above and those cited in the *2019 Revised Guidance*, the claims of the instant application are recited in a way, including “particular tool[s] for presentation,” that take them out of the realm of mental processes.

In the caselaw regarding software-implemented inventions it is also worth pointing out that, for those cases with claimed user interfaces that were found subject matter ineligible, there has been a pattern of those applications including extremely few details in the claims and specification about the user interfaces.

For example, the following was found to be drawn to an ineligible abstract idea: “[r]emotely accessing user-specific information through a mobile interface and pointers to retrieve the information without any description of how the mobile interface and pointers accomplish the result of retrieving previously inaccessible information, *Intellectual Ventures v. Erie Indem. Co.*, 850 F.3d 1315, 1331, 121 USPQ2d 1928, 1939 (Fed. Cir. 2017). The following was also found to be drawn to an ineligible abstract idea: “a system for generating and transmitting [restaurant] menus, [including] a graphical user interface” displaying the menus and linking the menus, where “the specification merely states that the user interface could permit linking of orders with customers, with no disclosure of how this would be technologically implemented.” *Apple v. Ameranth, Inc.*, 842 F.3d 1229, 120 USPQ2d 1844 (Fed. Cir. 2016).

In contrast, the following was found to be drawn to an idea that was subject matter eligible: “a specific, structured graphical user interface that improves the accuracy of trader transactions by displaying bid and asked prices in a particular manner that prevents order entry at a changed price. *Trading Techs. Int’l, Inc. v. CQG, Inc.*, 675 Fed. App’x 1001 (Fed. Cir. 2017). Accordingly, when user interfaces are specifically recited in the claims, as long as the claims and/or specification include sufficient detail of the appearance and functionality of the user interface elements, the claims cannot be considered “mental processes.” In the instant application, paragraphs [0079] and onward, and the drawings, give great detail about the appearance and functionality of the user interfaces, and as already described in detail above, the claims themselves include much detail about specific elements of the user interfaces to take the claims well out of the category of “mental processes.”

It is also worth pointing out that the addition of computer-related elements to claims 1-20 is not merely an incidental addition of a computer to a process otherwise able to be performed mentally—rather the use of the computer related elements is required in order to accomplish the systems and methods of claims 1-20 because the systems and methods are simply not capable of being performed mentally.

Accordingly, claims 1-20 do not fit into any of the categories for abstract ideas recited in the *2019 Revised Guidance*, including mathematical concepts, certain methods of organizing human activity, and mental processes. They accordingly, at Step 2A, would not be found to be “directed to” a judicial exception.

Furthermore, even if, *arguendo*, the claims were found to fall within one of those categories, the Examiner has not established a *prima facie* case of subject matter ineligibility of claims 1-20 under 35 U.S.C. 101 by failing to show under Step 2A that the claims, as a whole, do not integrate the alleged abstract idea into a practical application. As recited above, one of the examples of “practical applications” that the courts have found is “an improvement in the functioning of a computer, or an improvement to other technology or technical field.” The claims of the instant application “improve the functioning of a computer” and improve the “technical fields” of system, application and process modeling by helping users to model how to implement compensating controls in a computer network, system, application or process to prevent potential threats from harming individual components of the computer network, system, application or process without actually having to build and manually test the computer network, system, application or process. *Claims 1-20*. Accordingly, the claims of the instant application, even if they were found to fall within one of the three judicial exception categories as recited in the *2019 Revised Guidance*, would all nevertheless integrate the alleged abstract idea into a “practical application” such that the claims would be found to be subject matter eligible at Step 2A.

And even if, *arguendo*, the claims were found to be directed to ineligible subject matter under Step 2A and to not integrate the alleged abstract idea into a practical application, the Examiner has not established a *prima facie* case of subject matter ineligibility of claim 1 under 35 U.S.C. 101 by failing to show under Step 2B that the claim does not amount to “significantly more” than an abstract idea. One of the considerations relevant at the Step 2B analysis, referenced above, is whether the claim(s) “purport(s) to improve the functioning of the computer itself” or “any other technology or technical field.” As indicated above, the

claims in fact do improve the functioning of a computer, a computer network, and the technical fields of system, application and process modeling by allowing the user to model how to implement compensating controls in a computer network, system, application or process to prevent potential threats from harming individual components of the computer network, system, application or process without actually having to build/carry out and manually test (such as with penetration testing) the computer network, system, application or process. *Claims 1-20.*

Additionally, one of the considerations relevant at the Step 2B analysis, referenced above, is whether the “additional element(s) are well-understood, routine, conventional activities previously known to the industry.” The Examiner only discusses the “additional elements” of a computing device/system, but there are many more additional elements in the claims, none of which are well-understood, routine, or conventional activities previously known to the industry. For example, the additional elements of displaying threat model groups that can be added to a threat model diagram to automatically modify a threat model by including in it a second threat model, showing attack paths of attacking components, automatically toggling attack paths between mitigated/unmitigated states in response to adding/removing compensating controls from a diagram and/or toggling compensating controls on/off, showing attack paths passing through multiple components, displaying only attack paths of threats associated with a subset of diagrammed threat model components, altering attack paths in response to altering a profile of an attacking component, and storing compensating controls/threats/threat model components in a database and associating them with one another through a user interface, are not well understood, routine, conventional activities previously known to the modeling or threat modeling industries. *Claims 1-20.*

In short, the claims do not fall within any of the three enumerated judicial exception categories and, even if *arguendo* they did, they would integrate the alleged abstract idea into a practical application, so that at Step 2A the claims would be found subject matter eligible, and even if *arguendo* they weren’t they would be found under Step 2B to be subject matter

eligible for reciting “significantly more” than the alleged abstract idea. *Claims 1-20*. The Examiner has accordingly not made a *prima facie* case of subject matter ineligibility under section 101, or the Applicant has successfully rebutted it, and it is respectfully requested that the 101 rejections of claims 1-20 be withdrawn.

CONCLUSION

In conclusion, it is respectfully requested that the application be allowed. If it will in any way speed examination and/or allowance, the Examiner is invited to contact an attorney of record using the contact information listed below.

Respectfully submitted,

Date: October 25, 2019

By: /Paul B. Johnson/

Paul B. Johnson

Reg. No. 59375

Law Office of Paul B. Johnson

8483 S 1275 E

Sandy, UT 84094-1363

Ph: 801.719.5229

Fax: 801.317.8889

paul@pauljohnsonlaw.com

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875				Application or Docket Number 16/228,738		Filing Date 12/20/2018		☐ To be Mailed		
ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO										
APPLICATION AS FILED - PART I										
		(Column 1)	(Column 2)							
FOR		NUMBER FILED	NUMBER EXTRA	RATE (\$)		FEE (\$)				
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))		N/A	N/A	N/A						
☐ SEARCH FEE (37 CFR 1.16(k), (l), or (m))		N/A	N/A	N/A						
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))		N/A	N/A	N/A						
TOTAL CLAIMS (37 CFR 1.16(i))		minus 20 =	*	x \$50 =						
INDEPENDENT CLAIMS (37 CFR 1.16(h))		minus 3 =	*	x \$230 =						
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))		If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).								
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))										
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL						
APPLICATION AS AMENDED - PART II										
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT	10/25/2019	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	x \$50 =		0		
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0	x \$230 =		0		
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE		0		
		(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)		ADDITIONAL FEE (\$)		
	Total (37 CFR 1.16(i))	*	Minus	**	=	x \$0 =				
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x \$0 =				
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))									
						TOTAL ADD'L FEE				
* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.						LIE				
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".						/SHERRY A DAVIS/				
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".										
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.										

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Doc Code: DIST.E.FILE Document Description: Electronic Terminal Disclaimer - Filed		PTO/SB/26 U.S. Patent and Trademark Office Department of Commerce
Electronic Petition Request	TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A "PRIOR" PATENT	
Application Number	16228738	
Filing Date	20-Dec-2018	
First Named Inventor	Anurag Agarwal	
Attorney Docket Number	ThreatM008	
Title of Invention	Threat Model Chaining and Attack Simulation Systems and Related Methods	
☒ Filing of terminal disclaimer does not obviate requirement for response under 37 CFR 1.111 to outstanding Office Action ☒ This electronic Terminal Disclaimer is not being used for a Joint Research Agreement.		
Owner	Percent Interest	
ThreatModeler Software Inc.	100%	
<p>The owner(s) with percent interest listed above in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application which would extend beyond the expiration date of the full statutory term of prior patent number(s)</p> <p>10255439</p> <p>10200399</p> <p>as the term of said prior patent is presently shortened by any terminal disclaimer. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.</p> <p>In making the above disclaimer, the owner does not disclaim the terminal part of the term of any patent granted on the instant application that would extend to the expiration date of the full statutory term of the prior patent, "as the term of said prior patent is presently shortened by any terminal disclaimer," in the event that said prior patent later:</p> <ul style="list-style-type: none"> - expires for failure to pay a maintenance fee; - is held unenforceable; - is found invalid by a court of competent jurisdiction; - is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321; - has all claims canceled by a reexamination certificate; - is reissued; or - is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer. 		

- ☐ Terminal disclaimer fee under 37 CFR 1.20(d) is included with Electronic Terminal Disclaimer request.
- ☒ I certify, in accordance with 37 CFR 1.4(d)(4), that the terminal disclaimer fee under 37 CFR 1.20(d) required for this terminal disclaimer has already been paid in the above-identified application.

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

I certify, in accordance with 37 CFR 1.4(d)(4) that I am:

- ☒ An attorney or agent registered to practice before the Patent and Trademark Office who is of record in this application
- Registration Number 59375
- ☐ A sole inventor
- ☐ A joint inventor; I certify that I am authorized to sign this submission on behalf of all of the inventors as evidenced by the power of attorney in the application
- ☐ A joint inventor; all of whom are signing this request

Signature	/Paul B. Johnson/
Name	Paul B. Johnson

*Statement under 37 CFR 3.73(b) is required if terminal disclaimer is signed by the assignee (owner).
Form PTO/SB/96 may be used for making this certification. See MPEP § 324.

Doc Code: DISQ.E.FILE

Document Description: Electronic Terminal Disclaimer – Approved

Application No.: 16228738

Filing Date: 20-Dec-2018

Applicant/Patent under Reexamination: Agarwal

Electronic Terminal Disclaimer filed on November 12, 2019

☒ APPROVED

This patent is subject to a terminal disclaimer

☐ DISAPPROVED

Approved/Disapproved by: Electronic Terminal Disclaimer automatically approved by EFS-Web

U.S. Patent and Trademark Office

Electronic Acknowledgement Receipt

EFS ID:	37730970
Application Number:	16228738
International Application Number:	
Confirmation Number:	3702
Title of Invention:	Threat Model Chaining and Attack Simulation Systems and Related Methods
First Named Inventor/Applicant Name:	Anurag Agarwal
Customer Number:	145042
Filer:	Paul B. Johnson
Filer Authorized By:	
Attorney Docket Number:	ThreatM008
Receipt Date:	12-NOV-2019
Filing Date:	20-DEC-2018
Time Stamp:	17:59:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer-Filed (Electronic)	eTerminal-Disclaimer.pdf	32033	no	2
			db77d186a53667e99d9120489a5859fc71d3d18a		

Warnings:

IriusRisk

Information:	
Total Files Size (in bytes):	32033
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	12/20/2018	Anurag Agarwal	ThreatM008	3702
145042	7590	11/20/2019		
Law Office of Paul B. Johnson 8483 S. 1275 E. Sandy, UT 84094-1363			EXAMINER SONG, HOSUK	
			ART UNIT	PAPER NUMBER
			2435	
			NOTIFICATION DATE	DELIVERY MODE
			11/20/2019	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

paul@pauljohnsonlaw.com

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP §§ 706.02(I)(1) - 706.02(I)(3) for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10200399. Although the claims at issue are not identical, they are not patentably distinct from each other (see table below).

<u>Instant Application</u>	<u>U.S. Patent No. 10200399</u>
Claim 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	Claim 1: A threat model chaining and system configuration method, comprising: In response to receiving one or more user inputs, using one or more interfaces displayed on a display of a computing device communicatively coupled with a database: storing a plurality of threat model components in the database; storing a plurality of threats in the database associating each threat with at least one of the threat model components through the database; storing a plurality of compensating controls in the database;

<p>with at least one of the threats through the one or more databases;</p> <p>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;</p> <p>configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representation of one or more of the threat model components and visual representation of one or more of the compensating controls, the relational diagram defining a first threat model, and;</p> <p>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.</p>	<p>associating each compensating control with at least one of the threats through the database;</p> <p>displaying , using a diagram interface, a relational diagram of a system, 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;</p> <p>adding a component group to the first threat model and thereby redefining 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, and;</p> <p><i>physically arranging tangible components matching the threat model components of the diagrammed system to form an actual system, the actual system mitigating actual threats corresponding with the threats of the first threat model.</i></p>
---	--

Although the conflicting claims are not identical, they are not patentably distinct from each other because both are directed to detecting threat using a plurality of threat model and configuring the diagram interface to display a relational diagram using one or more threat model; and only differing in that the claims of '399 patent explicitly recite physically arranging tangible components matching the threat model components of the diagrammed system to form an actual system, the actual system mitigating actual threats corresponding with the threats of the first threat model. Thus the claims of the '399 patent are rendered as obvious variants of the instant claims.

Claims 1-20 are rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10255439. Although the claims at issue are not identical, they are not patentably distinct from each other (see table below).

<u>Instant Application</u>	<u>U.S. Patent No. 10200399</u>
Claim 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	Claim 1: A threat model and system configuration method, comprising: In response to receiving one or more user inputs, using one or more input interfaces displayed on a display of a computing device communicatively coupled with a database: storing a plurality of threats in the database; storing a plurality of threats in the database; associating each threat with at least one of the threat model components through the database; storing a plurality of security requirements in the database, including storing an indication of

<p>with at least one of the threats through the one or more databases;</p> <p>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;</p> <p>configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representation of one or more of the threat model components and visual representation of one or more of the compensating controls, the relational diagram defining a first threat model, and;</p> <p>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.</p>	<p>whether each security requirement is a compensating control;</p> <p>associating each compensating control with at least one of the threats through the database;</p> <p>displaying a relational diagram of a system, using visual representations of one or more of the threat model components, the diagram defining a threat model;</p> <p>generating and displaying a threat report displaying each threat that is associated through the databases with one of the threat model components included in the threat model, wherein the threat report displays a threat status for each threat indicating whether that threat has been mitigated, and wherein the threat report includes one or more input fields configured to manually change each threat status;</p> <p>generating and displaying a report displaying each compensating control that is associated through the database with one of the threats included in the threat report;</p> <p>removing one of the compensating controls from the diagram and automatically changing the threat status of at least one of the threats</p>
---	---

	<p>included in the threat report to an unmitigated status, and;</p> <p>physically arranging tangible components matching the threat model components of the diagrammed system to form an actual system, the actual system mitigating actual threats corresponding with the threats displayed in the threat report.</p>
--	--

Although the conflicting claims are not identical, they are not patentably distinct from each other because both are directed to detecting threat using a plurality of threat model and configuring the diagram interface to display a relational diagram using one or more threat model; and only differing in that the claims of '439 patent explicitly recite removing one of the compensating controls from the diagram and automatically changing the threat status of at least one of the threats included in the threat report to an unmitigated status, and physically arranging tangible components matching the threat model components of the diagrammed system to form an actual system, the actual system mitigating actual threats corresponding with the threats displayed in the threat report. Thus the claims of the '439 patent are rendered as obvious variants of the instant claims.

Response to Applicant's Arguments

The previous ground of rejection based on 35 U.S.C. 101 is withdrawn in view of applicant's argument filed 10/25/19. However, claims 1-20 remain rejected on the ground of nonstatutory double patenting as being unpatentable over claims 1-20 of U.S. Patent No. 10200399 and U.S. Patent No. 10255439 due to missing Terminal Disclaimer.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

USPTO Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HOSUK SONG whose telephone number is (571)272-3857. The examiner can normally be reached on Mon-Fri: 7:30AM-5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on 571-272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair->

Art Unit: 2435

direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/HOSUK SONG/

Primary Examiner, Art Unit 2435

<i>Search Notes</i> 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/577; G06F21/552; G06F 21/554; G06FG06F 17/30283; H04L 63/1433; H04L 63/20	07/31/2019	HS
G06F 21/577; G06F21/552; G06F 21/554; G06FG06F 17/30283; H04L 63/1433; H04L 63/20	11/06/2019	HS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
EAST, foreign patent database, IBM TDB, USPGPUB, inventor name search	07/31/2019	HS
CPC search with keywords	07/31/2019	HS
NPL(IEEE) with keywords	07/31/2019	HS
EAST, foreign patent database, IBM TDB, USPGPUB, inventor name search	11/06/2019	HS
CPC search with keywords	11/06/2019	HS

--	--

<i>Search Notes</i> 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
726	22-25	07/31/2019	HS
726	22-25	11/06/2019	HS

--	--

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S112	568	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 16:29
S113	69024	(G06F21/577 OR G06F21/552 OR G06F21/554 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 16:29
S114	1	("agarwal, anurag").INV. and 726/\$.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 16:33
S115	6	(threats and database and diagram\$5 and model and control\$4 and (visual or display\$4)).CLM.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 16:33
S116	2874	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 16:36
S117	254	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 16:36
S118	20	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/22.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 16:39
S119	49	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/23.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 16:41
S120	15	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4)	US-PGPUB; USPAT;	OR	ON	2019/11/06 17:17

		near5 (database or storage or record) and 726/24.ccls.	FPRS; EPO; JPO; DERWENT; IBM_TDB			
S121	78	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/25.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 17:17
S122	242	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 17:17
S124	159	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 19:08
S125	168	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 19:08
S126	140	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 19:08
S127	7	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and 726/22.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2019/11/06 19:08

11/ 7/ 2019 6:53:20 AM
C:\Users\hsong\Documents\EAST\Workspaces\16228738.wsp

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

Nov 20, 2019 03:35:45 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	CTFR	11/20/2019	ThreatM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16228738
	Filing Date	2018-12-20
	First Named Inventor	Anurag Agarwal
	Art Unit	2435
	Examiner Name	Song, Hosuk
	Attorney Docket Number	ThreatM008

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					
If you wish to add additional U.S. Patent citation information please click the Add button.						Add
U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20170213037	A1	2017-07-27	Toledano et al.	
	2	20180255084	A1	2018-09-06	Kotinas et al.	
	3	20150033346	A1	2015-01-29	Hebert et al.	
	4	20140157417	A1	2014-06-05	Grubel et al.	
	5	20110277034	A1	2011-11-10	Hanson	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Song, Hosuk
Attorney Docket Number	ThreatM008

6	20160248798	A1	2016-08-25	Cabrera et al.
---	-------------	----	------------	----------------

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Song, Hosuk
Attorney Docket Number	ThreatM008

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Paul B. Johnson/	Date (YYYY-MM-DD)	2019-11-25
Name/Print	Paul B. Johnson	Registration Number	59375

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	37857000
Application Number:	16228738
International Application Number:	
Confirmation Number:	3702
Title of Invention:	Threat Model Chaining and Attack Simulation Systems and Related Methods
First Named Inventor/Applicant Name:	Anurag Agarwal
Customer Number:	145042
Filer:	Paul B. Johnson
Filer Authorized By:	
Attorney Docket Number:	ThreatM008
Receipt Date:	25-NOV-2019
Filing Date:	20-DEC-2018
Time Stamp:	21:04:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS2.pdf	1034495	no	4
			4f293d71721819a4590c102fab4dd10e60b ec718		

Warnings:

IriusRisk

Information:	
Total Files Size (in bytes):	1034495
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		16228738
	Filing Date		2018-12-20
	First Named Inventor	Anurag Agarwal	
	Art Unit	2435	
	Examiner Name	Hosuk Song	
	Attorney Docket Number	ThreatM008	

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	10262132	B2	2019-04-16	Reinecke et al.	
	2	7624448	B2	2009-11-24	Coffman	
	3	7260844	B1	2007-08-21	Tidwell et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

[Add](#)

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20160162690	A1	2016-06-09	Reith et al.	
	2	20170213037	A1	2017-07-27	Toledano et al.	
	3	20180255084	A1	2018-09-06	Kotinas et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

4	20150033346	A1	2015-01-29	Hebert et al.
5	20140157417	A1	2014-06-05	Grubel et al.
6	20110277034	A1	2011-11-10	Hanson
7	20160248798	A1	2016-08-25	Cabrera et al.

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS

[Remove](#)

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button. [Add](#)

NON-PATENT LITERATURE DOCUMENTS

[Remove](#)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		

If you wish to add additional non-patent literature document citation information please click the Add button. [Add](#)

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Paul B. Johnson/	Date (YYYY-MM-DD)	2020-01-01
Name/Print	Paul B. Johnson	Registration Number	59375

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal				
Application Number:		16228738		
Filing Date:		20-Dec-2018		
Title of Invention:		Threat Model Chaining and Attack Simulation Systems and Related Methods		
First Named Inventor/Applicant Name:		Anurag Agarwal		
Filer:		Paul B. Johnson		
Attorney Docket Number:		ThreatM008		
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	120	120
Total in USD (\$)				120

Electronic Acknowledgement Receipt

EFS ID:	38179019
Application Number:	16228738
International Application Number:	
Confirmation Number:	3702
Title of Invention:	Threat Model Chaining and Attack Simulation Systems and Related Methods
First Named Inventor/Applicant Name:	Anurag Agarwal
Customer Number:	145042
Filer:	Paul B. Johnson
Filer Authorized By:	
Attorney Docket Number:	ThreatM008
Receipt Date:	01-JAN-2020
Filing Date:	20-DEC-2018
Time Stamp:	18:29:39
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 120
RAM confirmation Number	E202011I30446732
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

IriusRisk

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS3.pdf	1034664	no	5
			1903fa99bddc99b6d9c692a6ae934b11c8c39280		
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30179	no	2
			25ea7ba8a6299aaa83b7c35895a5a32b25aefbee		
Warnings:					
Information:					
Total Files Size (in bytes):			1064843		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: ThreatModeler Software Inc.

Docket No: THREATM008

Examiner: Song, Hosuk

Ser. No: 16228738

Filed: December 20, 2018

Group Art Unit: 2435

Title: Threat Model Chaining and Attack Simulation Systems and Related Methods

SUMMARY OF APPLICANT INITIATED EXAMINER INTERVIEW

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner:

Counsel for applicant left a voicemail for the examiner on Nov. 20, 2019 indicating that, although the 11/20/19 office action was final and had maintained the double patenting rejection, a terminal disclaimer related to the relevant references had been filed in the case a few days prior on 11/12/19. Examiner left a voicemail later that same day and indicated that a notice of allowance would be forthcoming.

Sincerely,

Date: January 11, 2020

By: /Paul B. Johnson/
Paul B. Johnson
Reg. No. 59375

Law Office of Paul B. Johnson
8483 S 1275 E
Sandy, UT 84094-1363
Ph: 801.719.5229
Fax: 801.317.8889
paul@pauljohnsonlaw.com

Electronic Acknowledgement Receipt

EFS ID:	38270471
Application Number:	16228738
International Application Number:	
Confirmation Number:	3702
Title of Invention:	Threat Model Chaining and Attack Simulation Systems and Related Methods
First Named Inventor/Applicant Name:	Anurag Agarwal
Customer Number:	145042
Filer:	Paul B. Johnson
Filer Authorized By:	
Attorney Docket Number:	ThreatM008
Receipt Date:	11-JAN-2020
Filing Date:	20-DEC-2018
Time Stamp:	03:07:44
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Applicant summary of interview with examiner	InterviewSummary.pdf	41878	no	1
			6708066ad32c37f5e6cffa4b509ef785406a846		

Warnings:

IriusRisk

Information:	
Total Files Size (in bytes):	41878
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16228738
	Filing Date	2018-12-20
	First Named Inventor	Anurag Agarwal
	Art Unit	2435
	Examiner Name	Hosuk Song
	Attorney Docket Number	ThreatM008

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010027388	A1	2001-10-04	Beverina et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

1	Roy, Maurer. "Top Database Security Threats and How to Mitigate Them." July 30, 2015. Retrieved from "https://www.shrm.org/resouresandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx" (Year: 2015).
2	A. Amini, N. Jamil, A.R. Ahmad and M.R. Z'aba, 2015. Threat Modeling Approaches for Securing Cloud Computing. Journal of Applied Sciences, 15: 953-967. Retrieved from "https://scialert.net/fulltextmobile/?doi=jas.2015.953.967" (Year: 2015).

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Paul B. Johnson/	Date (YYYY-MM-DD)	2020-01-27
Name/Print	Paul B. Johnson	Registration Number	59375

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Top Database Security Threats and How to Mitigate Them

By Roy Maurer

July 30, 2015

Every day, hackers unleash attacks designed to steal confidential data, and an organization's database servers are often the primary targets of these attacks. Databases are one of the most compromised assets according to the 2015 Verizon Data Breach Investigations Report (<http://www.verizonenterprise.com/DBIR/>).

"The reason databases are targeted so often is quite simple—they are at the heart of any organization, storing customer records and other confidential business data," said Morgan Gerhart, vice president of product marketing at cybersecurity firm Imperva (<http://www.imperva.com/>). Organizations are not protecting these crucial assets well enough, he added.

"When hackers and malicious insiders gain access to sensitive data, they can quickly extract value, inflict damage or impact business operations. In addition to financial loss or reputation damage, breaches can result in regulatory violations, fines and legal fees," he said.

Top Database Threats

The threats identified over the last couple of years are the same that continue to plague businesses today, according to Gerhart. The most common database threats include:

***Excessive privileges.** When workers are granted default database privileges that exceed the requirements of their job functions, these privileges can be abused, Gerhart said. "For example, a bank employee whose job requires the ability to change only account holder contact information may take advantage of excessive database privileges and increase the account balance of a colleague's savings account." Further, some companies fail to update access privileges for employees who change roles within an organization or leave altogether.

***Legitimate privilege abuse.** Users may abuse legitimate database privileges for unauthorized purposes, Gerhart said.

***Database injection attacks.** The two major types of database injection attacks are SQL injections that target traditional database systems and NoSQL injections that target "big data" platforms. "A crucial point to realize here is that, although it is technically true that big data solutions are impervious to SQL injection attacks because they don't actually use any SQL-based technology, they are, in fact, still susceptible to the same fundamental class of attack," Gerhart said. "In both types, a successful input injection attack can give an attacker unrestricted access to an entire database."

***Malware.** A perennial threat, malware is used to steal sensitive data via legitimate users using infected devices.

***Storage media exposure.** Backup storage media is often completely unprotected from attack, Gerhart said. "As a result, numerous security breaches have involved the theft of database backup disks and tapes. Furthermore, failure to audit and monitor the activities of administrators who have low-level access to sensitive information can put your data at risk. Taking the appropriate measures to protect

We use cookies to improve your browsing experience on our website, and we use our own, as well as third-party cookies, to display advertising for products and services we believe may be of interest to you. By closing this message or continuing to browse this site, you agree to the use of cookies in accordance with our [Cookie Policy](#).

Feedback



***Exploitation of vulnerable databases.** It generally takes organizations months to patch databases, during which time they remain vulnerable. Attackers know how to exploit unpatched databases or databases that still have default accounts and configuration parameters. “Unfortunately, organizations often struggle to stay on top of maintaining database configurations even when patches are available. Typical issues include high workloads and mounting backlogs for the associated database administrators, complex and time-consuming requirements for testing patches, and the challenge of finding a maintenance window to take down and work on what is often classified as a business-critical system,” Gerhart said.

***Unmanaged sensitive data.** Many companies struggle to maintain an accurate inventory of their databases and the critical data objects contained within them. “Forgotten databases may contain sensitive information, and new databases can emerge without visibility to the security team. Sensitive data in these databases will be exposed to threats if the required controls and permissions are not implemented,” he said.

***The human factor.** The root cause for 30 percent of data breach incidents is human negligence, according to the Ponemon Institute Cost of Data Breach Study (<http://www-03.ibm.com/security/data-breach/>). “Often this is due to the lack of expertise required to implement security controls, enforce policies or conduct incident response processes,” Gerhart said.

Multilayered Security Solutions

A defensive matrix of best practices and internal controls is needed to properly protect databases, according to Imperva. This matrix includes:

- Assessing for any database vulnerabilities, identifying compromised endpoints and classifying sensitive data.
- Managing user access rights and removing excessive privileges and dormant users.
- Monitoring all database access activity and usage patterns in real time to detect data leakage, unauthorized SQL and big data transactions, and protocol and system attacks.
- Blocking malicious web requests.
- Automating auditing with a database auditing and protection platform.
- Archiving external data and encrypting databases.
- Training employees on risk-mitigation techniques including how to recognize common cyberthreats such as a spear-phishing attack, best practices around Internet and e-mail usage, and password management. “Failure to enforce training and create a security-conscious work culture increases the chances of a security breach,” Gerhart said.

Roy Maurer is an online editor/manager for SHRM.

Follow him @SHRMRoy (<https://twitter.com/SHRMRoy>)

HR DAILY NEWSLETTER

News, trends and analysis, as well as breaking news alerts, to help HR professionals do their jobs better each business day.

Email Address

We use cookies to improve your browsing experience on our website, and we use our own, as well as third-party cookies, to display advertising for products and services we believe may be of interest to you. By closing the message or continuing to browse this site, you agree to the use of cookies in accordance with our [Cookie Policy](#).

Feedback

X

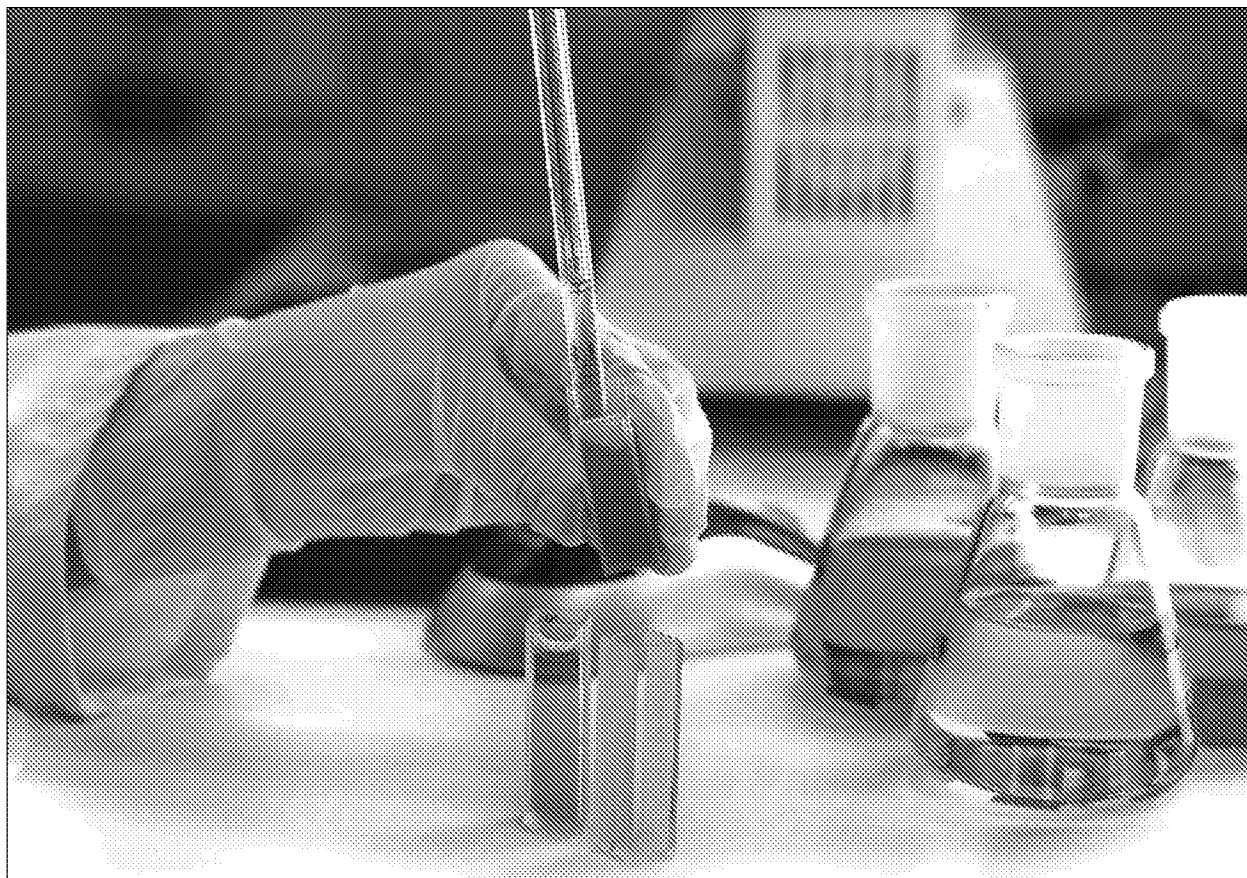
© 2020 SHRM. All Rights Reserved

SHRM provides content as a service to its readers and members. It does not offer legal advice, and cannot guarantee the accuracy or suitability of its content for a particular purpose.

Disclaimer (www.shrm.org/about-shrm/Pages/Terms-of-Use.aspx#Disclaimer)

Feedback





Journal of Applied Sciences

ISSN 1812-5654

science
alert

ANSI*net*
an open access publisher
<http://ansinet.com>

RESEARCH ARTICLE

OPEN ACCESS

DOI: 10.3923/jas.2015.953.967

Threat Modeling Approaches for Securing Cloud Computing

¹A. Amini, ¹N. Jamil, ¹A.R. Ahmad and ²M.R. Z'aba

¹College of Information Technology, Universiti Tenaga Nasional, Selangor, Malaysia

²MIMOS Berhad, Technology Park Malaysia, Kuala Lumpur, Malaysia

ARTICLE INFO

Article History:

Received: December 29, 2014

Accepted: April 25, 2015

Corresponding Author:

A. Amini

College of Information Technology,
Universiti Tenaga Nasional,
Selangor, Malaysia

ABSTRACT

The cloud computing delivers services of processing data by using parallel and high computational processors virtually and remotely. This is very useful and beneficial to enterprises that have limitations in terms of processing resources, data storages and man power. However, one of the main challenge in cloud computing is data security. Supposed each user has an access to the domain based on the privilege given by the server. However, an attacker always has the opportunity to bypass the privilege by exploring and exploiting every vulnerability and threat found in the cloud computing environment. A systematic approach to identify vulnerabilities and threats is thus very important to ensure only authorized party is allowed to access the data. In this study, several approaches of vulnerability and threat modeling are reviewed and found that none of them is suitable for the cloud computing environment. Therefore, authors presented a dynamic model of identifying vulnerabilities and threats in the cloud computing environment. The proposed model enables the organization to systematically identify vulnerability and threats and analyze the security risk when they use cloud computing services.

Key words: Cloud computing, data security, threat modeling, vulnerability

INTRODUCTION

Cloud computing as a new distributed computing paradigm delivers on-demand services by decreasing capital investment on infrastructure and maximizing the usage of available resources. Cloud technology brings application and infrastructure services mobility and physical/hardware platform independency to the existing distributed computing and networking application (Demchenko *et al.*, 2012). By growing cloud computing and making compute resources available for consumers, IT industry becomes more flexible, scalable, capable and cost effective for developing and hosting applications. However, by adopting this new powerful emerging system, security has been cited as the most essential and critical issue. For understanding security issues, threats, vulnerabilities and risks should be analysed as different factors that influenced cloud computing security.

Threat modeling as a systematic and comprehensive analysis of threats and vulnerabilities is needed to provide confidentiality, integrity and availability for deploying cloud computing security. Threat modeling collects background information required in the form of usage scenario, external dependencies, implementation assumption, internal and

external security implementation detail (Malik *et al.*, 2008). A number of threat modeling techniques have been developed for evaluating and analyzing the threats and vulnerabilities such as:

- Microsoft threat modeling is a model to offer an efficient process that includes five logical steps from classifying assets to addressing and classifying threats and vulnerabilities
- Microsoft's Threat Analysis and Modeling (TAM) (Malik *et al.*, 2008) is a model based on business objectives that have to be met by application. The TAM tools have been used to generate and classify threats by measuring their harm effects on system's components
- Practical Threat Analysis (PTA) (McRee, 2008) defines an effective risk mitigation plan for specific system architecture to obtain the value of system's assets
- Threat model framework and methodology for Personal Networks (PNs) (Jehangir and de Groot, 2012). This threat model by analyzing personal network gives a good view of system's assets and their values. Determining all assets by UML diagrams gives opportunity to protect data and network functions against any threats

- Threat modeling in pervasive computing paradigm by developing cloud computing, each user is faced by different security domains with multi identify. The above model presents a new threat modeling to incorporate the problem of pervasive computing environment

Unfortunately by growing cloud as a large scalable distributed computing, all above methodologies do not incorporate problems, so new approaches for threat modeling have to be evolved to solve problems of pervasive computing security.

This study presents a methodology of the threat model to deploy a secure computing environment by showing threats and vulnerabilities in the cloud computing and determining security solutions. The proposed methodology to build threat model consists of several steps, those after considering all steps the result represents the final threat model for cloud computing.

MATERIALS AND METHODS

Security issues of cloud computing: Before, a closer look is taken at cloud-specific threats, vulnerabilities and solutions, we define vulnerability and threat as follows:

- Threat is harm or unauthorized access that might occur due to vulnerability and destroy organization assets, organization operations or system information
- Vulnerability is any weakness in information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat resources (Bertino *et al.*, 2010)

Cloud computing threats: Cloud Security Alliance (CSA) (Soares *et al.*, 2013) as a security assurance provider released the security guidance for critical areas in cloud computing for managing risks and understanding security threats. The most of significant threats that are related to on-demand nature of cloud computing are categorized as below:

- **Data lose or leakage (T1):** This threat is measured as the most critical and terrifying threat for businesses and consumers. Any data deletion by service provider or baleful accident such as fire can lead to lose the consumer's data
- **Account or service hijacking (T2):** This weakness allows attackers to steal credentials and access to critical areas of cloud computing services. The organization should prohibit the sharing of credentials between different services and users and use strong authentication techniques
- **Insecure interface (T3):** Cloud computing's customers use Application Programming Interface (API) or software interfaces to interact and manage cloud services. Authentication, access control and monitoring technologies for APIs protect computing resources from malicious attacks

- **Denial of service (T4):** Distributed Denial of Service (DDoS) is the major security threat to availability when it comes to increase reliability of organizations on public cloud services (Lohman, 2011). On the other hand, this attack prevents users from accessing their data or applications and there is no way to reach their destination. Cloud service providers need to be sure about availability protection and customers need to be sure about the level of availability protection within a provider
- **Malicious insider (T5):** The system has been damaged by authorized employee, business partner or administrator that has access to a network or resources. This dangerous threat affects the confidentiality, integrity or availability of business information
- **Data breaches (T6):** One of the worse situations for each organization is unauthorized access or illegal viewing data by competitors. Data encryption can reduce the risk of this threat, but should be careful about encryption key because if you lose it, you will lose your data as well
- **Abuse of cloud services (T7):** Cloud computing providers do not enforce any strong registration process and any user with a valid credit card can register to receive cloud services (Hamza *et al.*, 2013). Integrating of registration faint and weak fraud detection allow attacker to leverage data by offensive cloud models same as PaaS and IaaS
- **Insufficient due diligence (T8):** The cost reduction, access to pool of resources and improving security are the most important interesting factors for organization to rush cloud computing. Without understanding of Cloud Service Provider (CSP) environment, mismatched expectation has been created as a critical issue on security control of cloud computing. However, for sufficient qualification of resources, organizations have to understand the service provider offerings and risks
- **Insecure VM migration (T9):** By migrating different VMs during hybrid and federated clouds, attackers can access data illegally and transfer VM to untrusted host (Hashizume *et al.*, 2013). Virtualization as the main component of IaaS is the main goal to be targeted by attackers. Trusted cloud computing and encryption technology protect data resources from insecure VM migration

Threat of shared vulnerabilities exists in all models (IaaS, PaaS, SaaS) because underlying components that deploy infrastructure, platforms and applications does not offer strong isolation between cloud computing models.

Cloud computing vulnerability: Vulnerability is a probability of an asset that will be unable to resist the action of a threat agent (The Open Group, 2009). By moving organization's critical data and applications to cloud computing, different significant vulnerabilities should be considered based on CC's

technologies, essential cloud characteristics, known security controls and state-of-the-art cloud offerings (Grobauer *et al.*, 2011). In this study, indicators were discussed as cloud specific vulnerabilities:

- **Session riding (V1):** Session riding refers to send command to web application by hackers to gain unauthorized access for the information or use web service weaknesses for giving the chance to hackers to do malicious activities same as deleting of user data or sending spam to a network via internet
- **Virtual machine escape (V2):** This vulnerability allows attacker runs code on a VM that let operating system to break out and interact directly with the hypervisor to access host operating system and other virtual machines (Rouse, 2009). For detecting and preventing system should detect malicious activity at VM level
- **Obsolete cryptography (V3):** Developing not enough strong encryption or no encryption at all allows attacker to decode encrypted data. To protect system from this vulnerability, user should be sure the true data is encrypted, use proper key storage and develop a good algorithm
- **Unauthorized access to management interface (V4):** The cloud management interface has access to cloud service users to manage on-demand services. An unauthorized access enables attackers to gain total control of users and applications
- **Internet protocol (V5):** The lack of authentication methods that is not a part of the base protocol design, allows attackers to inject their malicious traffic to network. On the other hand, the IP protocol or related protocols same as UDP and TCP are vulnerable to different type of Denial of Service (DoS) attacks, including session hijacking and cash poisoning
- **Data recovery (V6):** Cloud computing allows resources to be allocated or reallocated by different users. This elastic characteristic could lead to data stolen, data breaches and other security threats. The most of organizations use third party vendors to recover data so they should consider security risk of handling data with outside company and ensure proper security vetting of the service provider (Kenyon, 2010)
- **Metering and billing (V7):** Cloud computing meters and measures services such as storage, user account and processing are used to optimize service delivery. Applicable vulnerabilities contain metering and billing data treatment and billing elusion (Rai and Bunkar, 2014)
- **Vendor lock-in (V8):** Vendor lock-in is the situation that cloud's user is dependent to a single vendor and is unable to deal with another provider without substantial and inconvenience. The lack of the standards is the main reason that users cannot transfer easily from one provider to another.

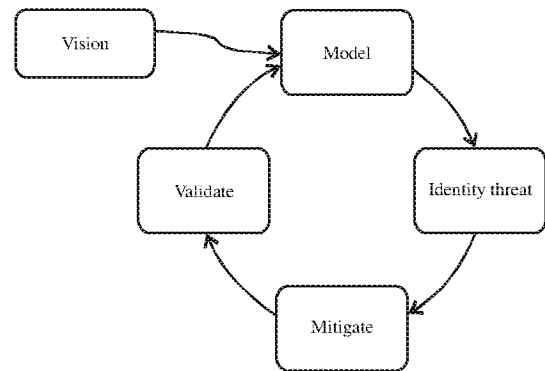


Fig. 1: SDLC process diagram

Existing threat modeling frameworks: In this section, existing threat models are discussed and new approach has been evolved to satisfy and fulfill cloud computing as a pervasive computing paradigm.

Microsoft threat modeling: Threat modeling as a core of the Microsoft Security Development Lifecycle (SDL) (Fig. 1), proposes a model to identify and mitigate threats and vulnerabilities by reducing the total cost of development process. This methodology offers a good process cycle by following five logical steps, start from classifying assets, system overview by creating Data Follow Diagram (DFD), modeling and identifying threats by using STRIDE¹, addressing issues and finally ranking the threats by DREAD².

Vulnerabilities as an important and hazardous security risk in cloud computing have to be addressed by threat model but Microsoft threat modeling cannot model vulnerabilities. Another important challenge to adopt this popular model with cloud computing is predefining a set of threats as STRIDE. In addition, STRIDE defines a static method to identify threats that cannot be used in dynamic computing environment. For instance, denial of service as one of the top ranked threat in 2013 was not listed as cloud computing threats in 2010. However, defining new threats which are more critical than expected STRIDE, should be intended in our new threat model.

Microsoft's Threat Analysis and Modeling (TAM): Threat Analysis and Modeling (TAM) proposes a model to identify threats and facilitate system to define a security strategy (Fig. 2) (Malik *et al.*, 2008). In the first step of this model, threat modeling has been addressed on the base of business objectives. Business objectives involve business needs and problems that have to be fulfilled by the application. Components as the main part of application's architecture, technology of creating components, user roles, trust level, authentication mechanisms and external dependencies are define as a second step. In the third step, TAM's tools generate

¹STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of Privilege

²DREAD: Damage potential, Reproducibility, Exploitability, Affected users, Discoverability

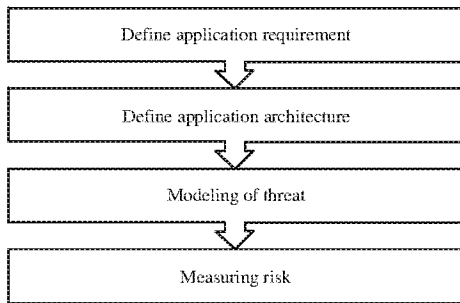


Fig. 2: TAN process diagram

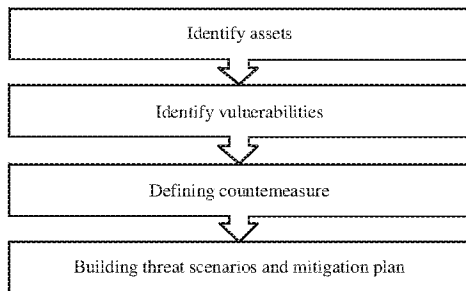


Fig. 3: PTA process diagram

and classify threats into confidentiality, integrity and availability. In the last step each threat is measured on the base of business needs.

The proposed threat modeling for computing environment unlike TAM has to determine assets which could be damaged by threats and need protection. The lack of identifying vulnerabilities is another issue of Microsoft threat analysis and modeling. On the other hand, determining and ranking threats are done as well in this model but this detecting and ranking vulnerability that are damaged by threats are not deployed.

Practical threat analysis: The Practical Threat Analysis (PTA) proposed a model to identify system vulnerabilities, map system assets, assess the risk of the threats and define an effective risk mitigation plan for a specific system architecture, functionality and configuration (McRee, 2008). The PTA by providing free tools for threat modeling allows provider to obtain system's assets values and level of damage that is caused by the attackers. The main functionality of PTA is defining a risk mitigation plan on the base of identify vulnerabilities and assets and assess the risk of threats. PTA technologies present PTA threat modeling and risk assessment that is shown in Fig. 3. Identifying assets and their financial values is done in the first step. The second step represents system's vulnerabilities on the base of architecture, functionality and different type of users. The effect of cost is calculated on the base of implementation cost. In the last step, threat scenario has been built to identify various threat and level of damage.

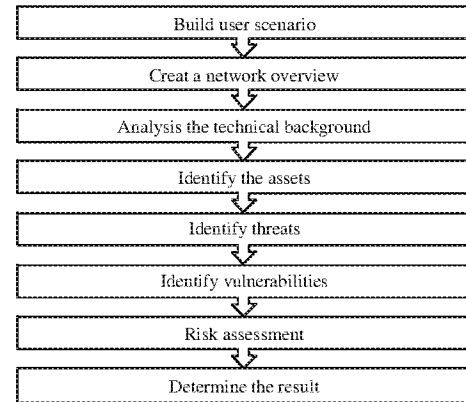


Fig. 4: Threat model for PNs

No risk evaluation method or methodology to calculate vulnerability's cost is an important issue. Actually, the cost of replacement, restoration or system down times is required to calculate the cost of vulnerabilities and thereby it gives idea to avoid system from different threats. The second disadvantage of this model is unranking vulnerability sizes. In the pervasive computing environment all known and credible vulnerabilities should be addressed. Anyway, vulnerabilities have to be ranked because known vulnerabilities can be eliminated and for unknown, some solutions should be deliberated. In PTA model, threats are ranked only by their financial values not by technical, functional, strategic or reputational values. Cloud computing as a complex multi-tenant environment, provides ability for users to be a member of different domains at the same times. In this situation, different factors and levels of security on the base of user's role should be considered to address threats not only financial values.

Threat model framework and methodology for Personal Networks (PNs): The PN as an intelligent and user-centric network consists of devices belonging to user for personal purpose, develop new application, telecommunications, entertainment and improve services (Jehangir and de Groot, 2012). Figure 4 shows primary steps of proposed threat model for PNs. Each of these main steps consists of some sub-steps (Prasad, 2007).

In the first step, the use case has been derived to describe everything in network from user's view. In the next step, the network requirements have been retrieved from use case diagrams and also network architecture, environment and technologies have been explained. In the third step, UML sequence diagram has been used to clarify data flows and determine which actors and devices are involved. The assets or everything that could be damaged should be determined and protected from harmful attacks in the next step. The fifth step involves all threats and expected result of them. The main outcome is determining threat scenario to extract fundamental threats and likelihood. After discovering threats, it is possible to

see and understand vulnerabilities that are affected by terrible threats. In the seventh step, highest risks have been determined by threat and vulnerabilities profile. The final step consists of the reports that involve threats and vulnerabilities rank on the base of risk and size.

This framework gives a good view of system by describing all network details, covering all functionalities and deploying use case. As mentioned before, in cloud computing user is faced by many services and domains that may have different and unknown vulnerabilities so proposed framework unlike PN's threat model need to be updated by new threats and vulnerability profiles.

Threat modeling in pervasive computing paradigm: By cloud computing as an on-demand service, provides reliability to user's daily life. Each user has multi identifies for different security domain so implementing security schema is a big challenge for cloud computing. This model (Fig. 5) presented as a new threat modeling to incorporate the problem of pervasive computing environment (Malik *et al.*, 2008).

In the first step all user's roles need to be established with their service usage and authentication mechanisms. The use case scenario and diagrams can be used in this method to identify users and their level of access to different services. In the computing environment, each user can be a part of various

domains with different roles. Identifying security domains that is mentioned in step two, presents the way that user interacts with applications inside the domain. Various type of user same as authorized user, admin and unregistered user have different trust levels. Identifying trust level in the third level, assists user to access the resources depending upon its trust level. In the next step, all vulnerabilities need to be detected. Known vulnerabilities can be eliminated and unknown vulnerabilities should be consider to protect system from harm attacks. Risk evaluation as a forth step, presents fair idea to avoid computing environment from threats. Threats have been qualified on the base of cost expectancy that is involved restoration and replacement cost. In the last step, new vulnerabilities and threats have been identified and post them to forth step for keeping system secure.

Today, by developing small and medium enterprises and growing the number of assets, the traditional assets tracking methods cannot be used anymore. In proposed framework unlike above model, cloud based assets management has been developed rather than traditional infrastructure to manage data, software, hardware and etc.

Before have a closer look at proposed model, we illustrate all details of discussed models in Table 1 to analyze and compare existing models by proposed model. Table 1 is based on characteristics of threat model to be adopted by cloud computing. In the next part of this study, each characteristic of new threat modeling schema was discussed to identify and rank threats and vulnerabilities.

RESULTS AND DISCUSSION

Proposed threat model: The proposed model for cloud computing security is shown in Fig. 6. This model consists of four main steps that each step involves some sub steps. The first step is identifying assets and clarifying who or what has access to assets. Trust represented by the term reliability that is using for multiple redundant web services to qualified trust between user and service provider or between different providers. Further, the second step defines capability of provider to provide user requirements literally. Identifying unique threats and addressing them by developing suitable

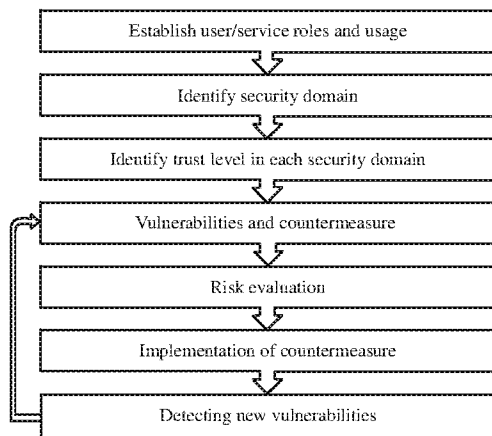


Fig. 5: Threat modeling process for pervasive computing

Table 1: Comparison of existing threat models by proposed model

Characteristics of threat modeling	Existing threat models					
	Microsoft threat modeling	TAM	PTA	Personal network threat modeling	Pervasive computing threat modeling	Proposed threat model
Identifying and classifying assets	✓		✓	✓	✓	✓
Establishing user's roles						✓
Identifying security domains					✓	✓
Estimating trustworthiness					✓	✓
Scanning domain security						✓
Identifying threat	✓	✓		✓	✓	✓
Identifying vulnerability				✓	✓	✓
Implementing countermeasure					✓	✓
Ranking and measuring threats	✓	✓		✓	✓	✓
Ranking and measuring vulnerabilities				✓		✓
Defining new assets, threats or vulnerabilities					✓	✓

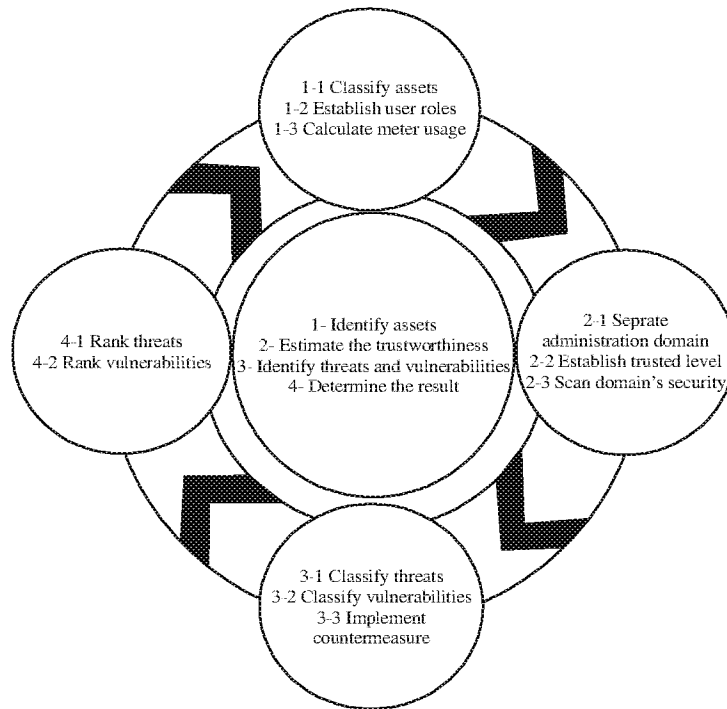


Fig. 6: Proposed threat modeling framework for cloud computing

countermeasure has been demonstrated in the third step. The main goal of this step is detecting and identifying new subsequently threats to improve security. The final step, presents system rating to identify more dangerous and effected threats and vulnerabilities.

Identify assets: The IT asset is data, software or hardware that is owned by company and used for business activities. The organizations have to be ensured these assets are accessed by authorized users and they are configured with latest security technologies to protect against security threats and vulnerabilities. The most unauthorized access or effective change during configuration management is being made by unofficial user to system. Therefore, knowing enterprises machines and their location is required to protect system from malicious attacks. Today, organizations use feasible and efficient asset management tools (SAM) to analyze their own data, software and hardware. Anyway, these tools by optimizing and managing IT assets help organization to identify what they have, control cost and risk and improve security. For discovering and monitoring assets and identifying users' roles in our suggested framework, some substeps (Fig. 6) have been proposed.

Classify assets: To implement threat modeling framework is necessary to define assets that can be damaged and need protection. The defined assets should be categorized on the base of their value that is measured by loss of availability, confidentiality and integrity types. Moreover, assets classification allows companies to store and manage their data

by sensitivity and determine risks. For instance, a company has computing resource (memory, storage or CPU), encryption key, applications and customers' personal information that can be classified by different values, damage costs and trust levels. Today, most of organizations are aware of data classification significant. Every enterprise has different assets that have to be managed and classified successfully so can not specify some special and unique assets classifications for all businesses. The below mentioned and discussed assets categorizations are the most important data that by protecting them, each organization meet its final targets.

Private information: By developing social networks, personal data can be exchanged between various enterprises and users for sharing and interacting more experiences. However, private data management is a key to protect data from malicious threats. The most significance threats to offend private information have been shown in Fig. 7. The major challenges and harms for private information are collecting and extracting information by unauthorized access, using fake data for registration and lacking of controls and standards. By deploying private information manager applications more private and confidential data has to be kept secure to help enterprises to meet the acceptable level of confidentiality, integrity and availability.

Financial assets: In recent years, by developing dramatically web service technologies, more and more financial and e-commerce values are shared and accessed by users and enterprises.

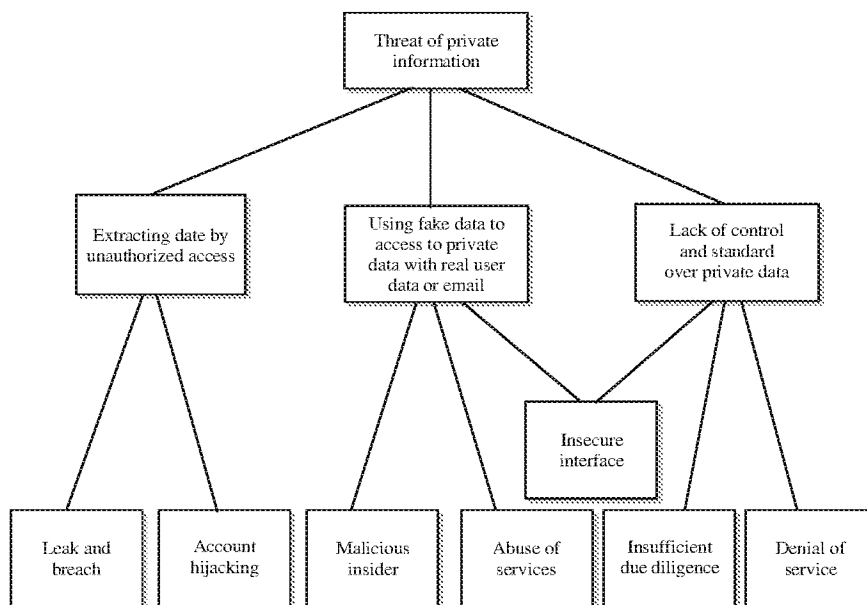


Fig. 7: Significance threats to offend privacy data

Unfortunately, this opportunity becomes the primary target for attackers to access financial assets by deploying cyber threats. For instance, Phishing and DDoS attacks are the major cyber threats that steal user financial assets same as password, bank account detail, credit card number and other confidential enterprises information. However, understanding and analyzing financial assets during threat modeling process allows enterprises to protect data from data stolen through on-line services.

Computing and network assets: This asset is an entity that is capable of creating, sustaining or destroying value at any stage in its life-cycle (Amadi-Echendu, 2004). Analyzing actual network devices or tangible assets (data center, server, desktop computer, router, switch and etc.) and providing security controls is necessary to protect system from malicious insider threats or attacks that are targeted physical assets for terrible damages. The network assets management as an on-demand service allows organization to manage risks and threats, reduce cost and increase the reliability of system.

Application assets: Applications are usually used to store, transfer and process of valuable information. For this reason, enterprises have to be sure about implementing and developing application securely. Application threat modeling by looking application as attacker's view helps enterprises to manage security risks and threats. Each application utilizes different data that allow organization to determine risk and level of expected security. For example an application consists of financial, personal information or users' account numbers. Eventually, analyzing application assets in threat modeling approach can improve security and reduce costs. Human error,

malfunction, spoofing, spamming and malware as the major threats should be detected to protect other assets from malicious attacks.

Establish user's roles: Cloud computing by providing data ubiquity, flexibility of access and relicense, gives opportunity to users for accessing the required service anywhere, anytime and pay per their usage (Ryan, 2013). Each user might assume different roles in various domains, for instance a user might be an administrator with high level privilege in one domain and be a user with low level privilege in another domain. However, establishing the user roles with authentication, authorization and access control mechanisms is necessary for improving data confidentiality, integrity and availability. Nowadays, by progressing online services, organizations same as bank and insurance industry attract huge number of users. For using this excellent opportunity organization have to determine their users' roles to control accesses and improve security. In such enterprises same as bank is impossible to assign users to roles manually so some techniques like as Role Based Access Control (RBAC) assigns organization roles to user, defines privileges and supports security policies (Takabi *et al.*, 2007). Furthermore, domain administrator should assign or remove roles for user or group of users on the base of requested service. For example a developer can be assigned as cloud database developer role to develop and deploy application or he/she can be assigned as a cloud user to implement an application.

By migrating more and more applications and services to the cloud as a centralized data center, CC providers are faced by more access control problems. In fact, cloud computing opportunities same as diversity and dynamicity make

authentication and authorization processes more complex because each cloud user has different access permissions in the same cloud. By the same token, using multiple services on the same cloud by the same user, the authentication and login time increase and also managing more identity process by user make system unsecure. Organization's purpose is managing different roles and assigning them to user to optimize their access control system. Eventually, some access control method same as Cloud Optimized RBAC (coRBAC) (Tianyi *et al.*, 2011) merge distributed authentication services, manage organization role and user in internal network, provide individual authentication service and improve efficiency of access control systems.

Meter usage: Metering and billing are two important issues that should be addressed during threat modeling framework. In computing area storage and network services have to be metered by duration and amount of used. Service Level Agreement (SLA) is a fixed cost or static method that is used as a metering mechanism. Particularly, by developing multi-tenancy and on-demand services, providers have to be used dynamic pay-per-use mechanisms in cloud computing to make bill based on dynamic tariff plan and real-time pricing (Narayan *et al.*, 2012). Furthermore, dynamic metering of cloud services is to prevent wastage of compute resources and improve overall utilization of the cloud infrastructure.

The metering application improves utilization of the infrastructures, cost and management of computing resources by developing dynamic pay-per-use pricing model. These great opportunities are the major interesting factors for organizations to adopt their resources and services to cloud computing. Eventually, attackers are interested to attack system by insufficient due diligence threat and metering and billing vulnerabilities to create the critical issues on security control of cloud computing. Due to the great importance of billing and metering, we proposed to use dynamic mapping pricing and effective billing mechanisms for cloud services based on the current load on the using of cloud infrastructures.

Estimate the trustworthiness: Trust is reliability in distributed systems, among two entities that relay on their credibility to deploy trustworthiness and improve security. Nowadays, trust plays an important role to integrate heterogeneous environments for estimating trustworthiness by confidentiality, integrity, availability, reliability and authenticity (Kallath, 2005). Separating administrative domains, identifying system's vulnerabilities and developing confidence level of trust are required for determining and estimating trust among different distributed systems.

Separating administration domains: Each domain as an administrative boundary collects assets and user roles that share common trust requirements with the same system's expectations. Particularly, different domains have different security levels and different information types so is necessary

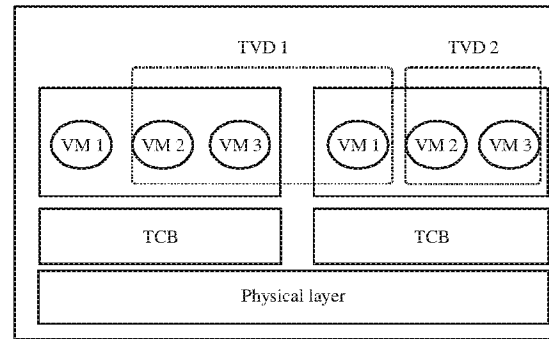


Fig. 8: TVD architecture

to isolate domains for security reason and isolate risks from different domains (Dong *et al.*, 2009). Eventually, the major challenge of security domain is an unauthorized access that prevents other domains to establish a secure relation with harmed domain.

Virtualization as the main feature and crucial technique allows computing duties, run under the virtual environment rather than physical hardware (He and Liang, 2012). Furthermore, leveraging virtualization and trusted computing technologies are required to develop threat modeling framework in distributed multi domains environment. Trusted Virtual Domains (TVD) (Fig. 8) as a coalition of virtual machines that trusted each other provides isolated computing environment, obvious trusted relationships, secure communications and transparent policy enforcement (Lohr *et al.*, 2010). On the other hand, TVDs provides limited boundaries to protect distributed environment over several physical platforms. The Trusted Computing Base (TCB) by responding to present domains trustworthiness, security and TVD policy, guarantees data integrity and confidentiality in execution environment. The most important critical and complex issues that have to be addressed by TVD is satisfying business level of security by simplifying management, improving level of trust and containment.

Establish trust level: Trust level is based on varied and wide necessary trust criteria same as user's roles, offered services, assets, organization structure and technology issues in each virtual domain that offer trustworthiness as a final result. Furthermore, is difficult to understand which trust perspective can be used by domain to asses trust. The trust level in a specific environment or domain always is helpful for manager or director to make their decision. On the other hand, establishing trust between different domains is based on assessment of trust level and balance of trustworthiness among different individual domains (Msanjila and Afsarmanesh, 2007a). However, measuring trustworthiness is complex with single values or metrics so several constraints have to be met to measure trust level of each domain. Nevertheless, this study tried to present the most important elements for modeling trust level in various domains with different trust perspectives.

Users: Different users with different accesses create various trust levels in each domain. For instance, different users same as administrator, authorized users, unregistered users have different trust levels.

Trust perspectives: Each character has a unique trust perspective for deciding on useful information to assess trust level. The organization, social, financial, technology and behavior are the more identified perspectives (Msanjila and Afsarmanesh, 2007b).

Time: Trust level in each virtual domain is dynamic and depending on changes of assessment approaches same as users, assets or other factors. Eventually, time as an important factor should be addressed for modeling trust level in each domain.

Trust level assessment in each domain is the fundamental step for establishing trust relationships among different domains. The main aims of this step is ensuring the acceptable level of trust in each domain, each domain's member conform to the specified trust level, trustworthiness for each object is met and allows trust's experts to more focus on low level trust domain to identify threat and vulnerabilities. For presenting trust level in an understandable format, we can rate trustworthiness in five rating namely Strongly less trustworthy, less trustworthy, average trustworthy, more trustworthy and strongly more trustworthy (Msanjila and Afsarmanesh, 2007b).

Scanning domain security: Scanning of distributed system for management purpose is a complex task by heterogeneity and distribution of resources and tools (Sladic *et al.*, 2011). By developing web services and distributed environments managing and protecting system against vulnerability is a crucial task that seeks out security faults and weaknesses by using different tools same as vulnerability scanning and firewalls. Detecting vulnerability by scanning distributed and virtual environment is used in this research to detect some dangerous gaps and weaknesses before exploiting by threats. Traditional vulnerability control center and several scanning agents in limited area. These models are obsoleted for scanning same as Nessus, X-Scan and agent-based, are using only one functional scanning entity or one scanning domain-based vulnerability scanning. In other words, only one control center handle huge amount of tasks so bottle-neck as the main issue affects system by poor accuracy and time performance (Wang *et al.*, 2013). By developing distributed environment more efficient security management method is required. For this reason, it seems necessary to develop domain-oriented distributed scanning mechanism to satisfy system by high scanning efficiency, simple service providing, flexible deployment and incredible scalability (Chao *et al.*, 2009). In this model, each administration domain has own scanning resources to detect vulnerabilities and all scanning resources

are managed by controlling domain or integrated center. These principles allows huge amount of tasks have to be analyzed without any bottleneck and satisfy load balancing.

Identify threats and vulnerabilities: By developing information and communication technology, organizations are more interested to outsource their computational resources on virtual domains. In fact, this huge amount of data can be damaged by threats from different resources (employees' activities or malicious attacks by attackers). Therefore, management and risk assessment need to understand and analyze threats and vulnerabilities as a crucial security issues. Thus, effective security classification is necessary to identify and organize threats and vulnerabilities into classes based on the intended effect of attacks and develop solutions to prevent system from effective threats (Jouini *et al.*, 2014).

There are several threat classification methods on the base of attack and attacker achievements like unauthorized access.

Threat classification: The classification of threat allows manager to protect system by identify characteristics of threats and select efficient security solution. The most of classification's approaches are based on threat definitions. On the other hand, threats are defined as a technique that is used by attacker to exploit vulnerabilities or impact system. For instance, three dimensional model (Ruf *et al.*, 2003) is represented on the base of attack technique by dividing threats to three subdivisions: motivation, localization and agent (Fig. 9).

- Threat agent is the actor that imposes the threat on specific assets and is divided to human, technological and force majeure
- The threat motivation is sufficient to classify threats to answer the question 'why' a threat is created. Threat motivation is classified into two classes: Deliberate and accidental
- Threat localization represents the origin of threats, internal or external

Hybrid model or information system security threat cube classification model (Geric and Hutinski, 2007) uses classification criteria that are necessary for constantly changing environments (Fig. 10). The three main steps of this model are:

- Security threat frequency shows the frequency of security threat occurrence
- Area of security threat activity shows the main domain that is effected by the threat same as personal, physical, communication and operational security

Security threat source represents the type of threat's resource same as insider and outsiders sources.

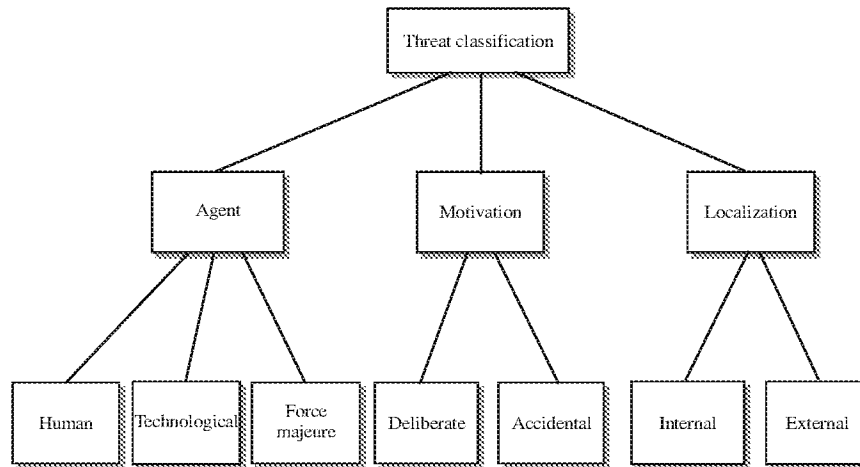


Fig. 9: Three dimension model

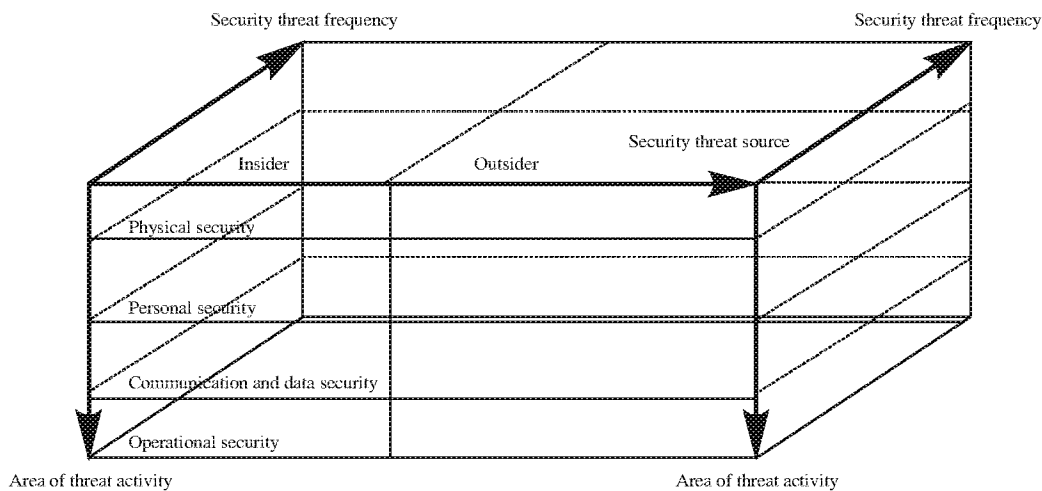


Fig. 10: Threat cube classification model

Information security threats classification pyramid (Alhabeeb *et al.*, 2010) has been presented to classify threats in a dynamic environment and deliberate threats based on three factors:

- Attackers' prior knowledge about system represents the attacker knowledge about system includes system hardware, software, employees and users information
- Critically of the area represents the parts of system that are more critical than other parts of system and they can be affected by threats
- Loss represents any loss that can occur in the system by effecting privacy, integrity, business repudiation and finance loss

The proposed threat classification models are usually limited on use of criteria so, they are sufficient for stable environment where security threats are stable. Nowadays, by developing computing and virtual environments, organizations

are faced by huge dynamic environment that allows different threats to attack system constantly. In this situation, dynamic classification model allows organizations to understand threats and their influence on assets and also realize area which threat could affect.

Multi-dimensions model (Jouini *et al.*, 2014) (Fig. 11) is a hybrid model for information system security threat classification to combine most criteria of threats classifications. In this model threat classification is based on five basic criteria as source, agent, motivation and impact. The first level of classification consists of threat's source. In addition, environmental threat is divided to internal and external threats. The human (insider or hacker), environment (flood, fire, earthquake, wind and etc.) and technological threats (power supplies) are known as a threat agent. Actually, threat agent is the actor that affects system by brings in threat to the system. The next level is threat motivation that is the main goal of attacker to attack system. Particularly, viruses, Trojans and worms are malicious threat that is caused by

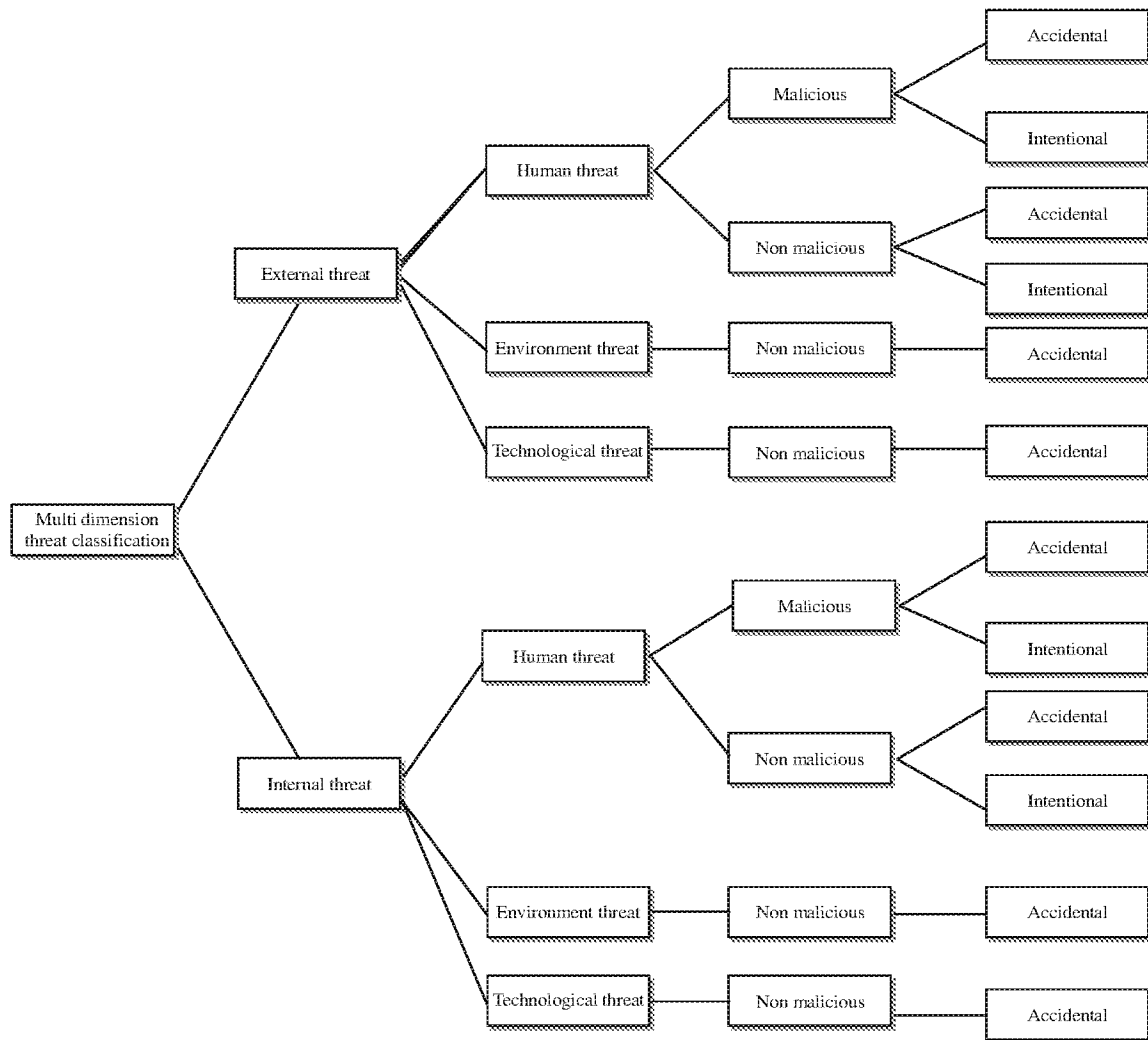


Fig. 11: Multi-dimensions model

attacker for disrupting or harming system. The vulnerabilities and errors are taking place in system because of poor security control or protocols and they are known as a none-malicious attack. The forth level of multi-dimensions model is related to user's intent that who caused the threat. International threat as a harmful decision (damage information deliberately, identity theft, ATM card crime) and accidental threat as a damage without awareness (operator mistake, coding error) are two kinds of this threat. The final part of this threat classification model is impacting threat. Each threat can cause one or many damaging impact to system same as information corruption, data loosing, disclosure of information, denial of use and data destruction.

This threat classification divides threats to different criteria to cover all security risks and allows organization to adopt large scale systems. For moving IT system to the cloud, new classes of threats have to be identified. Some of new available threats are inside trust boundary that should be considered by cloud's tenant and some else are related to cloud provider. Finally, all constraints and security issues propel

managers and providers to design and adopt dynamic and hybrid threat classification model with their system to cover security risk and protect system from exploitation of vulnerabilities by threats.

Vulnerability classification: The main effect of vulnerabilities is incurring high cost for businesses by undermining degree of integrity, confidentiality, safety, availability and reliability. Classification of vulnerability helps businesses to publish, identify and analysis known and unknown vulnerabilities. For this reason, an acceptable and sufficient classification method has to follow below principles (Jin *et al.*, 2009):

- **Public acceptance:** A classification model should be accepted publicly
- **Comprehensibility:** A classification has to be understood by expert and ordinary users
- **Completeness:** A classification should classify most of known and unknown vulnerabilities

Table 2: Relation between threats, vulnerabilities and their counter measure

Threats	Vulnerabilities	Countermeasure
T1	V1, V2, V3, V4, V5, V6	Data Encryption, data signature, DLP as a service
T2	V1, V3, V5, V6	Identity and Access Management (IAM) services (CSA., 2012)
T3	V1,V3,V4	Authentication (Soares <i>et al.</i> , 2013), Access control (Khan, 2012)
T4	V1, V2,V4, V5, V6, V7	Apply security patches, use an IPS for monitoring, configuring firewall, minimize IP spoofing
T5	V2,V5	Cryptography, separation of duties, logging and auditing, legal contracts and insider detection models (Kandias <i>et al.</i> , 2012)
T6	V1, V3, V4, V5	Stop incursions, data protection policies, automating periodic check, security event management, monitoring technologies and authenticate identities
T7	V1, V4, V5	Stricter initial registration, credit card fraud monitoring, black list monitoring (CSA., 2010)
T8	V8	Trusted Third Party (TTP), Rating cloud service provider
T9	V2	Trusted Cloud Computing Platform (TCCP) (Santos <i>et al.</i> , 2009), secure protocol and live migration

- **Determinism:** A classification should have comprehensive process
- **Mutual exclusion:** A classification has to classify vulnerabilities into minimum number of classes
- **Repeatability:** A classification model can be repeatable

Now-a-days, vulnerability is known as a new opportunity for attacker to access and exploit valuable business services. Cloud computing as a multi-tenancy and distributive environment increases substantially the possibility of vulnerability exploitation. In this situation, deploying online classification of vulnerability assists businesses to protect system from reported vulnerabilities. Web Services (WS) as a core cloud technology and XML implementation of Service-Oriented Architecture (SOA) plays an important role to classify and taxonomy vulnerabilities so we should have a closer look at SOA and WS based classification approaches. On the other hand, vulnerabilities those are associated with existing technologies of cloud computing same as SOA, WS and virtualization have significant impact on the cloud. The main goals of vulnerability analysis as avoiding, finding, fixing and monitoring vulnerability leads to vulnerability classification (Lowis and Accorsi, 2009).

Berghe *et al.* (2006) proposed a vulnerability classification model on the base of system components relation and their influence on vulnerabilities. Seacord and Householder (2005) suggested a classification view based on attributes and values to protect system from vulnerability exploitation. Parrend and Frenot (2008) deployed java Service Oriented Programming (SOP) platform to classify vulnerabilities on the base of vulnerability's categorizes and goal of attacks that are based on these vulnerabilities. The ATLIST as a vulnerability analysis method was represented by Lowis and Accorsi (2009) to detect known vulnerabilities rather than new vulnerabilities. However, for categorizing vulnerabilities in cloud computing the three different services of cloud computing as SaaS, PaaS, IaaS (SPI model) have to be considered. On the base of SPI model, insecure interface, unlimited allocation of resources, data related vulnerabilities, virtual machine, SOA and WS are the main impressive vulnerabilities in cloud computing (Hashizume *et al.*, 2013).

Cloud computing as a combination of different technologies is faced by huge amount of threats and vulnerabilities that force organization to consider more complex classification mechanisms than traditional method. Furthermore, traditional web services and virtualization

techniques offer some solutions that are unfledged for computing environment. Nevertheless, numerating cloud's vulnerabilities may not enough and based on existing new threats and security techniques can identify more vulnerability to make system more robust.

Implementing countermeasure: The main goal of countermeasure as an action, device, procedure, technique or other measure, is reducing vulnerability and protecting assets against threats (Laorden *et al.*, 2010). Regardless cloud computing services, data confidentiality, integrity and availability as the main security challenges of cloud computing present the base of countermeasures to protect critical information. On the other hand, each security countermeasure is based on the measured threat, being offered as a service in the cloud. Countermeasure as a service is identified on the base of relationship between threats and vulnerabilities (Table 2).

Determine the result: Estimating and ranking the severity of threats and vulnerabilities to inform decision about what to do to protect system from harmful effects is the last step of proposed model. Having a system to ranking threats and vulnerability is needed to save time and prevent system from more serious security risks. The result of this step can be a list or database of threat and vulnerability profiles that consist of sorted security risks.

Threat ranking: Ranking threats as a complex task is depended on various factors same as existing vulnerabilities, likelihood of attacks and potential impact of attacks. The first step for ranking threats is considering different risk factors that are posed by identified threats. On the base of threat model, various criteria have to be considered as the main exploitation factors of risks. For instance, Microsoft Threat Modeling introduces Damage potential, Reproducibility, Exploitability, Affected users and Discoverability (DREAD) as different influencing agents of a threat (Malik *et al.*, 2008). The equation that is used to compute a risk value has been shown as follows:

$$\text{Risk value} = (D+R+E+A+D)/5$$

The amount of risk value is a number between 0 and 10. It means the higher number is more serious risk. The Open Web Application Security Project (OWASP) as a universal

risk rating system estimates all risks for all organization accurately. This model introduces a rating system to estimate the severity of all security risks on the base of likelihood, impact and combination of them to determine threats as the main factor of security risk. The equation that is used in OWASP is shown as follows:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

In this rule the risk consists of threat agents and their impact on system. The likelihood factor is estimated from a successful attack to exploit vulnerabilities. The amount of likelihood is low, medium or high (0-9). The impact as an effect of successful attack, divided to technical and business. These impacts are related to each other and each one has a set of options with different impact rating from 0-9. In the final stage, impact and likelihood estimations are putting together to calculate the overall accuracy for the risk. The OWASP by defining a dynamic system is more suitable for web services. On the other hand, this model is not based on some predefined threats same in DREAD or Trike. In any case, the customizability and adoptability of this model help businesses to produce result based on their perception about more risky threats.

Vulnerability ranking: Estimating and ranking vulnerability as a complex multi-step mechanism allows businesses to protect system from harsh attacks. The Common Vulnerability Scoring System (CVSS) (Hanford, 2007) is a universal open and standardized method for rating IT vulnerabilities. The CVSS offers evaluation metrics; base metric, temporal metric and environment metric for evaluating security status. Base metric provides original and basic attribute of vulnerabilities, environment metric evaluate vulnerabilities' metrics that are depended on the environment and temporal metric deploys dynamic aspect of vulnerabilities.

Applying CVSS to a business process cannot fully deliver optimal security measure for dynamic environments same as SOA and Web-Services (Zhao *et al.*, 2011). VRank and hybrid ranking have been developed to satisfy business requirements. The VRank (Jiang *et al.*, 2012) as a dynamic framework is able to integrate existing vulnerability databases with the specific detail context of business process. Accordingly, the VRank provides more specific vulnerability assessment for SOA. The hybrid ranking model proposes a combination of CVSS rating and numerical estimation of vulnerability that influence the global network (Zhao *et al.*, 2011). By developing dynamic environments estimating vulnerability in an influential level and aggregating other rating models with high-level rating technics provides a hybrid model to precise measurement of vulnerabilities more economic and efficient.

CONCLUSION

This study reviewed the different existing threat modeling approaches and proposes a dynamic threat modeling method to be adopted by cloud computing. The proposed threat model

allows organization to identify threats and vulnerabilities, justify countermeasures and document the more effected security risks. Unlike other models, proposed dynamic model is not based on some predefine threats. On the other hand, we plan to deploy a novel model to define new threats which are more critical than expected threats in static models. Eventually, in this research we effort to expand a dynamic threat model by respecting cloud essence as a reliability, mobility, scalability and flexibility. By considering the contribution of cloud computing in IT industries, it's obvious that cloud computing is a leading and innovative strategy to attract much attentions. However, developing and designing in-depth security techniques same as threat modeling is needed to satisfy cloud users and providers.

ACKNOWLEDGMENTS

First I would like to thank to my supervisor Dr. Norziana BteJamil for guidance and advances. She inspired and contributed me greatly to work in this study. Beside, I should like to thank the authority of University Tenaga Nasional (UNITEN) for providing good environment and facilities to complete this research. Special thanks to Assoc. Prof. Abdul Rahim Bin Ahmad, for sharing their invaluable assistance. Finally, I would specially thank to my family that support me for completing this study. Without helps of the person that mentioned above, I couldn't be success to publish this paper.

REFERENCES

- Alhabeeb, M., A. Almuhaideb, P.D. Le and B. Srinivasan, 2010. Information security threats classification pyramid. Proceedings of the IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, April 20-23, 2010, Perth, WA., pp: 208-213.
- Amadi-Echendu, J.E., 2004. Managing physical assets is a paradigm shift from maintenance. Proceedings of the IEEE International Engineering Management Conference, Volume 3, October 18-21, 2004, Singapore, pp: 1156-1160.
- Berghe, C.V., J. Riordan and F. Piessens, 2006. A vulnerability tax-onomy methodology applied to web services. Proceedings of the 10th Nordic Workshop on Secure IT Systems, October 20-21, 2005, Tartu, Estonia.
- Bertino, E., L. Martino, F. Paci and A. Squicciarini, 2010. Security for Web Services and Service-Oriented Architectures. Springer, New York, USA., ISBN: 978-3-540-87742-4, Pages: 226.
- CSA., 2010. Top threats to cloud computing V1.0. Cloud Security Alliance (CSA), March, 2010, pp: 1-14. <https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf>
- CSA., 2012. Identity and access management. Cloud Security Alliance (CSA), September 2012, pp: 1-45. https://downloads.cloudsecurityalliance.org/initiatives/secaas/SecaaS_Cat_1_IAM_Implementation_Guidance.pdf

- Chao, D., Y. Danfeng, Y. Yun and Y. Fangchun, 2009. A domain-oriented distributed vulnerability scanning mechanism. Proceedings of the 2nd IEEE International Conference on Broadband Network and Multimedia Technology, October 18-20, 2009, Beijing, China, pp: 831-836.
- Demchenko, Y., C. Ngo, M.X. Makkes, R. Strijkers and C. de Laat, 2012. Defining inter-cloud architecture for interoperability and integration. Proceeding of the 3rd International Conference on Cloud Computing, GRIDs and Virtualization, July 22-27, 2012, Nice, France, pp: 174-180.
- Dong, G., Z. Liu and D. Zhao, 2009. A security domain isolation and data exchange system based on VMM. Proceedings of the 3rd International Conference on Signal Processing and Communication Systems, September 28-30, 2009, Omaha, NE., pp: 1-5.
- Geric, S. and Z. Hutinski, 2007. Information system security threats classifications. *J. Inform. Organiz. Sci.*, 31: 51-61.
- Grobauer, B., T. Walloschek and E. Stocker, 2011. Understanding cloud computing vulnerabilities. *IEEE Secur. Privacy*, 9: 50-57.
- Hamza, Y.A. and M.D. Omar, 2013. Cloud computing security: Abuse and nefarious use of cloud computing. *Int. J. Comput. Eng. Res.*, 3: 22-27.
- Hanford, S., 2007. Common Vulnerability Scoring System (CVSS-SIG): New version of common vulnerability scoring system released. <http://www.first.org/cvss>
- Hashizume, K., D.G. Rosado, E. Fernandez-Medina and E.B. Fernandez, 2013. An analysis of security issues for cloud computing. *J. Internet Services Applic.* 10.1186/1869-0238-4-5
- He, Z. and G. Liang, 2012. Research and evaluation of network virtualization in cloud computing environment. Proceedings of the 3rd International Conference on Networking and Distributed Computing, October 21-24, 2012, Hangzhou, pp: 40-44.
- Jehangir, A. and S.M.H de Groot, 2012. Securing inter-cluster communication in personal networks. Proceedings of the 4th Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, August 6-10, 2007, Philadelphia, PA., pp: 1-6.
- Jiang, J., D. Liping, E. Zhai and Y. Ting, 2012. VRank: A context-aware approach to vulnerability scoring and ranking in SOA. Proceedings of the IEEE 6th International Conference on Software Security and Reliability, June 20-22, 2012, Gaithersburg, MD., USA., pp: 61-70.
- Jin, S., Y. Wang, X. Cui and X. Yun, 2009. A review of classification methods for network vulnerability. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, October 11-14, 2009, San Antonio, pp: 1171-1175.
- Jouini, M., L.B.A. Rabai and A.B. Aissa, 2014. Classification of security threats in information systems. *Procedia Comput. Sci.*, 32: 489-496.
- Kallath, D., 2005. Trust in trusted computing the end of security as we know it. *Comput. Fraud Secur.*, 2005: 4-7.
- Kandias, M., N. Virvilis and D. Gritzalis, 2012. The insider threat in cloud computing. Proceedings of the 6th International Workshop on Critical Information Infrastructure Security, September 8-9, 2011, Switzerland, pp: 99-103.
- Kenyon, H., 2010. Closing an overlooked vulnerability. *Government Computer News*, June 9, 2010, pp: 25-27. https://www.drivesaversdatarecovery.com/images/pdf/GCN+09_06_10.pdf
- Khan, A.R., 2012. Access control in cloud computing environment. *ARN J. Eng. Applied Sci.*, 7: 613-615.
- Laorden, C., B. Sanz, G. Alvarez and P.G. Bringas, 2010. A threat model approach to threats and vulnerabilities in on-line social networks. Proceedings of the 3rd International Conference on Computational Intelligence in Security for Information Systems, November 11-12, 2010, Leon, Spain, pp: 135-142.
- Lohman, T., 2011. DDoS is cloud's security achilles heel. http://www.computerworld.com.au/article/401127/ddos_cloud_security_achilles_heel/
- Lohr, H., T. Poppelmann, J. Rave, M. Steegmanns and M. Winandy, 2010. Trusted virtual domains on OpenSolaris: Usable secure desktop environments. Proceedings of the 5th ACM Workshop on Scalable Trusted Computing, October 4-8, 2010, Chicago, IL., USA., pp: 91-96.
- Lowis, L. and R. Accorsi, 2009. On a classification approach for SOA vulnerabilities. Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, Volume 2, July 20-24, 2009, Seattle, WA., pp: 439-444.
- Malik, N.A., M.Y. Javed and U. Mahmud, 2008. Threat modeling in pervasive computing paradigm. Proceedings of the Mobility and Security, New Technologies, November 5-7, 2008, Tangier, pp: 1-5.
- McRee, R., 2008. PTA: Practical threat analysis. Information Systems Security Association, September 2008, pp: 37-40.
- Msanjila, S.S. and H. Afsarmanesh, 2007a. Modelling trust relationships in collaborative networked organisations. *Technol. Transfer Commer.*, 6: 40-55.
- Msanjila, S.S. and H. Afsarmanesh, 2007b. Towards Establishing Trust Relationships among Organizations in VBES. In: *Establishing the Foundation of Collaborative Networks: IFIP TC 5 Working Group 5.5 Eighth IFIP Working Conference on Virtual Enterprises* September 10-12, 2007, Guimaraes, Portugal, Camarinha-Matos, L.M., H. Afsarmanesh, P. Novais and C. Analide (Eds.). Springer-Verlag, Berlin, Germany, ISBN: 978-0-387-73798-0, pp: 3-14.
- Narayan, A., S. Rao, G. Ranjan and K. Dheenadayalan, 2012. Smart metering of cloud services. Proceedings of the IEEE International Systems Conference, March 19-22, 2012, Vancouver, BC., pp: 1-7.

- Parrend, P. and S. Frenot, 2008. Classification of component vulnerabilities in Java Service Oriented Programming (SOP) platforms. Proceedings of the 11th International Symposium, Component-Based Software Engineering, October 14-17, 2008, Karlsruhe, Germany, pp: 80-96.
- Prasad, N.R., 2007. Threat model framework and methodology for Personal Networks (PNs). Proceedings of the 2nd International Conference on Communication Systems Software and Middleware, January 7-12, 2007, Bangalore, pp: 1-6.
- Rai, P.K. and R.K. Bunkar, 2014. Study of security risk and vulnerabilities of cloud computing. *Int. J. Comput. Sci. Mobile Comput.*, 3: 490-496.
- Rouse, M., 2009. Virtual machine escape. <http://whatis.techtarget.com/definition/virtual-machine-escape>
- Ruf, L., A. Thorn, T. Christen, B. Gruber and R. Portmann, 2003. Threat modeling in security architecture: The nature of threats. https://www.iss.ch/fileadmin/publ/agasa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf
- Ryan, M.D., 2013. Cloud computing security: The scientific challenge and a survey of solutions. *J. Syst. Software*, 86: 2263-2268.
- Santos, N., K.P. Gummadi and R. Rodrigues, 2009. Towards trusted cloud computing. Proceedings of the Conference on Hot Topics in Cloud Computing, June 14-19, 2009, Berkeley, CA, USA.
- Seacord, R.C. and A.D. Householder, 2005. A structured approach to classifying security vulnerabilities. Technical Note CMU/SEI-2005-TN-003, Carnegie Mellon Software Engineering Institute, Pittsburgh, PA., USA., January 2005.
- Sladic, G., M. Vidakovic and Z. Konjovic, 2011. Agent based system for network availability and vulnerability monitoring. Proceedings of the IEEE 9th International Symposium on Intelligent Systems and Informatics, September 8-10, 2011, Subotica, pp: 53-58.
- Soares, L.F.B., D.A.B. Fernandes, M.M. Freire and P.R.M. Inacio, 2013. Secure user authentication in cloud computing management interfaces. Proceedings of the IEEE 32nd International Performance Computing and Communications Conference, December 6-8, 2013, San Diego, CA., USA., pp: 1-2.
- Takabi, H., M. Amini and R. Jalili, 2007. Trust-based user-role assignment in role-based access control. Proceedings of the IEEE/ACS International Conference on Computer Systems and Applications, May 13-16, 2007, Amman, pp: 807-814.
- The Open Group, 2009. Risk Taxonomy. The Open Group, London, UK., ISBN: 1-931624-77-1, Pages: 39.
- Tianyi, Z., L. Weidong and S. Jiaying, 2011. An efficient role based access control system for cloud computing. Proceedings of the 11th IEEE International Conference on Computer and Information Technology, August 31-September-2, 2011, Paphos, Cyprus, pp: 97-102.
- Wang, S., Y. Gong, G. Chen, Q. Sun and F. Yang, 2013. Service vulnerability scanning based on service-oriented architecture in web service environments. *J. Syst. Architecture*, 59: 731-739.
- Zhao, F., H. Huang, H. Jin and Q. Zhang, 2011. A hybrid ranking approach to estimate vulnerability for dynamic attacks. *Comput. Math. Applic.*, 62: 4308-4321.

Electronic Patent Application Fee Transmittal

Application Number:	16228738			
Filing Date:	20-Dec-2018			
Title of Invention:	Threat Model Chaining and Attack Simulation Systems and Related Methods			
First Named Inventor/Applicant Name:	Anurag Agarwal			
Filer:	Paul B. Johnson			
Attorney Docket Number:	ThreatM008			
Filed as Small Entity				
Filing Fees for Utility under 35 USC 111(a)				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	120	120
Total in USD (\$)				120

Electronic Acknowledgement Receipt

EFS ID:	38409807
Application Number:	16228738
International Application Number:	
Confirmation Number:	3702
Title of Invention:	Threat Model Chaining and Attack Simulation Systems and Related Methods
First Named Inventor/Applicant Name:	Anurag Agarwal
Customer Number:	145042
Filer:	Paul B. Johnson
Filer Authorized By:	
Attorney Docket Number:	ThreatM008
Receipt Date:	27-JAN-2020
Filing Date:	20-DEC-2018
Time Stamp:	16:36:14
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	\$ 120
RAM confirmation Number	E20201QG36422347
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

IriusRisk

File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Form (SB08)	IDS4.pdf	1034553	no	4
			5b64f05c6956c185142eb918183131da13b0bd26		
Warnings:					
Information:					
2	Non Patent Literature	NPL08.pdf	134210	no	3
			f5e2ca8cb9f2c6a596108dd199d05dd89779947b		
Warnings:					
Information:					
3	Non Patent Literature	NPL09.pdf	1542821	no	16
			66b4c0c674846a00f8c3fe6646d24d1eee9b19d6		
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30181	no	2
			746f0e22593826df13f3a81cbde391b14a2266f1		
Warnings:					
Information:					
Total Files Size (in bytes):			2741765		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

145042 7590 02/24/2020
Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363

EXAMINER	
SONG, HOSUK	
ART UNIT	PAPER NUMBER
2435	

DATE MAILED: 02/24/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	12/20/2018	Anurag Agarwal	THREATM008	3702

TITLE OF INVENTION: THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	05/26/2020

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

145042 7590 02/24/2020
Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	12/20/2018	Anurag Agarwal	THREATM008	3702

TITLE OF INVENTION: THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$500	\$0.00	\$0.00	\$500	05/26/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
SONG, HOSUK	2435	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,

1 _____

(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government4a. Fees submitted: ☐ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: (Please first reapply any previously paid fee shown above)

☐ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. Change in Entity Status (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29☐ Applicant asserting small entity status. See 37 CFR 1.27☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____

Date _____

Typed or printed name _____

Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	12/20/2018	Anurag Agarwal	THREATM008	3702
145042	7590	02/24/2020	EXAMINER	
Law Office of Paul B. Johnson 8483 S. 1275 E. Sandy, UT 84094-1363			SONG, HOSUK	
			ART UNIT	PAPER NUMBER
			2435	
DATE MAILED: 02/24/2020				

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 16/228,738	Applicant(s) Agarwal, Anurag	
	Examiner HOSUK SONG	Art Unit 2435	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 1/11/2020.
☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1-20. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.

2. ☐ Certified copies of the priority documents have been received in Application No. _____.

3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)	5. ☐ Examiner's Amendment/Comment
2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>1/27/2020;1/1/2020</u> .	6. ☒ Examiner's Statement of Reasons for Allowance
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.	7. ☐ Other _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.	

/HOSUK SONG/ Primary Examiner, Art Unit 2435	
---	--

DETAILED ACTION

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Reasons for Allowance

The following is an examiner's statement of reasons for allowance: Claims 1-20 are allowed.

Claims 1,4: Prior art of record does not teach configuring the diagram interface to display a relational diagram of one of a system, an application, and a process, using visual representations of one or more of the threat model components and visual representations of one or more of the compensating controls, the relational diagram defining a first threat model, and configuring the diagram interface to, in response to receiving one or more inputs, add a component group to the first threat model and thereby redefine the first threat model by including in it a second threat model associated with the component group, wherein the component group comprises a predefined interrelated group of two or more of the threat model components.

Therefore, the pending claims are allowed as the prior art of record does not anticipate each and every limitation recited in the claims; nor would it have been obvious to one of ordinary skill in the art to modify the prior art to include all of the deficient features, as set forth in the allowed claims.

With regard to independent claim 12, while not identical to independent claims 1,4, they are substantively similar to independent claims 1,4 and are therefore allowed under the same rationale.

Claims 2-3, 5-11, and 13-20 are each dependent from one of claims 1, 4, or 12, and are therefore allowed under the same rationale.

USPTO Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HOSUK SONG whose telephone number is (571)272-3857. The examiner can normally be reached on Mon-Fri: 7:30AM-5:00PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at <http://www.uspto.gov/interviewpractice>.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on 571-272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <https://ppair-my.uspto.gov/pair/PrivatePair>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/HOSUK SONG/
Primary Examiner, Art Unit 2435

Issue Classification 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

CPC						
Symbol					Type	Version
G06F	/	21	/	552	F	2013-01-01
G06F	/	16	/	27	I	2019-01-01
G06F	/	21	/	554	I	2013-01-01
G06F	/	21	/	577	I	2013-01-01
G06F	/	30	/	20	I	2020-01-01
G06F	/	2221	/	034	A	2013-01-01

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version
/				

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 20	
/HOSUK SONG/ Primary Examiner, Art Unit 2435 (Primary Examiner) _____ (Date) _____		O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

INTERNATIONAL CLASSIFICATION			
CLAIMED			
H04L	/	29	/ 06

NON-CLAIMED			
/	/		

US ORIGINAL CLASSIFICATION	
CLASS	SUBCLASS
726	25

CROSS REFERENCES(S)						
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	20	
/HOSUK SONG/ Primary Examiner, Art Unit 2435	12 February 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

☐ Claims renumbered in the same order as presented by applicant
 ☐ CPA
 ☒ T.D.
 ☐ R.1.47

CLAIMS															
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	10	10	19	19										
2	2	11	11	20	20										
3	3	12	12												
4	4	13	13												
5	5	14	14												
6	6	15	15												
7	7	16	16												
8	8	17	17												
9	9	18	18												

NONE (Assistant Examiner) _____ (Date) _____		Total Claims Allowed: 20	
/HOSUK SONG/ Primary Examiner, Art Unit 2435 (Primary Examiner) _____ (Date) 12 February 2020		O.G. Print Claim(s) 1	O.G. Print Figure 1

<i>Index of Claims</i> 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS										
☐ Claims renumbered in the same order as presented by applicant					☐ CPA		☒ T.D.		☐ R.1.47	
CLAIM		DATE								
Final	Original	07/31/2019	11/06/2019	02/12/2020						
1	1	✓	✓	=						
2	2	✓	✓	=						
3	3	✓	✓	=						
4	4	✓	✓	=						
5	5	✓	✓	=						
6	6	✓	✓	=						
7	7	✓	✓	=						
8	8	✓	✓	=						
9	9	✓	✓	=						
10	10	✓	✓	=						
11	11	✓	✓	=						
12	12	✓	✓	=						
13	13	✓	✓	=						
14	14	✓	✓	=						
15	15	✓	✓	=						
16	16	✓	✓	=						
17	17	✓	✓	=						
18	18	✓	✓	=						
19	19	✓	✓	=						
20	20	✓	✓	=						

<i>Search Notes</i> 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

CPC - Searched*		
Symbol	Date	Examiner
G06F 21/577; G06F21/552; G06F 21/554; G06FG06F 17/30283; H04L 63/1433; H04L 63/20	07/31/2019	HS
G06F 21/577; G06F21/552; G06F 21/554; G06FG06F 17/30283; H04L 63/1433; H04L 63/20	11/06/2019	HS
G06F 21/577; G06F21/552; G06F 21/554; G06FG06F 17/30283; H04L 63/1433; H04L 63/20	02/12/2020	HS

CPC Combination Sets - Searched*		
Symbol	Date	Examiner

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

--	--

<i>Search Notes</i> 	Application/Control No. 16/228,738	Applicant(s)/Patent Under Reexamination Agarwal, Anurag
	Examiner HOSUK SONG	Art Unit 2435

Search Notes		
Search Notes	Date	Examiner
EAST, foreign patent database, IBM TDB, USPGPUB, inventor name search	07/31/2019	HS
CPC search with keywords	07/31/2019	HS
NPL(IEEE) with keywords	07/31/2019	HS
EAST, foreign patent database, IBM TDB, USPGPUB, inventor name search	11/06/2019	HS
CPC search with keywords	11/06/2019	HS
EAST, foreign patent database, IBM TDB, USPGPUB, inventor name search	02/12/2020	HS
CPC search with keywords	02/12/2020	HS
NPL(IEEE) with keywords	02/12/2020	HS

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
726	22-25	07/31/2019	HS
726	22-25	11/06/2019	HS
726	22-25	02/12/2020	HS

--	--

Access provided by:
United States Patent and
Trademark Office
Sign Out

Browse

My Settings

Get Help

Search within results 🔍

Download PDFs

Per Page: 17 Per Page 25

Export

Alert Set Search Alerts

Search History

Showing 1-25 of 85 for network threat and chaining model ✕

Conferences (62)

Journals (15)

Courses (5)

Magazines (2)

Standards (1)

Filter:

Alert Set Search Alerts

sort: 17 Sort Relevance

Show

All Results

My Subscribed
Content

Open Access

Year

Single Year Range

2002 2002 2019 2019

From To

2002 2019

Author

Affiliation

Publication Title

Publisher

Supplemental Items

Conference Location

Standard Status

Standard Type

Index Terms

Layered defense: modeling terrorist transfer threat networks and optimizing network risk reduction

Eric Taquechel

IEEE Network

Year: 2010 | Volume: 24, Issue: 6 | Magazine Article

Cited by: Papers (3)

Abstract

(2576 Kb)

Layered defense: modeling terrorist transfer threat networks and optimizing network risk reduction

Eric Taquechel

IEEE Network

Year: 2010 | Volume: 24, Issue: 6 | Magazine Article

Feature Design and Selection Based on Web Application-Oriented Active Threat Awareness Model

Wen-Chao Jia ; Rong-Gui Hu ; Fan Shi

2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)

Year: 2016 | Conference Paper

Cited by: Papers (2)

Abstract

(152 Kb)

Feature Design and Selection Based on Web Application-Oriented Active Threat Awareness Model

Wen-Chao Jia | Rong-Gui Hu | Fan Shi

2016 Sixth International Conference on Instrumentation & Measurement, Computer, Communication and Control (IMCCC)

Year: 2016 | Conference Paper

Combating Insider Threats by User Profiling from Activity Logging Data

Mohamed Dahmane ; Samuel Foucher

2018 1st International Conference on Data Intelligence and Security (ICDIS)

Year: 2018 | Conference Paper

Cited by: Papers (1)

Abstract

(155 Kb)

Combating Insider Threats by User Profiling from Activity Logging Data

Mohamed Dahmane | Samuel Foucher

2018 1st International Conference on Data Intelligence and Security (ICDIS)

Year: 2018 | Conference Paper

Standard's Dictionary
Terms

- 0SE
- 0SF
- 0SI
- 1/0
- 1/0 task-structuring criteria
- 1GL
- 2GL
- 3G
- 4GL
- 5GL
- <Viewpoint>

Browse »

- **Performance analysis of network attack based on continuous time Markov Chain in dynamic spectrum access networks**
 Hui Sun ; Xianyu Wang ; Chengjie Wang ; Rui Wang
 2017 9th International Conference on Modelling, Identification and Control (ICMIC)
 Year: 2017 | Conference Paper
 Abstract (540 Kb)

Performance analysis of network attack based on continuous time Markov Chain in dynamic spectrum access networks

Hui Sun | Xianyu Wang | Chengjie Wang | Rui Wang
 2017 9th International Conference on Modelling, Identification and Control (ICMIC)
 Year: 2017 | Conference Paper

- **Security threat probability computation using Markov Chain and Common Vulnerability Scoring System**
 Ngoc T. Le ; Doan B. Hoang
 2018 28th International Telecommunication Networks and Applications Conference (ITNAC)
 Year: 2018 | Conference Paper
 Cited by: Papers (1)
 Abstract (278 Kb)

Security threat probability computation using Markov Chain and Common Vulnerability Scoring System

Ngoc T. Le | Doan B. Hoang
 2018 28th International Telecommunication Networks and Applications Conference (ITNAC)
 Year: 2018 | Conference Paper

- **DroidChain: A novel malware detection method for Android based on behavior chain**
 Zhaoguo Wang ; Chenglong Li ; Yi Guan ; Yibo Xue
 2015 IEEE Conference on Communications and Network Security (CNS)
 Year: 2015 | Conference Paper
 Cited by: Papers (4)
 Abstract (101 Kb)

DroidChain: A novel malware detection method for Android based on behavior chain

Zhaoguo Wang | Chenglong Li | Yi Guan | Yibo Xue
 2015 IEEE Conference on Communications and Network Security (CNS)
 Year: 2015 | Conference Paper

- **Moving Target Defense Against Advanced Persistent Threats for Cybersecurity Enhancement**
 Masoud Khosravi-Farmad ; Ali Ahmadian Ramaki ; Abbas Ghaemi Bafghi
 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE)
 Year: 2018 | Conference Paper
 Abstract (312 Kb)

Moving Target Defense Against Advanced Persistent Threats for Cybersecurity Enhancement

Masoud Khosravi-Farmad | Ali Ahmadian Ramaki | Abbas Ghaemi Bafghi
 2018 8th International Conference on Computer and Knowledge Engineering (ICCKE)
 Year: 2018 | Conference Paper

- **The Dual Ownership Model: Using Organizational Relationships for Access Control in Safety Supply Chains**

Alexander Illic ; Florian Michahelles ; Elgar Fleisch

21st International Conference on Advanced Information Networking and Applications Workshops (AINAW07)

Year: 2007 | Volume: 2 | Conference Paper

Cited by: Papers (3) | Patents (1)

Abstract

(1033 Kb)

The Dual Ownership Model: Using Organizational Relationships for Access Control in Safety Supply Chains

Alexander Illic | Florian Michahelles | Elgar Fleisch

21st International Conference on Advanced Information Networking and Applications Workshops (AINAW07)

Year: 2007 | Volume: 2 | Conference Paper

■ Potential Malicious Insiders Detection Based on a Comprehensive Security Psychological Model

Guang Yang ; Lijun Cai ; Aimin Yu ; Jiangang Ma ; Dan Meng ; Yu Wu

2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)

Year: 2018 | Conference Paper

Abstract

(530 Kb)

Potential Malicious Insiders Detection Based on a Comprehensive Security Psychological Model

Guang Yang | Lijun Cai | Aimin Yu | Jiangang Ma | Dan Meng | Yu Wu

2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService)

Year: 2018 | Conference Paper

■ Pop-up threat models for persistent area denial

Yong Liu ; Jose B. Cruz ; Corey J. Schumacher

IEEE Transactions on Aerospace and Electronic Systems

Year: 2007 | Volume: 43, Issue: 2 | Journal Article

Cited by: Papers (8)

Abstract

(1280 Kb)

Pop-up threat models for persistent area denial

Yong Liu | Jose B. Cruz | Corey J. Schumacher

IEEE Transactions on Aerospace and Electronic Systems

Year: 2007 | Volume: 43, Issue: 2 | Journal Article

■ Robust detection of signaling DDoS threats for more secure machine type communications in next generation mobile networks

Raja Ettiane ; Abdelaali Chaoub ; Rachid Elkouch

2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON)

Year: 2018 | Conference Paper

Abstract

(124 Kb)

Robust detection of signaling DDoS threats for more secure machine type communications in next generation mobile networks

Raja Ettiane | Abdelaali Chaoub | Rachid Elkouch

2018 19th IEEE Mediterranean Electrotechnical Conference (MELECON)

Year: 2018 | Conference Paper

■ Dependability and security models

Kishor S. Trivedi ; Dong Seong Kim ; Arpan Roy ; Deep Medhi

2009 7th International Workshop on Design of Reliable Communication Networks

Year: 2009 | Conference Paper

Cited by: Papers (53)

Abstract

(859 Kb)

Dependability and security models

Kishor S. Trivedi | Dong Seong Kim | Arpan Roy | Deep Medhi
 2009 7th International Workshop on Design of Reliable Communication
 Networks
 Year: 2009 | Conference Paper

■ **Analysis of Coordinated Denial-of-Service Attacks in IEEE 802.22
 Networks**

Yi Tan ; Shamik Sengupta ; K.P. Subbalakshmi
 IEEE Journal on Selected Areas in Communications
 Year: 2011 | Volume: 29, Issue: 4 | Journal Article
 Cited by: Papers (21)

Abstract (848 Kb)

**Analysis of Coordinated Denial-of-Service Attacks in IEEE
 802.22 Networks**

Yi Tan | Shamik Sengupta | K.P. Subbalakshmi
 IEEE Journal on Selected Areas in Communications
 Year: 2011 | Volume: 29, Issue: 4 | Journal Article

■ **Network Security Risk Assessment Using Bayesian Belief Networks**

Suleyman Kondakci
 2010 IEEE Second International Conference on Social Computing
 Year: 2010 | Conference Paper
 Cited by: Papers (12)

Abstract (299 Kb)

**Network Security Risk Assessment Using Bayesian Belief
 Networks**

Suleyman Kondakci
 2010 IEEE Second International Conference on Social Computing
 Year: 2010 | Conference Paper

■ **Conceptual Model of Risk Assessment for Insider Threats Detection**

Z. Zainal Abidin ; Z. Abal Abas ; N. A. Zakaria ; N. A. Hashim ; E. Mardaid ;
 R. Ahmad ; A. P. Puvanasvaran
 2019 1st International Conference on Electrical, Control and Instrumentation
 Engineering (ICECIE)
 Year: 2019 | Conference Paper

Abstract (2874 Kb)

**Conceptual Model of Risk Assessment for Insider Threats
 Detection**

Z. Zainal Abidin | Z. Abal Abas | N. A. Zakaria | N. A. Hashim | E. Mardaid | R.
 Ahmad | A. P. Puvanasvaran
 2019 1st International Conference on Electrical, Control and Instrumentation
 Engineering (ICECIE)
 Year: 2019 | Conference Paper

■ **Research on security evaluation of cloud computing based on attack
 graph**

Yexia Cheng ; Yuejin Du ; Junfeng Xu ; Chunyang Yuan ; Zhi Xue
 2012 IEEE 2nd International Conference on Cloud Computing and
 Intelligence Systems
 Year: 2012 | Volume: 01 | Conference Paper
 Cited by: Papers (2)

Abstract (145 Kb)

**Research on security evaluation of cloud computing based on
 attack graph**

Yexia Cheng | Yuejin Du | Junfeng Xu | Chunyang Yuan | Zhi Xue

2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems

Year: 2012 | Volume: 01 | Conference Paper

■ **Diagnostics and assessment of the industrial network security expert system**

Polina Repp

2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)

Year: 2017 | Conference Paper

Cited by: Papers (1)

Abstract

(555 Kb)

Diagnostics and assessment of the industrial network security expert system

Polina Repp

2017 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)

Year: 2017 | Conference Paper

■ **The Impacts of Carbon Tariff on Green Supply Chain Design**

Yuan Zhou ; Dah-Chuan Gong ; Boray Huang ; Brett A. Peters

IEEE Transactions on Automation Science and Engineering

Year: 2017 | Volume: 14, Issue: 3 | Journal Article

Cited by: Papers (4)

Abstract

(1920 Kb)

The Impacts of Carbon Tariff on Green Supply Chain Design

Yuan Zhou | Dah-Chuan Gong | Boray Huang | Brett A. Peters

IEEE Transactions on Automation Science and Engineering

Year: 2017 | Volume: 14, Issue: 3 | Journal Article

■ **Detecting IoT Malware by Markov Chain Behavioral Models**

Massimo Ficco

2019 IEEE International Conference on Cloud Engineering (IC2E)

Year: 2019 | Conference Paper

Abstract

(4011 Kb)

Detecting IoT Malware by Markov Chain Behavioral Models

Massimo Ficco

2019 IEEE International Conference on Cloud Engineering (IC2E)

Year: 2019 | Conference Paper

■ **Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability**

Xiaoguang Wei ; Shibin Gao ; Tao Huang ; Ettore Bompard ; Renjian Pi ; Tao Wang

IEEE Transactions on Industrial Informatics

Year: 2019 | Volume: 15, Issue: 3 | Journal Article

Cited by: Papers (5)

Abstract

(2484 Kb)

Complex Network-Based Cascading Faults Graph for the Analysis of Transmission Network Vulnerability

Xiaoguang Wei | Shibin Gao | Tao Huang | Ettore Bompard | Renjian Pi | Tao Wang

IEEE Transactions on Industrial Informatics

Year: 2019 | Volume: 15, Issue: 3 | Journal Article

■ **A Theoretical Model for Analysis of Firewalls Under Bursty Traffic Flows**

Yahya Shahsavari ; Hadishahriar Shahhoseini ; Kaiwen Zhang ; Halima Elbiaze

IEEE Access

Year: 2019 | Volume: 7 | Journal Article

Abstract (5942 Kb)

A Theoretical Model for Analysis of Firewalls Under Bursty Traffic Flows

Yahya Shahsavari | Hadishahriar Shahhoseini | Kaiwen Zhang | Halima Elbiaze

IEEE Access

Year: 2019 | Volume: 7 | Journal Article

BEAMS: Battery Exhaustion Anomaly Monitoring System model in SENSORNET

Tapalina Bhattachali ; Rituparna Chaki

2012 Sixth International Conference on Sensing Technology (ICST)

Year: 2012 | Conference Paper

Abstract (276 Kb)

BEAMS: Battery Exhaustion Anomaly Monitoring System model in SENSORNET

Tapalina Bhattachali | Rituparna Chaki

2012 Sixth International Conference on Sensing Technology (ICST)

Year: 2012 | Conference Paper

A Dynamic Mutual RFID Authentication Model Preventing Unauthorized Third Party Access

Matthieu-P. Schapranow ; Alexander Zeier ; Hasso Plattner

2010 Fourth International Conference on Network and System Security

Year: 2010 | Conference Paper

Cited by: Papers (8) | Patents (1)

Abstract (677 Kb)

A Dynamic Mutual RFID Authentication Model Preventing Unauthorized Third Party Access

Matthieu-P. Schapranow | Alexander Zeier | Hasso Plattner

2010 Fourth International Conference on Network and System Security

Year: 2010 | Conference Paper

VASA: Interactive Computational Steering of Large Asynchronous Simulation Pipelines for Societal Infrastructure

Sungahn Ko ; Jieqiong Zhao ; Jing Xia ; Shehzad Afzal ; Xiaoyu Wang ; Greg

Abram ; Niklas Elmquist ; Len Kne ; David Van Riper ; Kelly Gaither ; Shaun

Kennedy ; William Tolone ; William Ribarsky ; David S. Ebert

IEEE Transactions on Visualization and Computer Graphics

Year: 2014 | Volume: 20, Issue: 12 | Journal Article

Cited by: Papers (6)

Abstract (1242 Kb) Media

VASA: Interactive Computational Steering of Large Asynchronous Simulation Pipelines for Societal Infrastructure

Sungahn Ko | Jieqiong Zhao | Jing Xia | Shehzad Afzal | Xiaoyu Wang | Greg

Abram | Niklas Elmquist | Len Kne | David Van Riper | Kelly Gaither | Shaun

Kennedy | William Tolone | William Ribarsky | David S. Ebert

IEEE Transactions on Visualization and Computer Graphics

Year: 2014 | Volume: 20, Issue: 12 | Journal Article

Supply network protection under capacity constraint

Naji Bricha ; Mustapha Noureldath

Proceedings of 2013 International Conference on Industrial Engineering and Systems Management (IESM)

Year: 2013 | Conference Paper

Abstract (802 Kb)

Supply network protection under capacity constraint

Naji Bricha | Mustapha Noureldath

Proceedings of 2013 International Conference on Industrial Engineering and Systems Management (IESM)

Year: 2013 | Conference Paper

Load More

IEEE Personal Account	Purchase Details	Profile Information	Need Help?	Follow
CHANGE USERNAME/PASSWORD	PAYMENT OPTIONS	COMMUNICATIONS PREFERENCES	US & CANADA: +1 800 678 4333	f in t
	VIEW PURCHASED DOCUMENTS	PROFESSION AND EDUCATION	WORLDWIDE: +1 732 981 0060	
		TECHNICAL INTERESTS	CONTACT & SUPPORT	

About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions

IEEE Account	Purchase Details	Profile Information	Need Help?
» Change Username/Password	» Payment Options	» Communications Preferences	» US & Canada: +1 800 678 4333
» Update Address	» Order History	» Profession and Education	» Worldwide: +1 732 981 0060
	» View Purchased Documents	» Technical Interests	» Contact & Support

About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S171	1	("20010027388").PN.	US-PGPUB; USPAT	OR	OFF	2020/02/12 13:00
S172	10	("10262132" "20110277034" "20140157417" "20150033346" "20160162690" "20160248798" "20170213037" "20180255084" "7260844" "7624448").PN.	US-PGPUB; USPAT	OR	OFF	2020/02/12 13:00
S173	600	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:13
S174	77622	(G06F21/577 OR G06F21/552 OR G06F21/554 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:13
S175	1	("agarwal, anurag").INV. and 726/\$.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:22
S176	6	(threats and database and diagram\$5 and model and control\$4 and (visual or display\$4)).CLM.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:22
S177	3131	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:25
S178	272	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:26
S179	20	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/22.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:27
S180	49	(threat\$4 or attack\$4 or vulnerabilit\$4)	US-PGPUB;	OR	ON	2020/02/12

		near5 (model or graph or display\$4) near5 (database or storage or record) and 726/23.ccls.	USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB			14:35
S181	15	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/24.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:35
S182	79	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near5 (database or storage or record) and 726/25.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:36
S183	261	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record)	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:37
S184	172	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:37
S185	181	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:38
S186	150	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:39
S187	7	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and 726/22.ccls.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:41
S191	150	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or diagram\$4) near4 (second or multiple or pluralit\$5) same (database or storage or record) and (collect\$4 or gather\$4 or organiz\$) near5 (data or information or packets) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:51

S192	310	(threat\$4 or attack\$4 or vulnerabilit\$4) near5 (model or graph or display\$4 or tree) near5 (database or storage or record or file) and (G06F21/577 OR H04L63/1433 OR H04L63/20 OR G06F17/30283).CPC.	US-PGPUB; OR USPAT; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2020/02/12 14:59
------	-----	--	---	----	----	---------------------

2/ 13/ 2020 1:14:27 PM
C:\ Users\ hsong\ Documents\ EAST\ Workspaces\ 16228738.wsp

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

U.S.PATENTS

[Remove](#)

Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/H.S./	1	10262132	B2	2019-04-16	Reinecke et al.	
/H.S./	2	7624448	B2	2009-11-24	Coffman	
/H.S./	3	7260844	B1	2007-08-21	Tidwell et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

[Add](#)

U.S.PATENT APPLICATION PUBLICATIONS

[Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/H.S./	1	20160162690	A1	2016-06-09	Reith et al.	
/H.S./	2	20170213037	A1	2017-07-27	Toledano et al.	
/H.S./	3	20180255084	A1	2018-09-06	Kotinas et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

/H.S./	4	20150033346	A1	2015-01-29	Hebert et al.
/H.S./	5	20140157417	A1	2014-06-05	Grubel et al.
/H.S./	6	20110277034	A1	2011-11-10	Hanson
/H.S./	7	20160248798	A1	2016-08-25	Cabrera et al.

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS

[Remove](#)

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button. [Add](#)

NON-PATENT LITERATURE DOCUMENTS

[Remove](#)

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		

If you wish to add additional non-patent literature document citation information please click the Add button. [Add](#)

EXAMINER SIGNATURE

Examiner Signature	/HOSUK SONG/	Date Considered	02/12/2020
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Paul B. Johnson/	Date (YYYY-MM-DD)	2020-01-01
Name/Print	Paul B. Johnson	Registration Number	59375

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16228738
	Filing Date	2018-12-20
	First Named Inventor	Anurag Agarwal
	Art Unit	2435
	Examiner Name	Hosuk Song
	Attorney Docket Number	ThreatM008

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/H.S./	1	20010027388	A1	2001-10-04	Beverina et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS							Remove	
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²ⁱ	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button

Add

NON-PATENT LITERATURE DOCUMENTS			Remove
Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

/H.S./	1	Roy, Maurer. "Top Database Security Threats and How to Mitigate Them." July 30, 2015. Retrieved from "https://www.shrm.org/resouresandtools/hr-topics/risk-management/pages/top-database-security-threats.aspx" (Year: 2015).
/H.S./	2	A. Amini, N. Jamil, A.R. Ahmad and M.R. Z'aba, 2015. Threat Modeling Approaches for Securing Cloud Computing. Journal of Applied Sciences, 15: 953-967. Retrieved from "https://scialert.net/fulltextmobile/?doi=jas.2015.953.967" (Year: 2015).

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/HOSUK SONG/	Date Considered	02/12/2020
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Hosuk Song
Attorney Docket Number	ThreatM008

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

☒ The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Paul B. Johnson/	Date (YYYY-MM-DD)	2020-01-27
Name/Print	Paul B. Johnson	Registration Number	59375

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

Feb 24, 2020 03:39:16 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	NOA	02/24/2020	THREATM008
	1449	02/24/2020	THREATM008
	1449	02/24/2020	THREATM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://sportal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

CORRESPONDENCE

Applicant: ThreatModeler Software Inc.

Docket No: THREATM008

Examiner: Song, Hosuk

Ser. No: 16228738

Filed: December 20, 2018

Group Art Unit: 2435

Title: Threat Model Chaining and Attack Simulation Systems and Related Methods

COMMENTS ON STATEMENT OF REASONS FOR ALLOWANCE

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner:

The following is responsive to the Notice of Allowance mailed Feb. 24, 2020. Comments on the Examiner's stated reasons for allowance are given in the following section.

Remarks begin on page 2 of this paper.

REMARKS

Claims 1-20 have been allowed in the application. Applicant wishes to thank the Examiner for confirmation of the patentable subject matter of these claims.

Comments on Examiner's Reasons for Allowance

The Applicant hereby acknowledges the Examiner's Reasons for Allowance in the Notice of Allowance referenced above. The Applicant respectfully notes that there may be additional reasons for allowance that have not been specifically cited, and which may apply to various of the allowed claims, in addition to or instead of the cited Reasons. Applicant respectfully suggests that notwithstanding the Examiner's Reasons for Allowance, it is believed that each of the allowed claims is patentable in its own right and/or for other reasons raised during the prosecution and/or explained in the specification of this application. To the extent that any statements regarding patentability of any claim(s) allowed by the Examiner made by the Applicant or the Examiner in any document filed in this application are inconsistent with or not included in the Examiner's Reasons for Allowance, they are incorporated by reference herein.

Respectfully submitted,

Date: March 2, 2020

By: /Paul B. Johnson/

Paul B. Johnson

Reg. No. 59375

Law Office of Paul B. Johnson

8483 S 1275 E

Sandy, UT 84094-1363

Ph: 801.719.5229

Fax: 801.317.8889

paul@pauljohnsonlaw.com

Electronic Acknowledgement Receipt

EFS ID:	38747811
Application Number:	16228738
International Application Number:	
Confirmation Number:	3702
Title of Invention:	THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS
First Named Inventor/Applicant Name:	Anurag Agarwal
Customer Number:	145042
Filer:	Paul B. Johnson
Filer Authorized By:	
Attorney Docket Number:	THREATM008
Receipt Date:	02-MAR-2020
Filing Date:	20-DEC-2018
Time Stamp:	20:31:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	PATCommentsOnReasonsForAllowance.pdf	52635 05426da39c3b56e00849ba0b690ec81f94d3455	no	2

Warnings:

IriusRisk

Information:	
Total Files Size (in bytes):	52635
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>	

PRINTER RUSH
(PTO ASSISTANCE)

Application: 16228738

Examiner: Song

GAU: 2435

From:

Location: IDC

Creation Date: 04/16/2020

Week Date: 2/17/2020

<u>DOC CODE</u>	<u>DOC DATE</u>	<u>MISCELLANEOUS</u>
<div style="display: flex; align-items: center; margin-bottom: 5px;">☐ 1449</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☒ IDS</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ CLM</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ IIFW/FWCLM</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ SRFW</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ DRW</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ OATH</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ 312</div> <div style="display: flex; align-items: center;">☐ SPEC</div>	<p style="margin: 0;"><u>11/25/2019</u></p>	<div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Continuing Data</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Foreign Priority</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Document Legibility</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Fees</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Petition (TC)</div> <div style="display: flex; align-items: center;">☐ Other</div>

[RUSH] Message:

Please initial/line through citations on IDS 11/25/19.
Thank you.

[XRUSH] Response:

Initials: _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	12/20/2018	Anurag Agarwal	THREATM008	3702
145042	7590	04/22/2020	EXAMINER	
Law Office of Paul B. Johnson			SONG, HOSUK	
8483 S. 1275 E.				
Sandy, UT 84094-1363				
			ART UNIT	PAPER NUMBER
			2435	
			NOTIFICATION DATE	DELIVERY MODE
			04/22/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

paul@pauljohnsonlaw.com

Corrected Notice of Allowability	Application No. 16/228,738	Applicant(s) Agarwal, Anurag	
	Examiner HOSUK SONG	Art Unit 2435	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--
 All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to _____.
 ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☒ The allowed claim(s) is/are 1-20. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:
 a) ☐ All b) ☐ Some *c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892) 2. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date <u>11/25/2019</u> . 3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____. 4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.	5. ☐ Examiner's Amendment/Comment 6. ☐ Examiner's Statement of Reasons for Allowance 7. ☐ Other _____.
---	---

/HOSUK SONG/
 Primary Examiner, Art Unit 2435

PRINTER RUSH
(PTO ASSISTANCE)

Application: 16228738

Examiner: Song

GAU: 2435

From:

Location: IDC

Creation Date: 04/16/2020

Week Date: 2/17/2020

<u>DOC CODE</u>	<u>DOC DATE</u>	<u>MISCELLANEOUS</u>
<div style="display: flex; align-items: center; margin-bottom: 5px;">☐ 1449</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☒ IDS</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ CLM</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ IIFW/FWCLM</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ SRFW</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ DRW</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ OATH</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ 312</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ SPEC</div>	<p style="margin: 0;"><u>11/25/2019</u></p>	<div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Continuing Data</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Foreign Priority</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Document Legibility</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Fees</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Petition (TC)</div> <div style="display: flex; align-items: center; margin-bottom: 5px;">☐ Other</div>

[RUSH] Message:

Please initial/line through citations on IDS 11/25/19.
Thank you.

[XRUSH] Response:

Done
Thank you

Initials: /H.S./

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	16228738
	Filing Date	2018-12-20
	First Named Inventor	Anurag Agarwal
	Art Unit	2435
	Examiner Name	Song, Hosuk
	Attorney Docket Number	ThreatM008

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
/H.S/	1	20170213037	A1	2017-07-27	Toledano et al.	
/H.S/	2	20180255084	A1	2018-09-06	Kotinas et al.	
/H.S/	3	20150033346	A1	2015-01-29	Hebert et al.	
/H.S/	4	20140157417	A1	2014-06-05	Grubel et al.	
/H.S/	5	20110277034	A1	2011-11-10	Hanson	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Song, Hosuk
Attorney Docket Number	ThreatM008

/H.S./	6	20160248798	A1	2016-08-25	Cabrera et al.
--------	---	-------------	----	------------	----------------

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ²	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		

If you wish to add additional non-patent literature document citation information please click the Add button.

EXAMINER SIGNATURE

Examiner Signature	/HOSUK SONG/	Date Considered	11/26/2019
--------------------	--------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	16228738
Filing Date	2018-12-20
First Named Inventor	Anurag Agarwal
Art Unit	2435
Examiner Name	Song, Hosuk
Attorney Docket Number	ThreatM008

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☒ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Paul B. Johnson/	Date (YYYY-MM-DD)	2019-11-25
Name/Print	Paul B. Johnson	Registration Number	59375

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

Apr 22, 2020 03:58:14 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	NOA	04/22/2020	THREATM008
	1449	04/22/2020	THREATM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ISSUE FEE TRANSMITTAL FORM

APPLICATION #
16228738

FILING DATE
12/20/2018

FIRST NAMED INVENTOR
Anurag Agarwal

ATTORNEY DOCKET #
THREATM008

Title of Invention

THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

Application Information

APPLICATION TYPE Nonprovisional Application under 35
USC 111(a)

DATE DUE 05/26/2020

CONFIRMATION # 3702

ISSUE FEE DUE \$ 500

EXAMINER HOSUK SONG

PUBLICATION DUE \$ 0

GROUP ART UNIT 2435

TOTAL FEES DUE \$500

CLASS - SUBCLASS 726/025000

PREV. PAID FEE \$ 0

ENTITY STATUS Small

1. CHANGE OF CORRESPONDENCE ADDRESS AND/OR INDICATION OF FEE ADDRESS (37 CFR 1.33 & 1.363)

Correspondence Address

Maintenance Fee Address

CURRENT ADDRESS

CURRENT ADDRESS



Change of correspondence address requested, system
generated AIA/122-PC form attached



Fee address indication requested, system
generated SB/47-PC form attached

2. ENTITY STATUS

Change in Entity Status

NEW STATUS

3. THE FOLLOWING FEES ARE SUBMITTED



Issue Fee



Publication Fee



Advance Order - # of copies:

4. FEE AUTHORIZATION



I authorize USPTO to apply my previously paid issue fee to the current fees due



The Director is hereby authorized to apply my previously paid issue fee to the current fee due and to charge deficient fees to Deposit Account Number:



If in addition to the payment of the issue fee amount submitted with this form, there are any discrepancies in any amount(s) due, the Director is authorized to charge any deficiency, or credit any overpayment, to Deposit Account Number:

5. FIRM AND/OR ATTORNEY NAMES TO BE PRINTED

NOTE: If no name is listed, no name will be printed

For printing on the patent front page, list to be displayed as entered

Law Office of Paul B. Johnson
Paul B. Johnson

6. ASSIGNEE NAME(S) AND RESIDENCE DATA TO BE PRINTED

NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

ThreatModeler Software Inc.

Jersey City, NJ UNITED STATES

Organization

Signature

I certify, in accordance with 37 CFR 1.4(d)(4) that I am an attorney or agent registered to practice before the Patent and Trademark Office who has filed and has been granted power of attorney in this application. I also

certify that this Fee(s) Transmittal form is being transmitted to the USPTO via Patent Center on the date indicated below.

Signature	Name	Registration #	Date
/Paul B. Johnson/	Paul Johnson	59375	05/25/2020



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #
16/228,738

RECEIPT DATE / TIME
05/25/2020 09:23:31 PM ET

ATTORNEY DOCKET #
THREATM008

Title of Invention

THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

Application Information

APPLICATION TYPE Utility - Nonprovisional Application
under 35 USC 111(a)

PATENT # -

CONFIRMATION # 3702

FILED BY Paul Johnson

PATENT CENTER # 60027554

AUTHORIZED BY -

CUSTOMER # 145042

FILING DATE 12/20/2018

CORRESPONDENCE ADDRESS -

FIRST NAMED INVENTOR Anurag Agarwal

Payment Information

PAYMENT METHOD
CARD / 6354

PAYMENT TRANSACTION ID
E20205QL23514400

PAYMENT AUTHORIZED BY
Paul Johnson

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2501	UTILITY ISSUE FEE	500.00	1	500.00
TOTAL AMOUNT:				\$500.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage

IriusRisk

Ex. 1002 - Page 572

submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
16/228,738

RECEIPT DATE / TIME
05/25/2020 09:23:31 PM ET

ATTORNEY DOCKET #
THREATM008

Title of Invention

THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

Application Information

APPLICATION TYPE Utility - Nonprovisional Application
under 35 USC 111(a)

PATENT # -

CONFIRMATION # 3702

FILED BY Paul Johnson

PATENT CENTER # 60027554

FILING DATE 12/20/2018

CUSTOMER # 145042

FIRST NAMED
INVENTOR Anurag Agarwal

CORRESPONDENCE
ADDRESS -

AUTHORIZED BY -

Documents

TOTAL DOCUMENTS: 1

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
web85b.pdf	3	Issue Fee Payment (PTO-85B)	62 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
web85b.pdf	7E421A853BA6119F733B8D9528EA3AD2D8F5BC8A096D3AB12 FA61C2E9FCFAAB4D185C3C3F1EC1FF362B2C5A81B9FB863D EA75896F0D247FF3F4CA50052BB25C4

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as

IriusRisk

Ex. 1002 - Page 574

described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	06/30/2020	10699008	THREATM008	3702

145042 7590 06/10/2020

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Anurag Agarwal, Jersey City, NJ;
ThreatModeler Software Inc., Jersey City, NJ;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

Jun 11, 2020 03:57:51 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	ISSUE.NTF	06/10/2020	THREATM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM



ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
16/228,738

RECEIPT DATE / TIME
07/06/2020 10:36:25 PM ET

ATTORNEY DOCKET #
THREATM008

Title of Invention

THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

Application Information

APPLICATION TYPE Utility - Nonprovisional Application
under 35 USC 111(a)

PATENT # 10699008

CONFIRMATION # 3702

FILED BY Paul Johnson

PATENT CENTER # 60049389

FILING DATE 12/20/2018

CUSTOMER # 145042

FIRST NAMED
INVENTOR Anurag Agarwal

CORRESPONDENCE
ADDRESS -

AUTHORIZED BY -

Documents

TOTAL DOCUMENTS: 3

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
sb0044-1.pdf	1	Request for Certificate of Correction	126 KB
sb0044-2.pdf	1	Request for Certificate of Correction	130 KB
CertOfCorrectionRequestLtr.pdf	2	Miscellaneous Incoming Letter	119 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
----------	-------------------------

sb0044-1.pdf	FE4147C4C79F5850FBE120A1AF93BFCA067006E2AF4710114F 40C402930592BB7D991B6DC4B11A97E9F85DF5DAC35F7DB8 EC8B94D4ADB2D565704AD0F3220F2B
--------------	--

sb0044-2.pdf	61317F10C4B997C68867275ACFF7F7DB1B639DD3F31851A30 E80A0E7A1B1118289812D57E3DC8FCD9ADBD2DD4250406963 353C17DC7C5D54D1469C5780051F8A
--------------	--

CertOfCorrectionRequestLtr.pdf	20F7F086F6BC0C3F16FBDC4E82F4C0748B033E76243AF99DE 37330D771379933D45E2D64E703AC5D4C684C049DAABB746C DB33A2089728BACFEA1A290F89335A
--------------------------------	--

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

**UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION**Page 2 of 2

PATENT NO. : 10699008

APPLICATION NO.: 16228738

ISSUE DATE : June 30, 2020

INVENTOR(S) : Anurag Agarwal

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the specification:

Column 23, Line 62, change "some sub-component" to -a sub-component-.

Column 23, Line 63, change "some element" to -an element-.

Column 27, Line 1, change "analyze" to -analyzing-.

Column 27, Line 3, change "analyze" to -analyzing-.

Column 27, Lines 4-5, change "measure and quantify" to -measuring and quantifying-.

Column 33, Line 50, change "functionality" to -the web page having functionality-.

Column 34, Line 33, change "is" to -includes-.

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):

Law Office of Paul B. Johnson
8483 S 1275 E, Sandy, UT 84094

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



ELECTRONIC PAYMENT RECEIPT

APPLICATION #
16/228,738

RECEIPT DATE / TIME
07/06/2020 10:36:25 PM ET

ATTORNEY DOCKET #
THREATM008

Title of Invention

THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

Application Information

APPLICATION TYPE Utility - Nonprovisional Application
under 35 USC 111(a)

PATENT # 10699008

CONFIRMATION # 3702

FILED BY Paul Johnson

PATENT CENTER # 60049389

AUTHORIZED BY -

CUSTOMER # 145042

FILING DATE 12/20/2018

CORRESPONDENCE
ADDRESS -

FIRST NAMED
INVENTOR Anurag Agarwal

Payment Information

PAYMENT METHOD
CARD / 6354

PAYMENT TRANSACTION ID
E202076M37148944

PAYMENT AUTHORIZED BY
Paul Johnson

FEE CODE	DESCRIPTION	ITEM PRICE(\$)	QUANTITY	ITEM TOTAL(\$)
2811	CERTIFICATE OF CORRECTION	150.00	1	150.00
TOTAL AMOUNT:				\$150.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE CERTIFICATE OF CORRECTION

Page 1 of 2

PATENT NO. : 10699008
APPLICATION NO.: 16228738
ISSUE DATE : June 30, 2020
INVENTOR(S) : Anurag Agarwal

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the drawings:

In FIG. 10, the rightmost line connecting the "AKAMAI DNS" component with the "FIRE WALL" component should have the end arrow pointing at the "FIRE WALL" component.
In FIG. 21, the rightmost line connecting the "AKAMAI DNS" component with the "FIRE WALL" component should have the end arrow pointing at the "FIRE WALL" component.
In FIG. 22, the rightmost line connecting the "AKAMAI DNS" component with the "FIRE WALL" component should have the end arrow pointing at the "FIRE WALL" component.

In the abstract:

In the Abstract, Line 2, change "including a threat model components" to -including threat model components-.
In the Abstract, Line 5, change "associate with" to -associated with-.
In the Abstract, Line 9, change "model include" to -model and include-.

In the specification:

Column 5, Line 55, change "compensated" to -compensating-.
Column 6, Line 30, change "compensatory" to -compensating-.
Column 15, Line 4, change "showing" to -shows-.
Column 16, Line 36, change "a cloud computing" to -cloud computing-.
Column 17, Line 35, change "popup threat" to -popup threat report-.
Column 18, Lines 2-3, change "a similar" to -an-.
Column 18, Line 3, change "to the" to -similar to the-.
Column 18, Line 39, change "list" to -lists-.
Column 20, Line 6, change "the component" to -component-.
Column 20, Line 12, change "ID a version" to -a CPE ID indicating a version-.
Column 23, Line 19, change "to" to -to/from-.

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):

Law Office of Paul B. Johnson
8483 S 1275 E, Sandy, UT 84094

This collection of information is required by 37 CFR 1.322, 1.323, and 1.324. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1.0 hour to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Attention Certificate of Corrections Branch, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



Paul B. Johnson
Registered Patent Attorney
paul@pauljohnsonlaw.com

July 6, 2020

Commissioner for Patents
Office of Data Management Attention: Certificates of Correction Branch
P.O. Box 1450
Alexandria, VA 22313-1450

Certificate of Correction Request

Patent Number: 10699008
Application Number: 16228738
Inventor: Anurag Agarwal
Issue Date: June 30, 2020
Title of Invention: Threat Model Chaining and Attack Simulation Systems and Related Methods

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the drawings:

In FIG. 10, the rightmost line connecting the "AKAMAI DNS" component with the "FIRE WALL" component should have the end arrow pointing at the "FIRE WALL" component.
In FIG. 21, the rightmost line connecting the "AKAMAI DNS" component with the "FIRE WALL" component should have the end arrow pointing at the "FIRE WALL" component.
In FIG. 22, the rightmost line connecting the "AKAMAI DNS" component with the "FIRE WALL" component should have the end arrow pointing at the "FIRE WALL" component.

In the abstract:

In the Abstract, Line 2, change "including a threat model components" to -including threat model components-.
In the Abstract, Line 5, change "associate with" to -associated with-.
In the Abstract, Line 9, change "model include" to -model and include-.

In the specification:

Column 5, Line 55, change "compensated" to -compensating-.

Column 6, Line 30, change "compensatory" to -compensating-.

Column 15, Line 4, change "showing" to -shows-.

Column 16, Line 36, change "a cloud computing" to -cloud computing-.

Column 17, Line 35, change "popup threat" to -popup threat report-.

Column 18, Lines 2-3, change "a similar" to -an-.

Column 18, Line 3, change "to the" to -similar to the-.

Column 18, Line 39, change "list" to -lists-.

Column 20, Line 6, change "the component" to -component-.

Column 20, Line 12, change "ID a version" to -a CPE ID indicating a version-.

Column 23, Line 19, change "to" to -to/from-.

Column 23, Line 62, change "some sub-component" to -a sub-component-.

Column 23, Line 63, change "some element" to -an element-.

Column 27, Line 1, change "analyze" to -analyzing-.

Column 27, Line 3, change "analyze" to -analyzing-.

Column 27, Lines 4-5, change "measure and quantify" to -measuring and quantifying-.

Column 33, Line 50, change "functionality" to -the web page having functionality-.

Column 34, Line 33, change "is" to -includes-.

Statement of Facts Supporting the Requested Corrections

The submitted corrections are to correct grammatical errors. Inasmuch as at least one of the errors was in the application as originally submitted, the appropriate fee is submitted herewith. Form PTO/SB/44 is included with this correspondence. Please contact me if you have any questions.

Sincerely,

Paul



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	12/20/2018	Anurag Agarwal	THREATM008	3702
145042	7590	09/21/2020		
Law Office of Paul B. Johnson 8483 S. 1275 E. Sandy, UT 84094-1363			EXAMINER SONG, HOSUK	
			ART UNIT	PAPER NUMBER
			2435	
			NOTIFICATION DATE	DELIVERY MODE
			09/21/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

paul@pauljohnsonlaw.com

**Response to the
Request for
Certificate of Correction**

Patent No.
10699008

Applicant(s)
Agarwal, Anurag

Issue Date
06/30/2020

Docket No.
THREATM008

This is in response to the request for a Certificate of Correction filed 06 July 2020

☒ **Request Approval- In- Part** - Consideration has been given to your request for the issuance of a Certificate of Correction under the provisions of 37 CFR 1.322 and/or 37 CFR 1.323. The Request is improper and approved in part for the reason(s) below:

☐ **Supersede/Vacate** - The Certificate of Correction issued in error, in that error(s) was made in identifying the patent number and/or keying text/corrections. See Other Comments below:

1. ☐ Assignees' names and addresses (assignment data) printed in a patent, are based solely on information supplied in the appropriate space for identifying the assignment data on the Issue Fee Transmittal Form (PTOL-85b). Any request for a patent to be corrected to state the name of the assignee, must state that the assignment was submitted for recordation as set forth in 37 CFR 3.11 before issuance of the patent. Petition under 3.81 is to be filed for consideration of correction to assignee. The petition fee set forth in 37 CFR 1.17(i)(1) (currently \$140, \$70, \$35 for large, small and micro entities, respectively).
2. ☐ The alleged error in _____, is in fact an Amendment and/or Change made by the examiner and considered to be in accordance with the permissible amendments enumerated in the Manual of Patent Examining Procedure (MPEP) Section 1302.04. Applicant did not file objection or amendment under 37 CFR 1.312 prior to payment of the issue fee.
3. ☐ A petition under CFR 1.182 is required to correct the alleged errors in spelling or order of inventor's names, since inventor's names are printed solely in accordance with the type-written names, and in the order of the type-written names on the Application Data Sheet (ADS). The required fee currently under rule 1.17(f) (small entity \$200, large entity \$400, micro entity fee \$100).
4. ☐ With respect to the alleged error in changing the inventor name on the patent due to clerical error in ADS/OATH of related patents. The inventors name is printed in accordance with the OATH/ADS submitted at the time of filing the application. However, your attention is directed to C.F.R. 1.324, wherein a request is being made to change, add or delete inventor(s), after issuance of the patent.
5. ☐ With respect to the alleged error in _____, comparison of the printed patent with the corresponding location in the application file reveals that there is no discrepancy.
6. ☐ With respect to 37 CFR 1.72, the title should be brief but technically accurate and descriptive and should contain fewer than 500 characters. Inasmuch as the words new, improved, improvement of, and improvement in are not considered as part of the title of an invention, these words should not be included at the beginning of the title of the invention and will be deleted when the Office enters the title into the Offices computer records, and when any patent issues.
7. ☐ The fee for correction under 37 CFR 1.323 is set forth in 37 CFR 1.20(a). ☐ Partial fee ☐ No fee was received with your request. Full fee payment is required before further action is taken on this request.
8. ☐ With respect to the request for corrected Letters Patent (Grant), corrections to the original Letters Patent are made under the provisions of Rule 1.322(b), not Rule 1.323, unless a petition is granted.
9. ☒ Other Comments: See Continuation Sheet

Further correspondence concerning this matter should be filed and directed to the Certificates of Correction Branch.

Legal Instrument Examiner: /DORIS M BURNS/
LIE, ODM

Phone: (703)756-1958

Certificates of Correction Branch email: CustomerServiceCoC@uspto.gov

CoC Central Phone Number: (703)756-1814

If applicable, information regarding a petition under 37 CFR 1.183 should be directed to the attention of the Commissioner for Patents using the FAX number (571) 273-8300

Continuation of Other Comments: The Request for the Drawings has been denied. Please provide the Office with a new set of Drawings. Request Approved in Part
A certificate of correction will be issued to correct the remaining errors noted in your request.

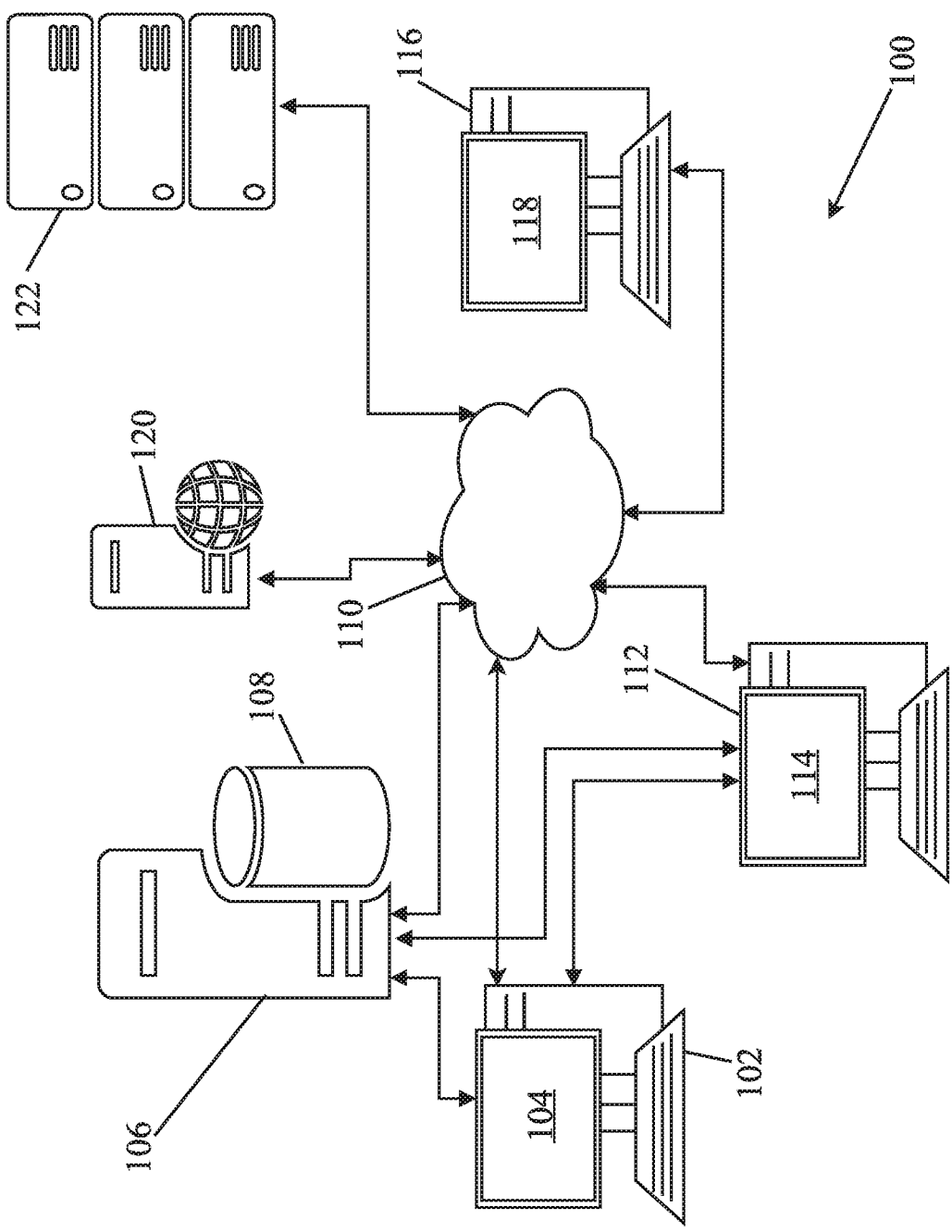
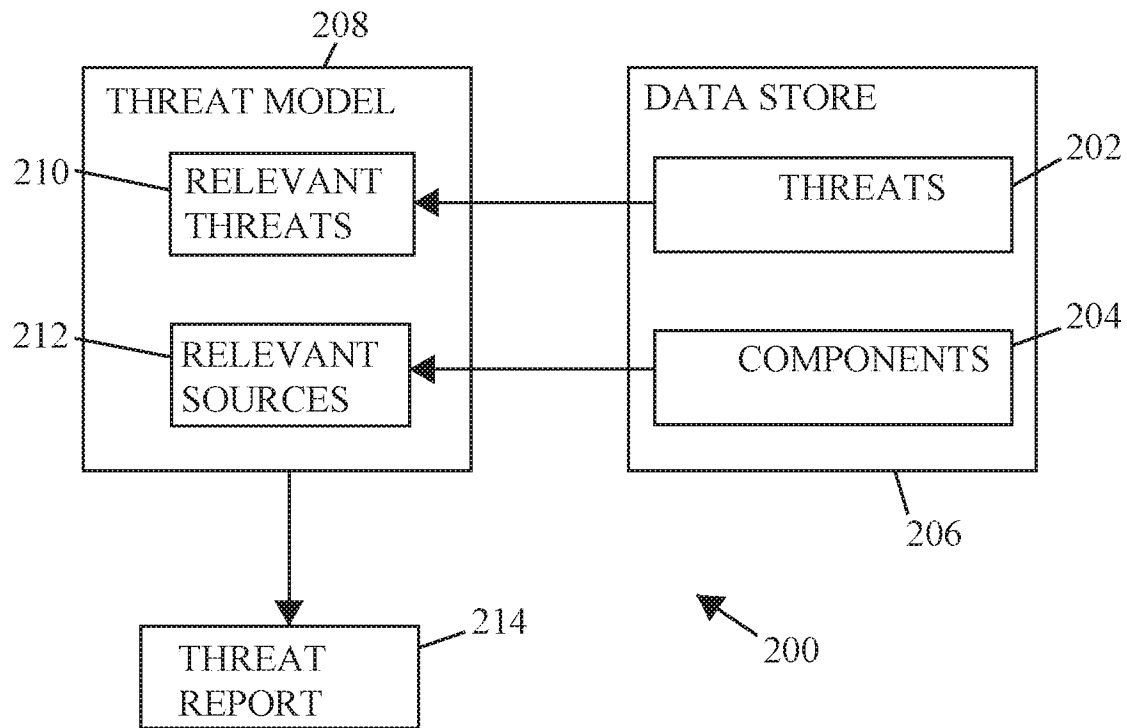
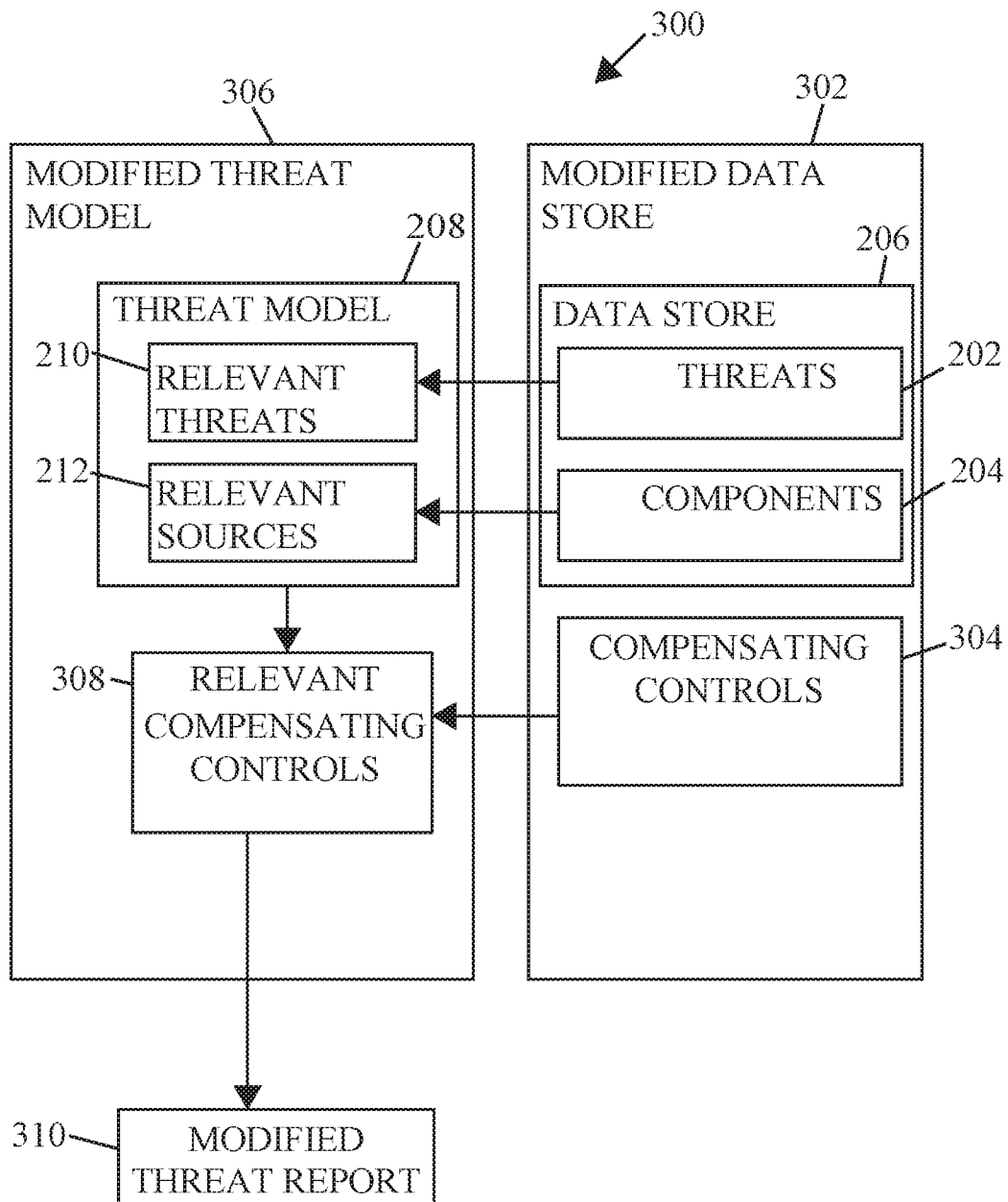


FIG. 1

**FIG. 2**

**FIG. 3**

4/22

400

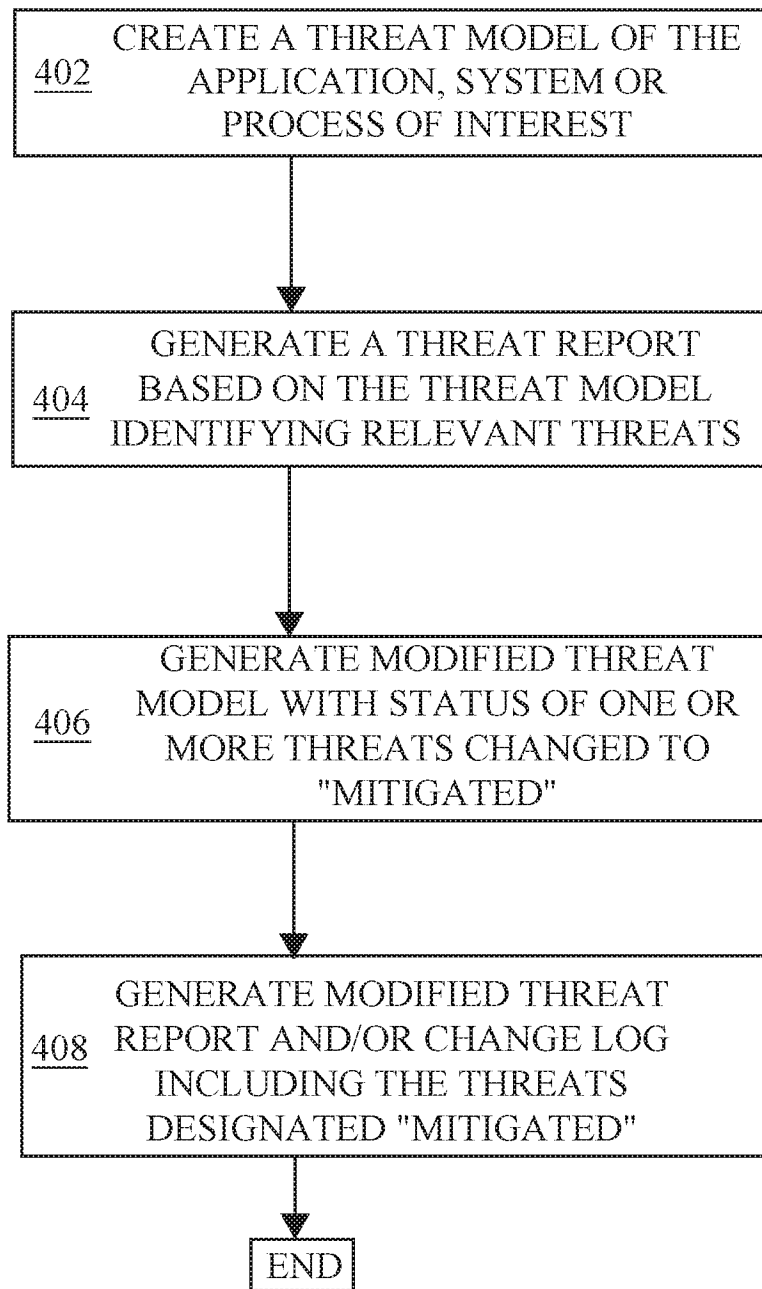
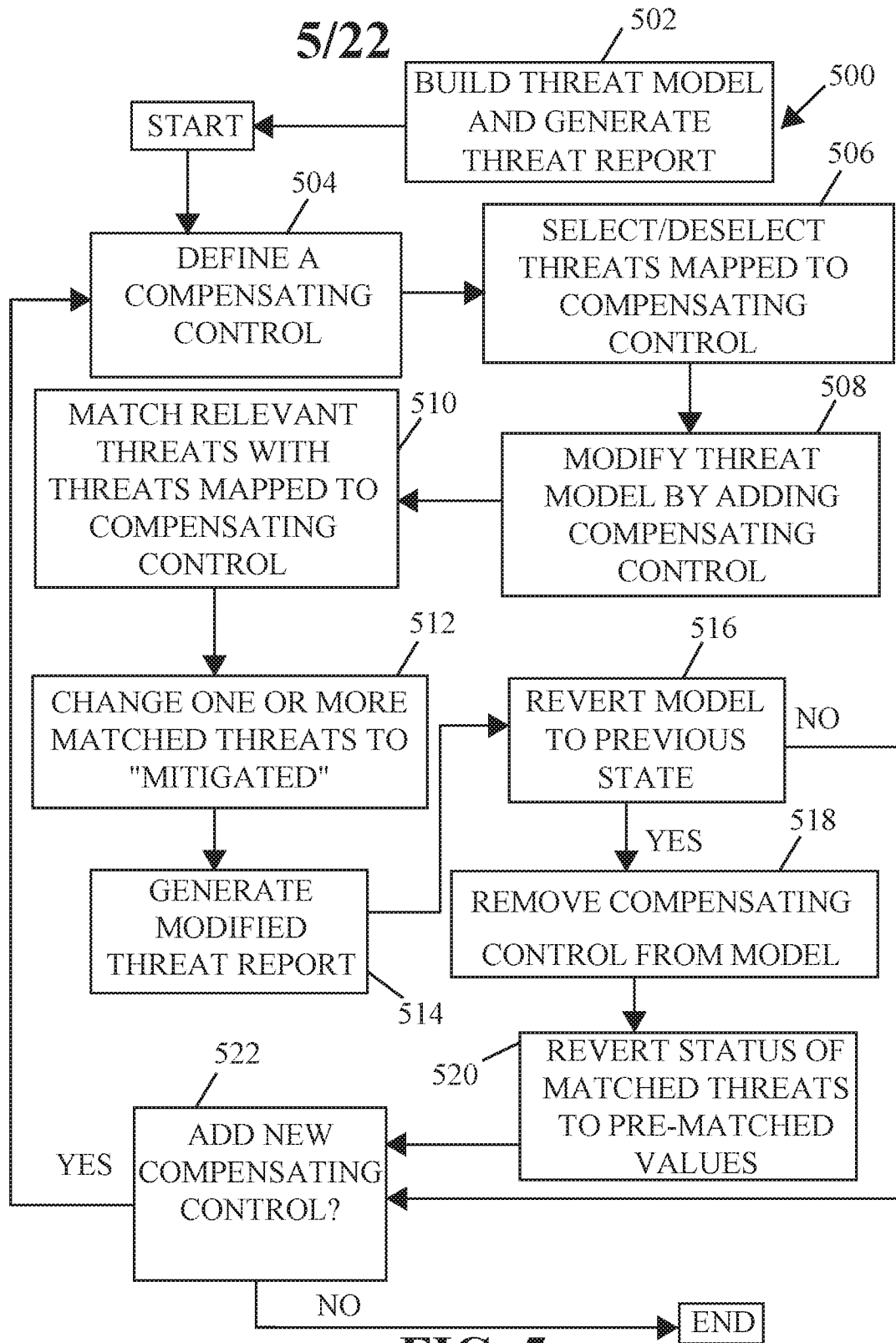


FIG. 4



6/22

<div> <div>HOME</div> <div>KNOWLEDGE BASE</div> <div>TEMPLATES</div> <div>PROFILE</div> </div>			
<div> <div>SELECT ALL</div> <div>NEW</div> <div>DELETE</div> <div>COPY TO LIBRARY</div> </div>		<div> <div>CHANGE PASSWORD</div> <div>SIGN OUT</div> </div>	
<div> <div>EDIT</div> <div>SELECT LIBRARY</div> <div>THREAT MODELER ▼</div> </div>			
COMPONENTS			
NAME	TYPE	LABELS	LOGIN
			TYPE: APPLICATION COMPONENT
WIFI TR	DEVICE		WEB APPLICATION
MODEM	DEVICE	EMBED. SYS.	PASSWORD
WIFI PORT	IOT DEVICE	IOT	AUTHENTICATION
HTTPS	PROTOCOLS		FEATURE
COOKIES	GEN DT STORE	TMT	DESCRIPTION
DATABASE	DB	HARDWARE	
LOGIN	APP. COMPONENT.	WEB, APP, FEAT.	
COMMENT	APP. COMPONENT.	WEB, APP, FEAT.	
SHOP CART	APP. COMPONENT.	WEB, APP, FEAT.	
ACH TRANS.	APP. COMPONENT.	WEB, APP, FEAT.	
USB PORT	IOT DEVICE	IOT	
FILE SVR	DEPLOY. COMP.		
EMAIL SVR	DEPLOY. COMP.		
FIREWALL	APP. COMPONENT.		

PROPERTIES	
THREATS	+
INDUCING	×
ACCT LOCKOUT	
SESSION	×
HJACKING	
CLICK JACKING	×
SECURITY REQUIREMENTS	+
RANDOMIZING SECRET	×
ENCRYPTION ALGORITHM	×
PARAM. DYNAMIC SQL	×

FIG. 6

600

7/22

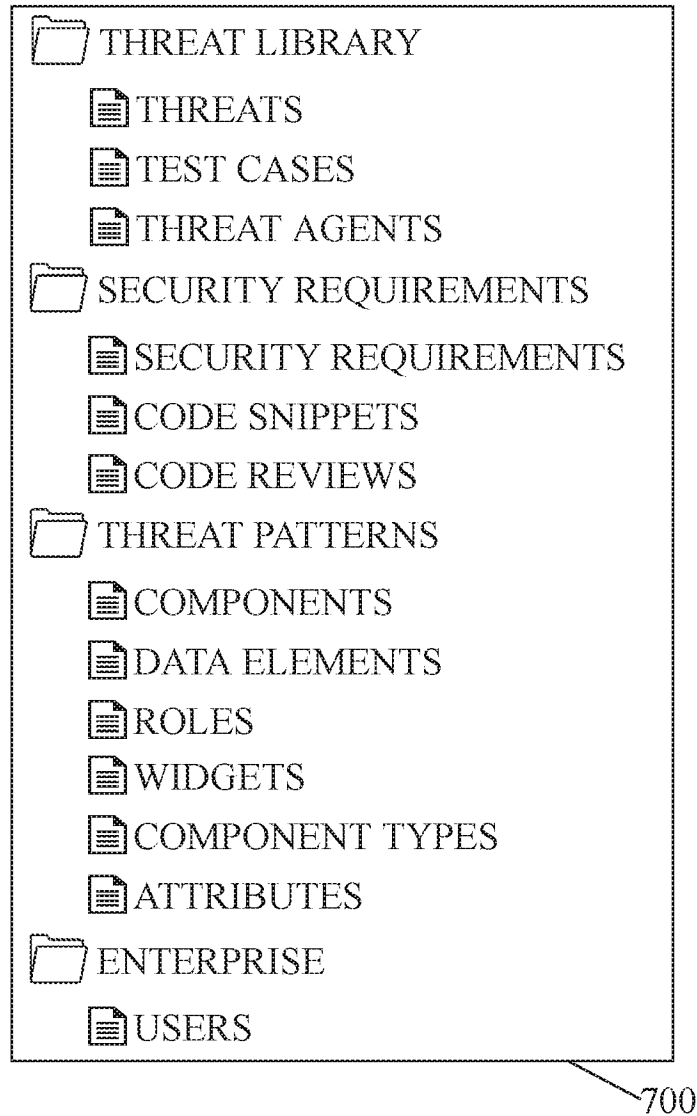


FIG. 7

THREATS			SENSITIVE DATA		PROPERTIES
NAME	RISK	LABELS	EXPOSURE		THREAT AGENTS
BUFFER OVERFLW	VERY HIGH	BUFFER	RISK: VERY HIGH		+
SESSION HIJACK	VERY HIGH	JAVA, CAPEC,...	OWASP-A6		×
PHYSICAL THEFT	VERY HIGH	CAPEC-507,...	CAPEC-610		×
HTTP SPLITTING	HIGH		OWASP-A5- SECURITY MIS- CONFIGURATION		+
BRUTE FORCE	HIGH	CAPEC-112,...	DESCRIPTION		×
DBL ENCODING	MEDIUM	CAPEC-120,...			×
SENS. DATA EXP.	VERY HIGH	OWASP-A6,...	WWW.OWASP.ORG		+
INTEGER ATTACKS	MEDIUM	CAPEC-128,...			REQUIREMENTS
POINTER ATTACK	MEDIUM	CAPEC-129,...			CLICKJACK
SYMLINK ATTACK	MEDIUM	CAPEC-132,...			CHEAT SHEET
EMAIL INJECT.	MEDIUM	CAPEC-134,...			TEST COMP
FORMAT STR. INJ.	HIGH	CAPEC-135,...			CONTROL
AUTOMATION ATK	VERY HIGH				SS-COMPENS.
SPAM	VERY HIGH				CONTROL

FIG. 8

9/22

✓

+

✗

✕

SELECT LIBRARY

THREAT MODELER ▼

🏠

📁

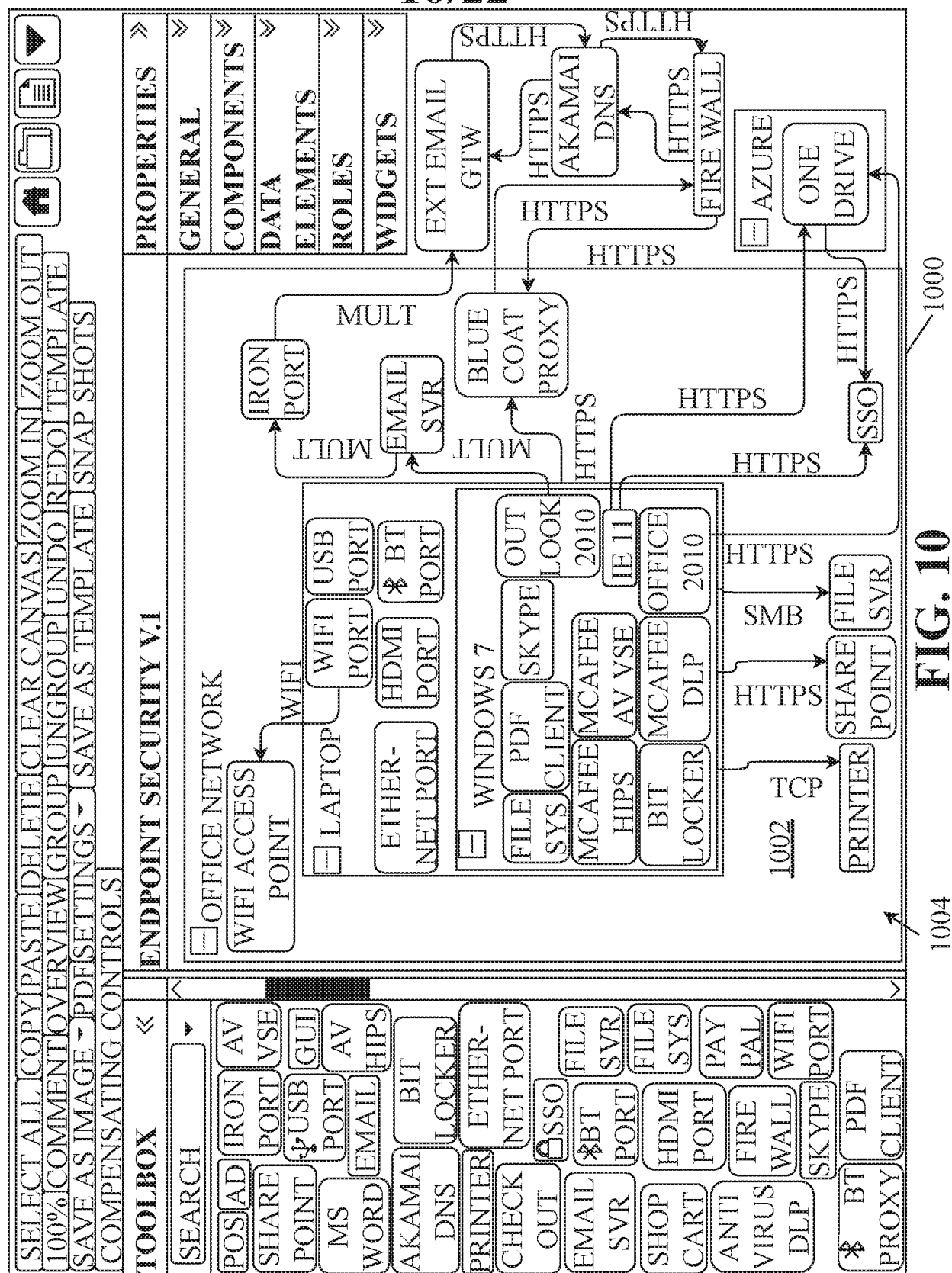
📄

▼

SECURITY REQUIREMENTS		PROPERTIES	
NAME	LABELS	NAME	CODE SNIPPETS
		DESCRIPTION	CODE REVIEWS
ENCRYPTION: USE ONLY STR...	AZURE LIB...		
ENCRYPTION: ENSURE RAND...	DOM,...		
INPUT VALIDATION WITH...	HARDWARE,...		
TM - INPUT VALIDATION	JAVA,INI,...	IS COMPENSATING CONTROL ☐	
USING SSL	CERTS,...	LABELS	
KEY MANAGEMENT: ENSU...	OWASP,...		
TLS: PREVENT CACHING OF...			
CERTIFICATES: USE AN APP...	CERTS,...		
ADD FIREWALL RULES	EVENT,TO,...		
HOST INTEGRITY CHECKING	TO,SSE,...		
SECURE BROWSERS	SCRIPT,LOG,...		
OUTPUT ENCODING			
APPLY PATCHES	XSS,REL,...	SAVE	CANCEL
DISABLE HTTP TRACE	INI,HTTP,...		

FIG. 9

900



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	TCP 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	
MCAFEES 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

NEW

EDIT

DELETE

DIAGRAM

REPORT

THREAT TREE

🏠

📄

📁

⏴

THREAT MODELS PDF

ENDPOINT SECURITY V.1

NAME	V.	THREATS	SECURITY REQ'TS	82	TEST CASES	5	CODE RVW	3
AIR VEHIC SYS	1.0							
AWS - EC2	1.0							
BANKING APP	1.2							
IOT ENVIR.	1							
WRK COMMUTE	1							
CRM APP	2.0							
ECOMM POC	2.5							
END POINT SEC.	1							
IOT SERVER	1							
MICROWEB SVC	1.0							
MOBILE BAKE...	1							
SQL DB	12							
HEALTH THREAT	1.0							
ONLINE BANK	1							
FINAN. THREAT	1							

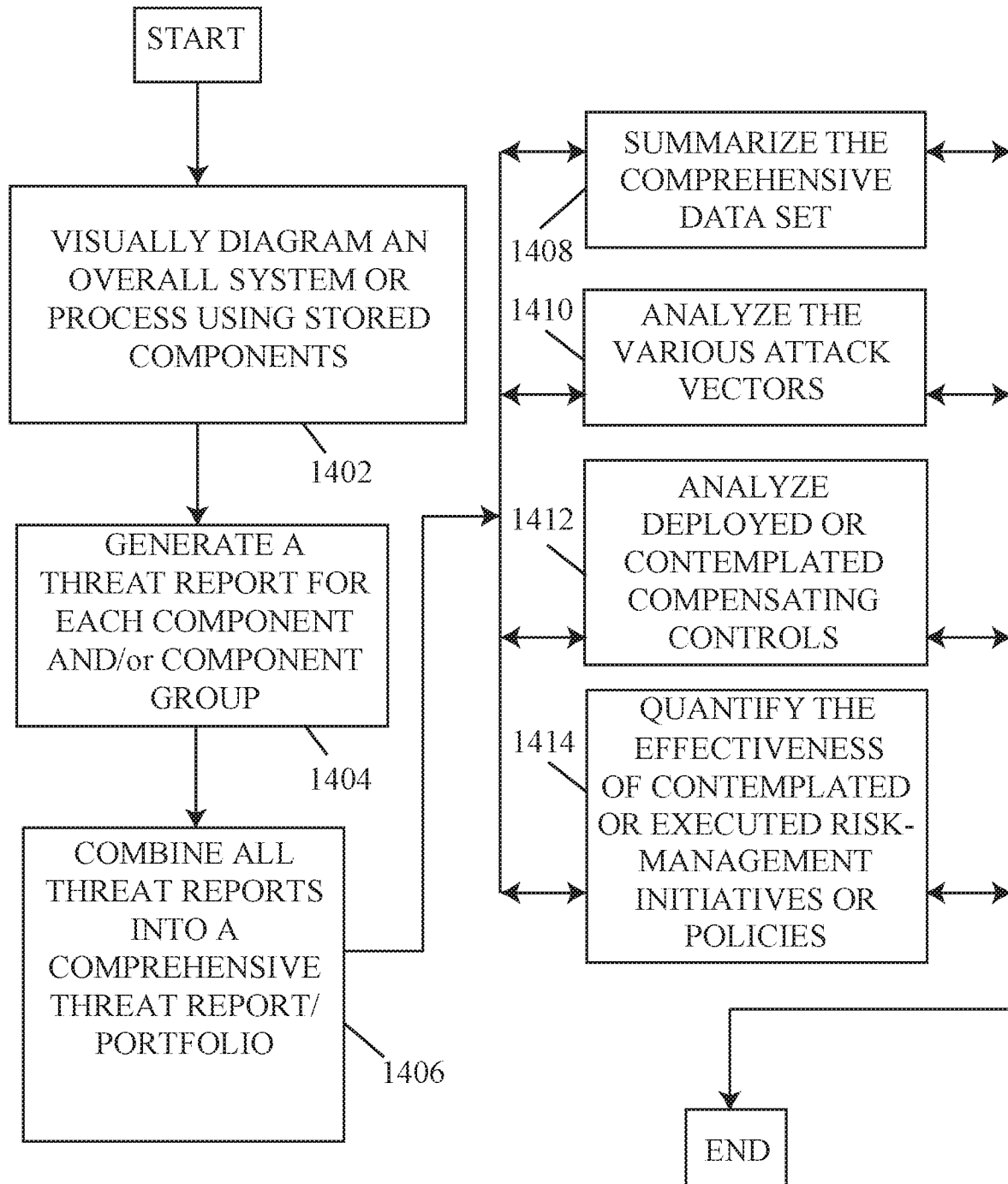
CHANGE RISK CHANGE RISK STATUS

DRAG HEADER HERE TO GROUP BY THAT COLUMN

THREAT	RISK	STATUS	SOURCE	ACTION
ACCT HIJACK	VERY HIGH	OPEN	AWS ELB	D NOTE
INSEC. COMM.	VERY HIGH	OPEN	AWS ELB	D NOTE
PWD BRUTE F..	HIGH	OPEN	APP	D NOTE
SENS DATA EXP	VERY HIGH	OPEN	APP	D NOTE
SQL INJECTION	HIGH	MITIGATED	APP	D NOTE
BLIND SQL INJ	HIGH	MITIGATED	APP	D NOTE
IDENT SPOOF	MEDIUM	OPEN	WEB BR	D NOTE
TARGETED MAL	VERY HIGH	OPEN	WEB BR	D NOTE
CLICKJACKING	VERY HIGH	OPEN	APP	D NOTE
X SITE TRACING	VERY HIGH	OPEN	WEB SVR	D NOTE
IIS SNIFFING	VERY HIGH	OPEN	WCF SVC	D NOTE
XML SVC DEN	VERY HIGH	OPEN	WEB SVC	D NOTE
BUFFER OVFLW	VERY HIGH	OPEN	MS WORD	D NOTE
FILE MANIP	MEDIUM	MITIGATED	FILE SYS	D NOTE
PHYS THEFT	VERY HIGH	MITIGATED	LAPTOP	D NOTE
BLUEJACKING	VERY HIGH	OPEN	BT PORT	D NOTE

1302 1300

FIG. 13

**FIG. 14**

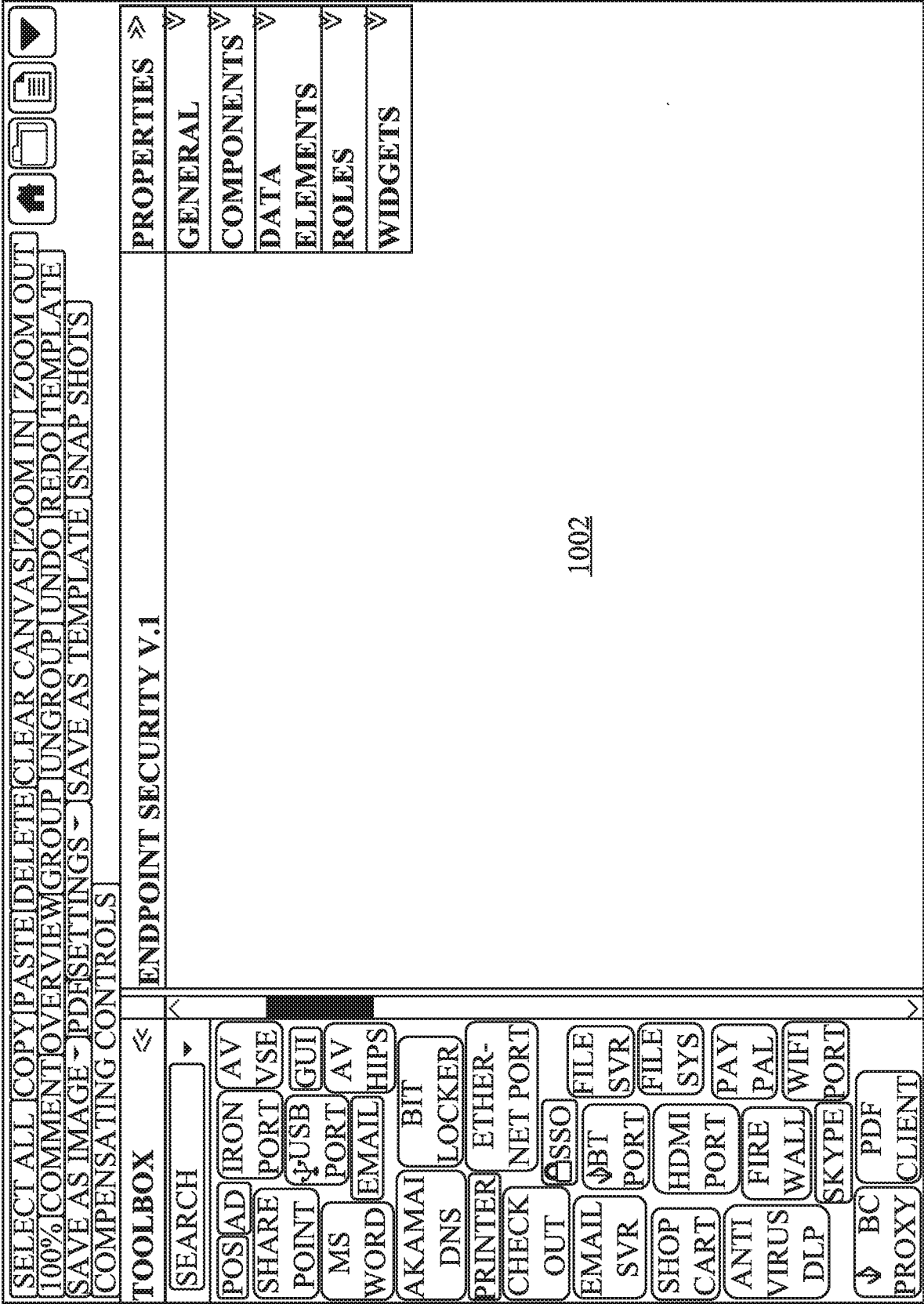


FIG. 15

16/22

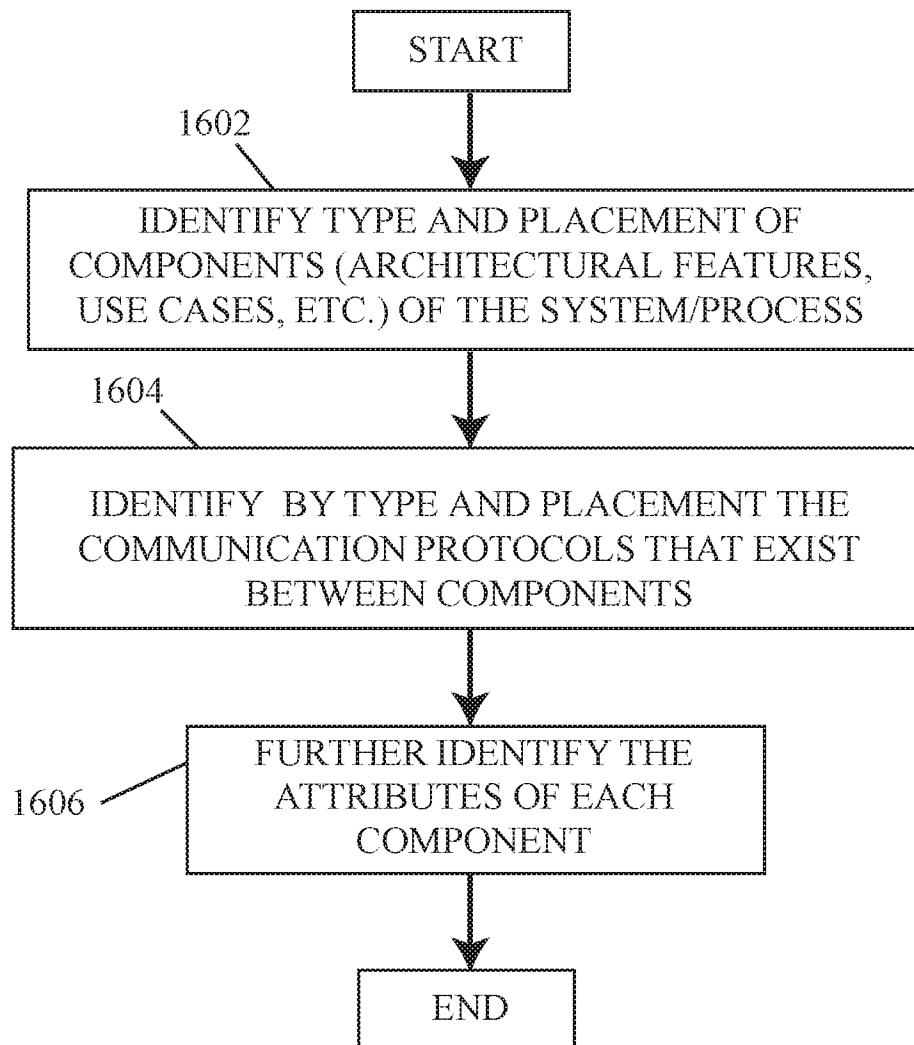


FIG. 16

17/22

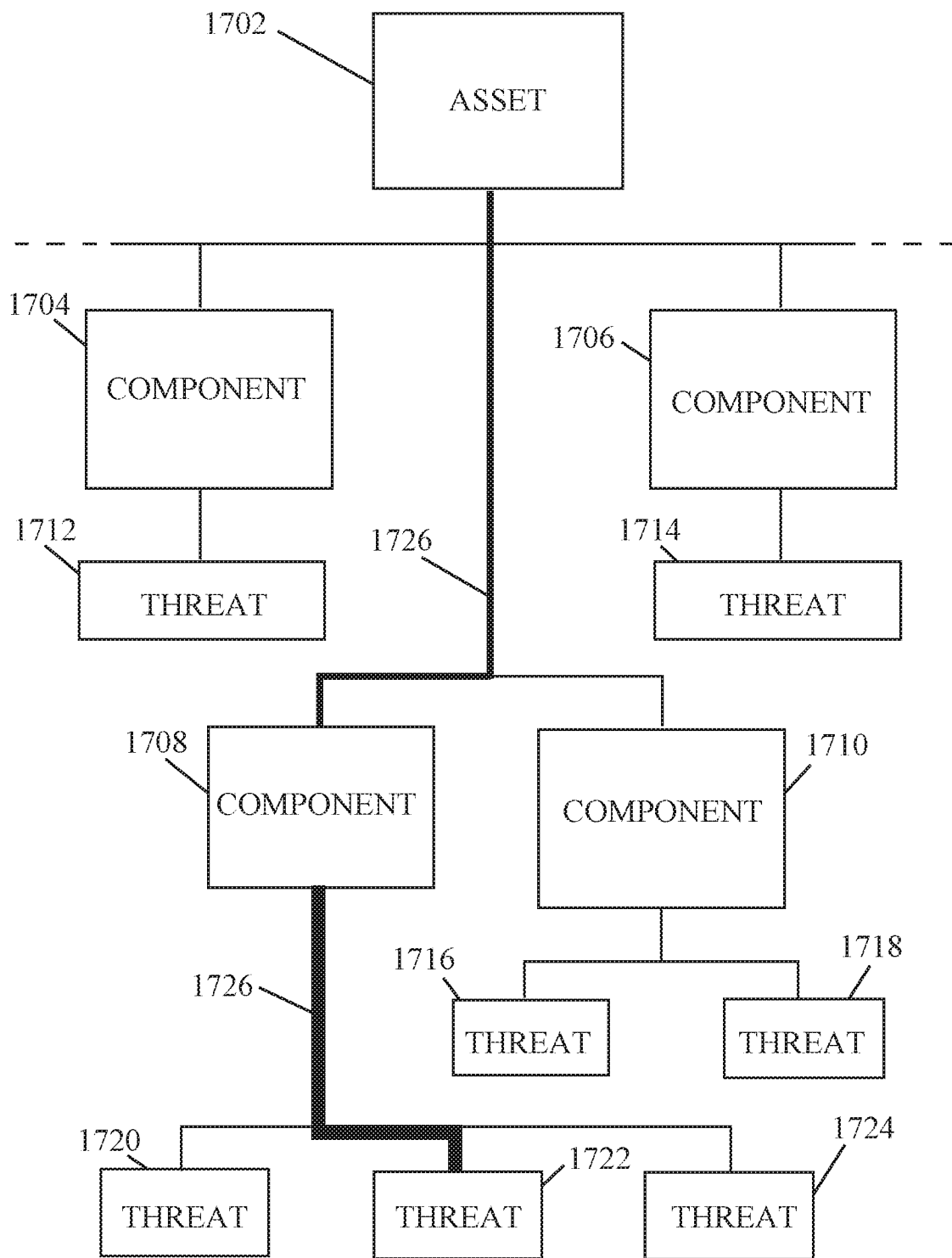


FIG. 17

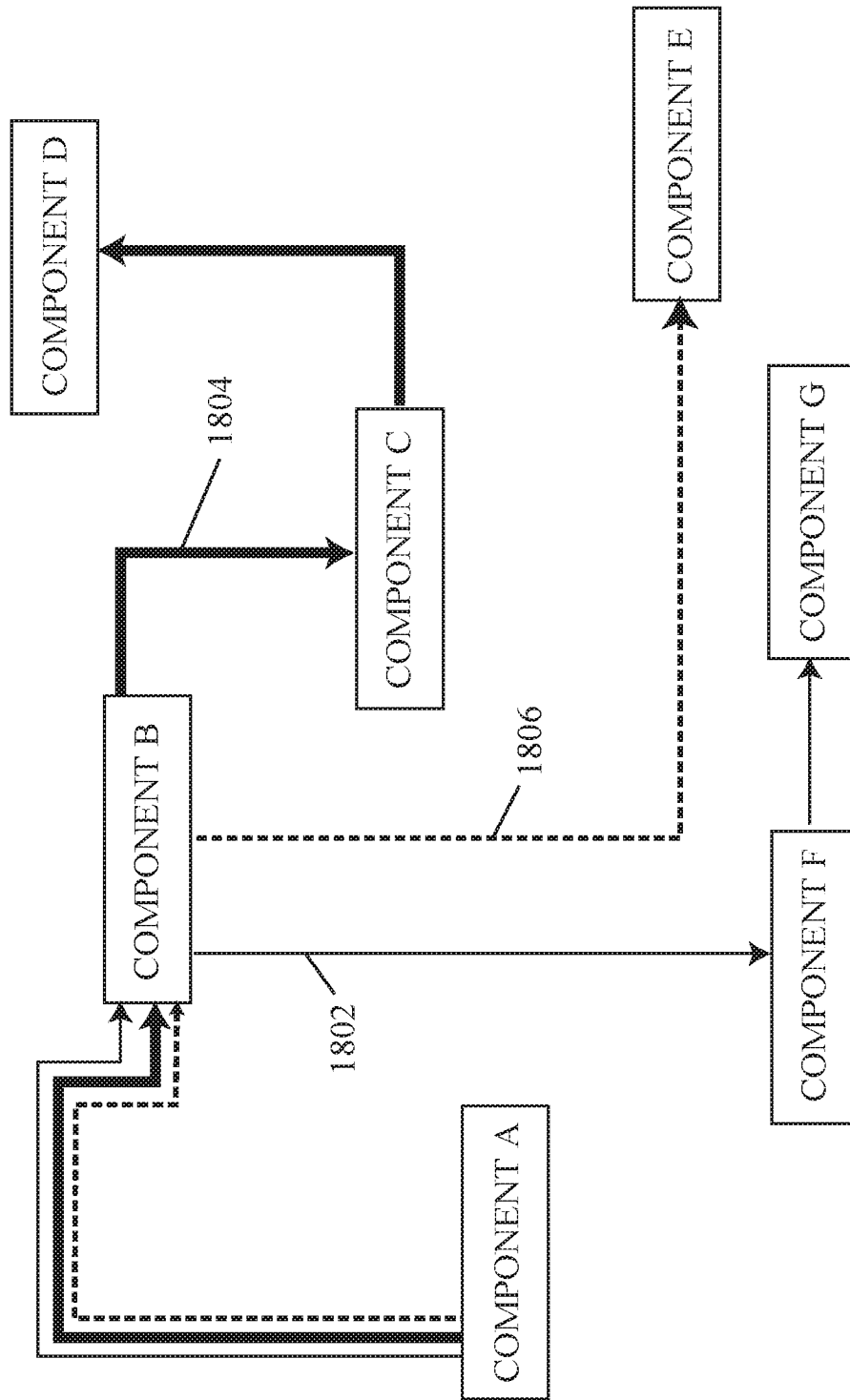


FIG. 18

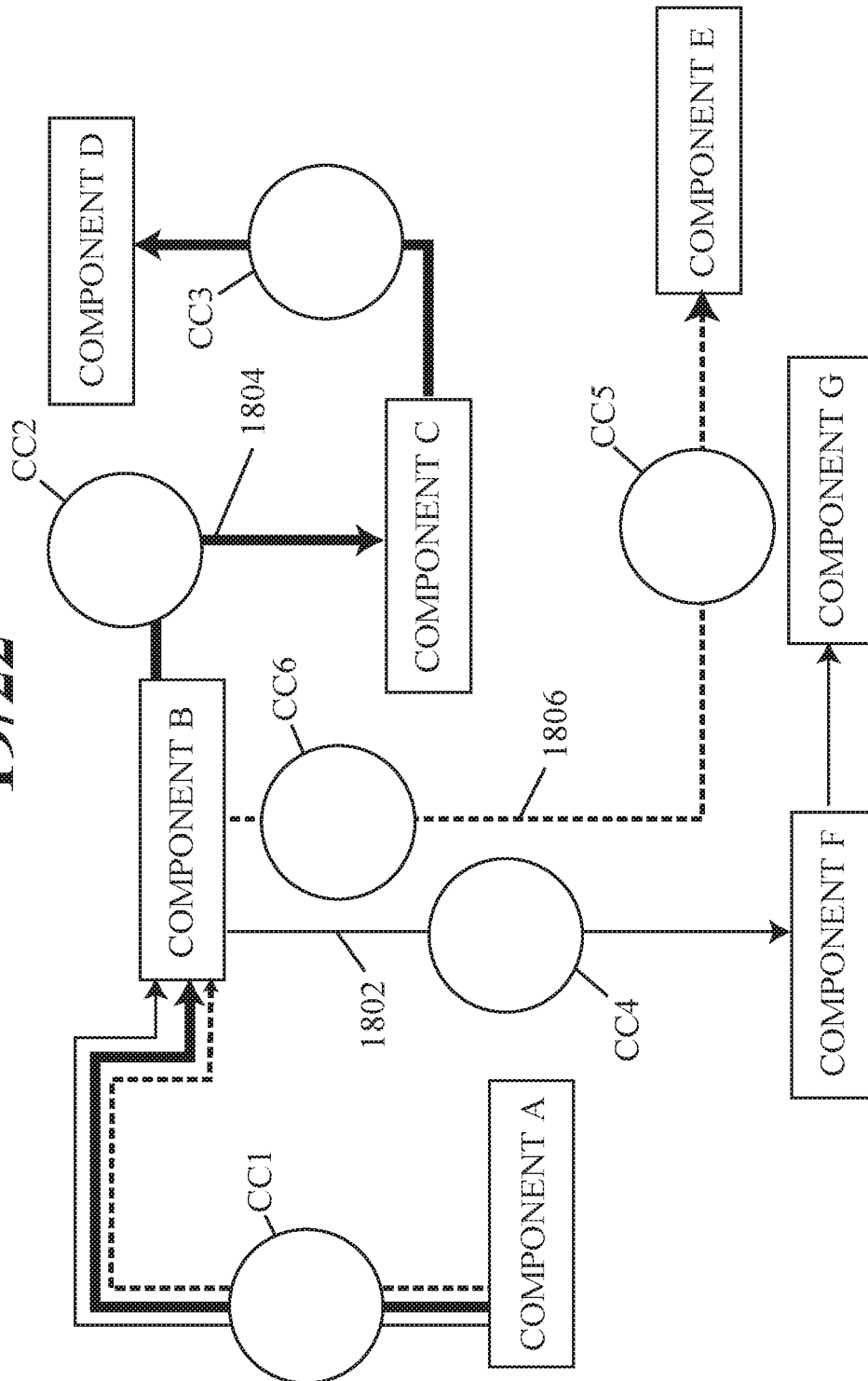


FIG. 19

20/22

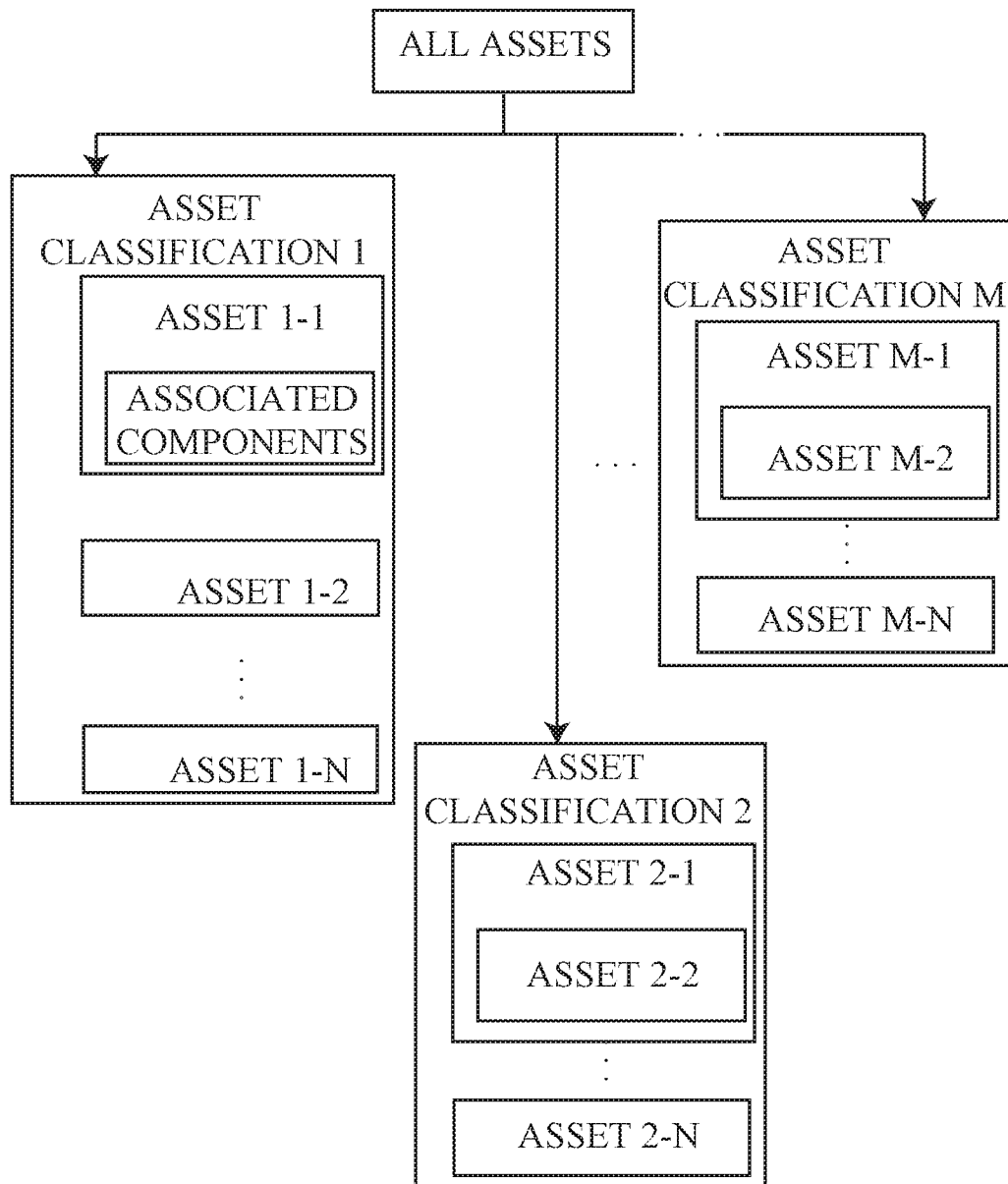
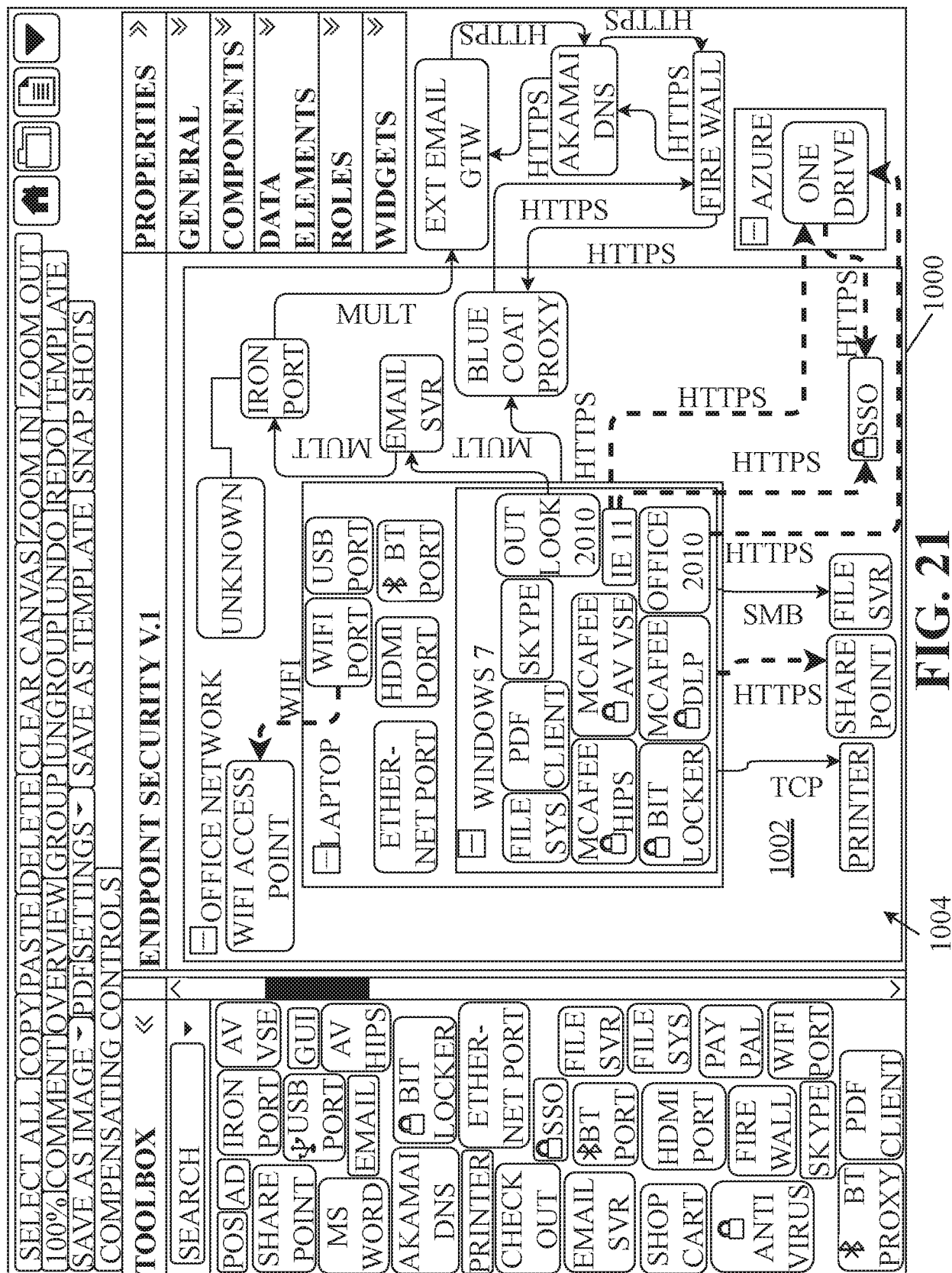


FIG. 20





ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #
16/228,738

RECEIPT DATE / TIME
09/21/2020 05:13:13 PM ET

ATTORNEY DOCKET #
THREATM008

Title of Invention

THREAT MODEL CHAINING AND ATTACK SIMULATION SYSTEMS AND RELATED METHODS

Application Information

APPLICATION TYPE Utility - Nonprovisional Application
under 35 USC 111(a)

PATENT # 10699008

CONFIRMATION # 3702

FILED BY Paul Johnson

PATENT CENTER # 60084235

FILING DATE 12/20/2018

CUSTOMER # 145042

FIRST NAMED
INVENTOR Anurag Agarwal

CORRESPONDENCE
ADDRESS -

AUTHORIZED BY -

Documents

TOTAL DOCUMENTS: 4

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
Drawings008_CleanCopy.pdf	22	Drawings-only black and white line drawings	2126 KB
AnnotatedSheets.pdf	3	Drawings-only black and white line drawings	226 KB
ReplacementSheets.pdf	3	Drawings-only black and white line drawings	222 KB
ResponseToCOCBranch.pdf	3	Miscellaneous Incoming Letter	67 KB

Digest

DOCUMENT**MESSAGE DIGEST(SHA-512)**

Drawings008_CleanCopy.pdf	8A63DFF94B561D4D97304E8B3663D7D750DF3E15E3A0AC0C2 1F578855DA78CEE829D173607ADE1C715BD29491B37343681F A9B40EF0AF88A9E59137211CC30AD
AnnotatedSheets.pdf	25146A5450252B4B6CD41509BC5014AE0FCC93F17A27E93C7 1CCFA440D41FC8A0173BFD26EB8894FA60B4CB2997F3CA86 F60E8E94AC4A6A6187E2E613DADEC4F
ReplacementSheets.pdf	9D19B85912B65FAA5E961568E88B9AC3657EFA29262D38755D 9F582B3809226543ECC6BAEC0FA40D9F5014EB5E305E18EF4 E111D0AE5DE92016E5407AF640A27
ResponseToCOCBranch.pdf	05EEE7BD0D571DBBF3F2A2EF23992BED1ABADAB46F09E46D 0A98AF3BD6D81915F5C1FF5512FB45F72B26FCCFA3617B764 FCA6636C003AFEE4BBE5283A132BAB9

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

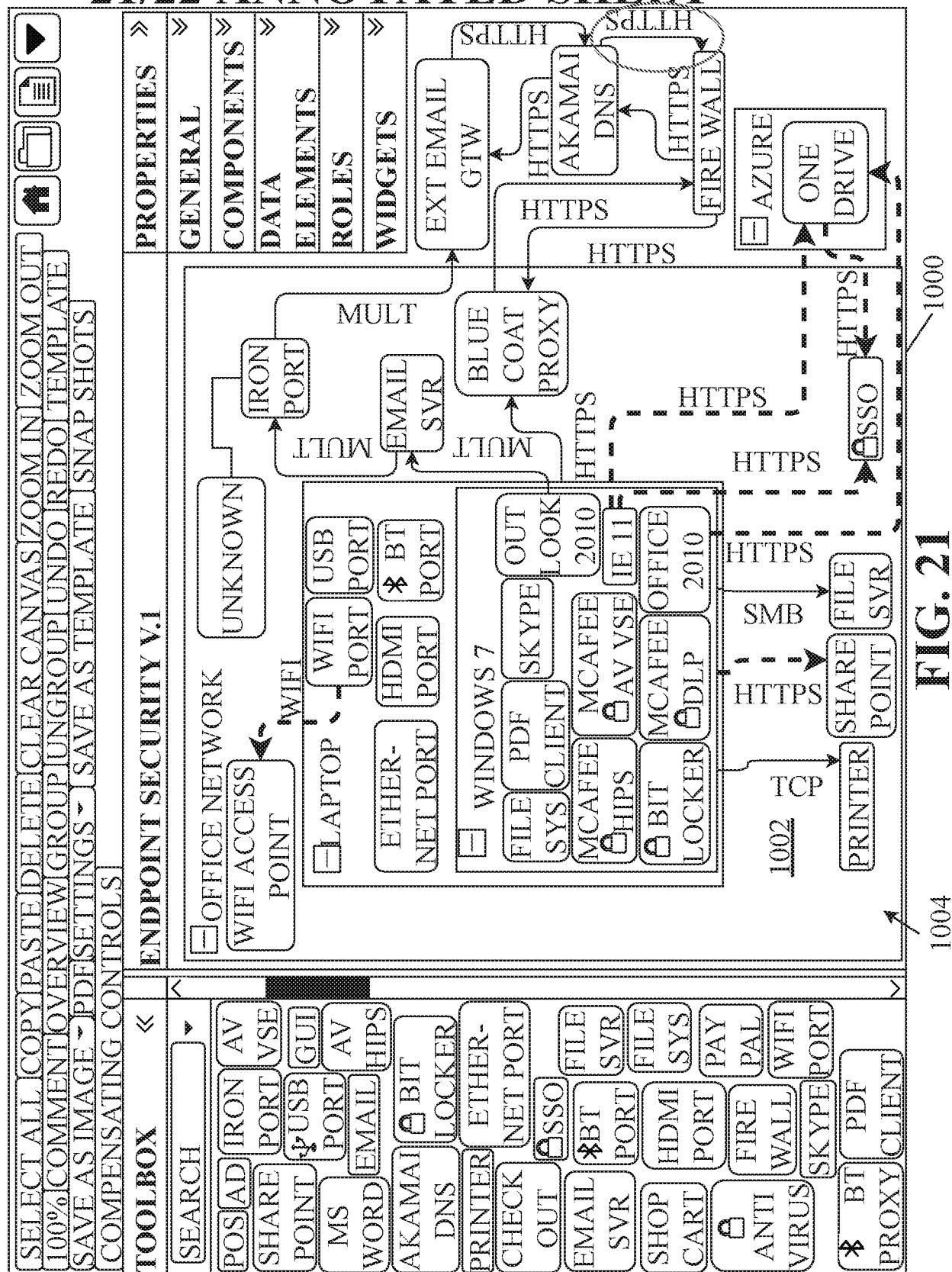
If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

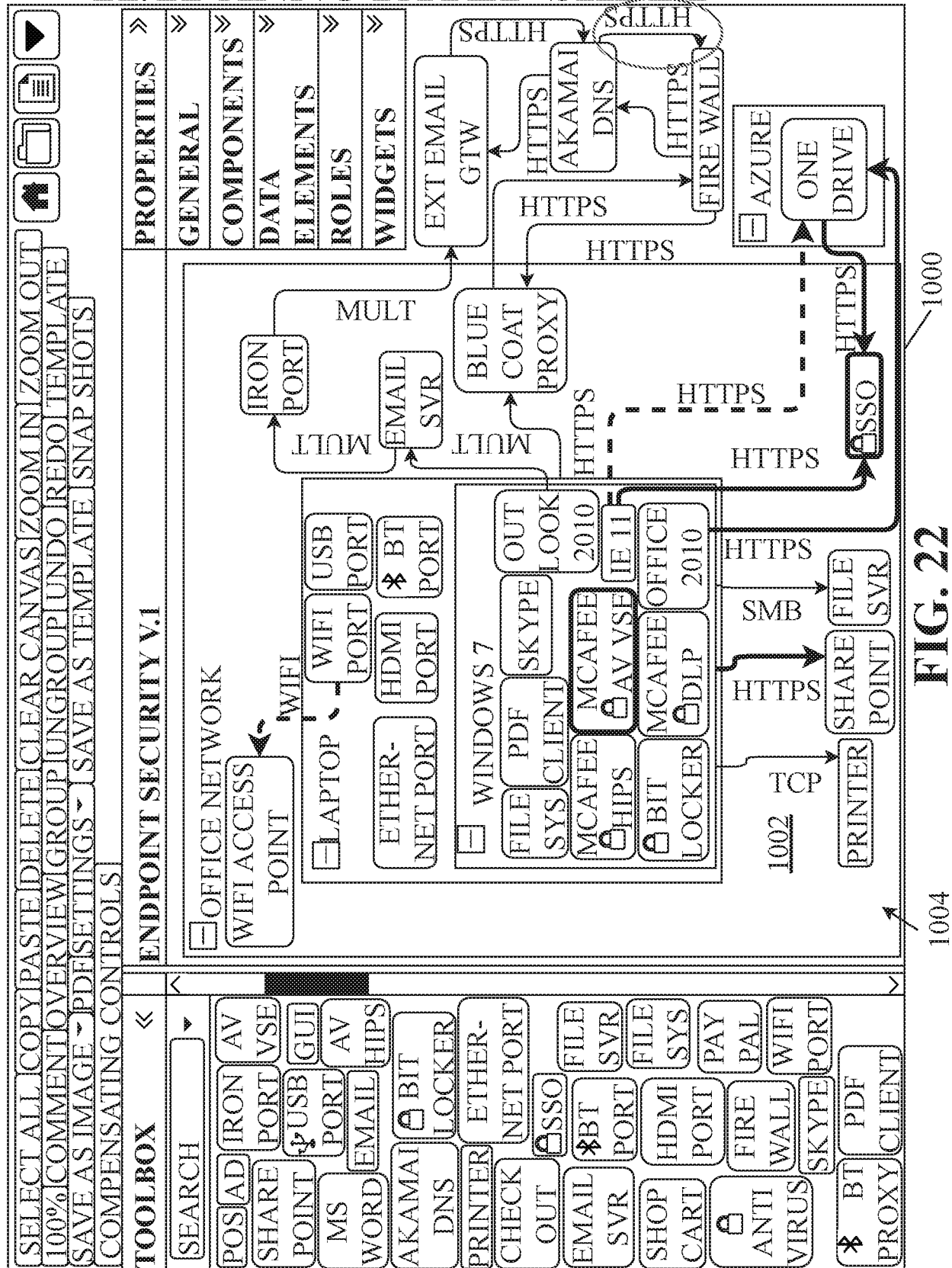
National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.





10/22 REPLACEMENT SHEET

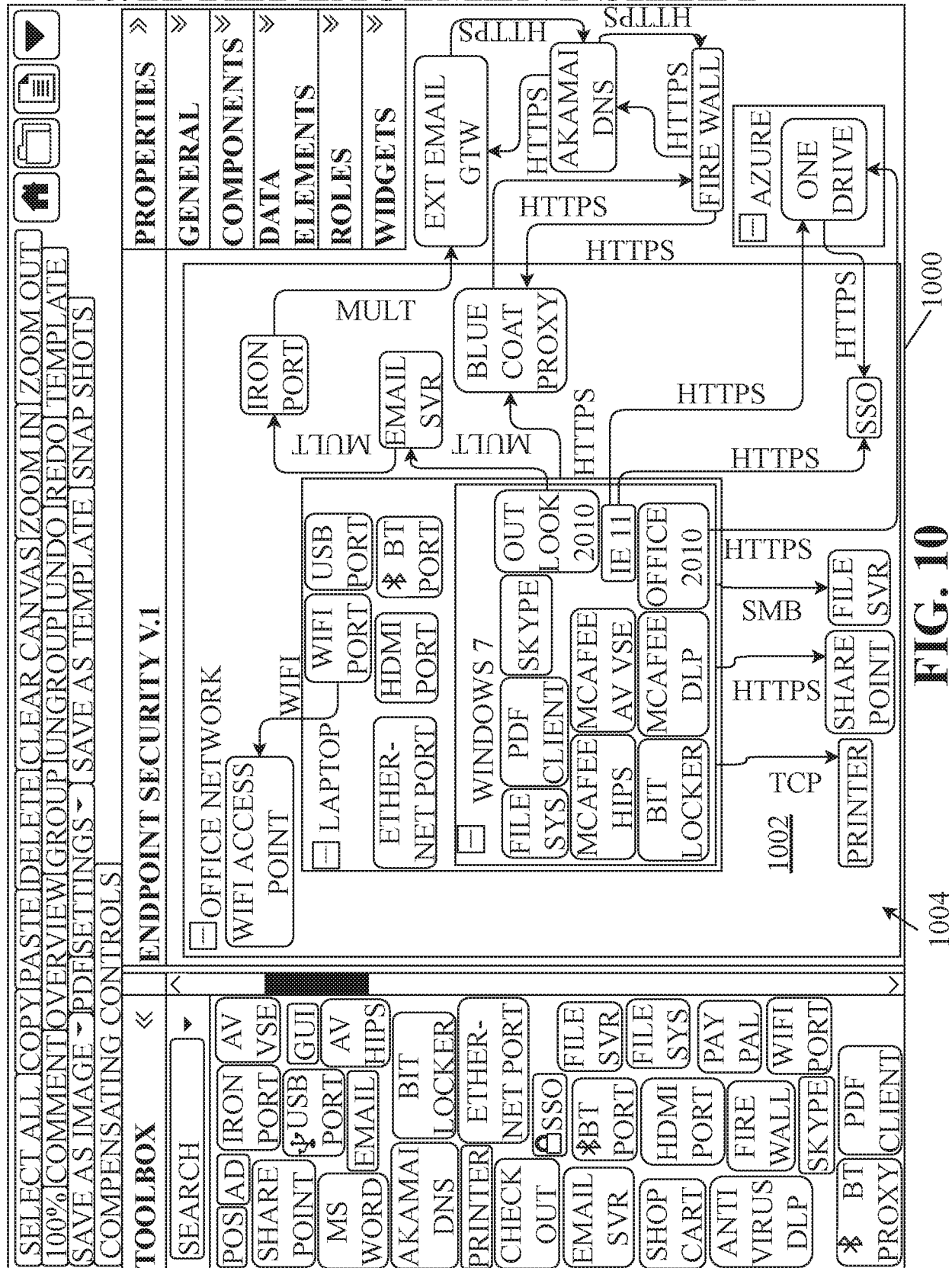


FIG. 10

21/22 REPLACEMENT SHEET

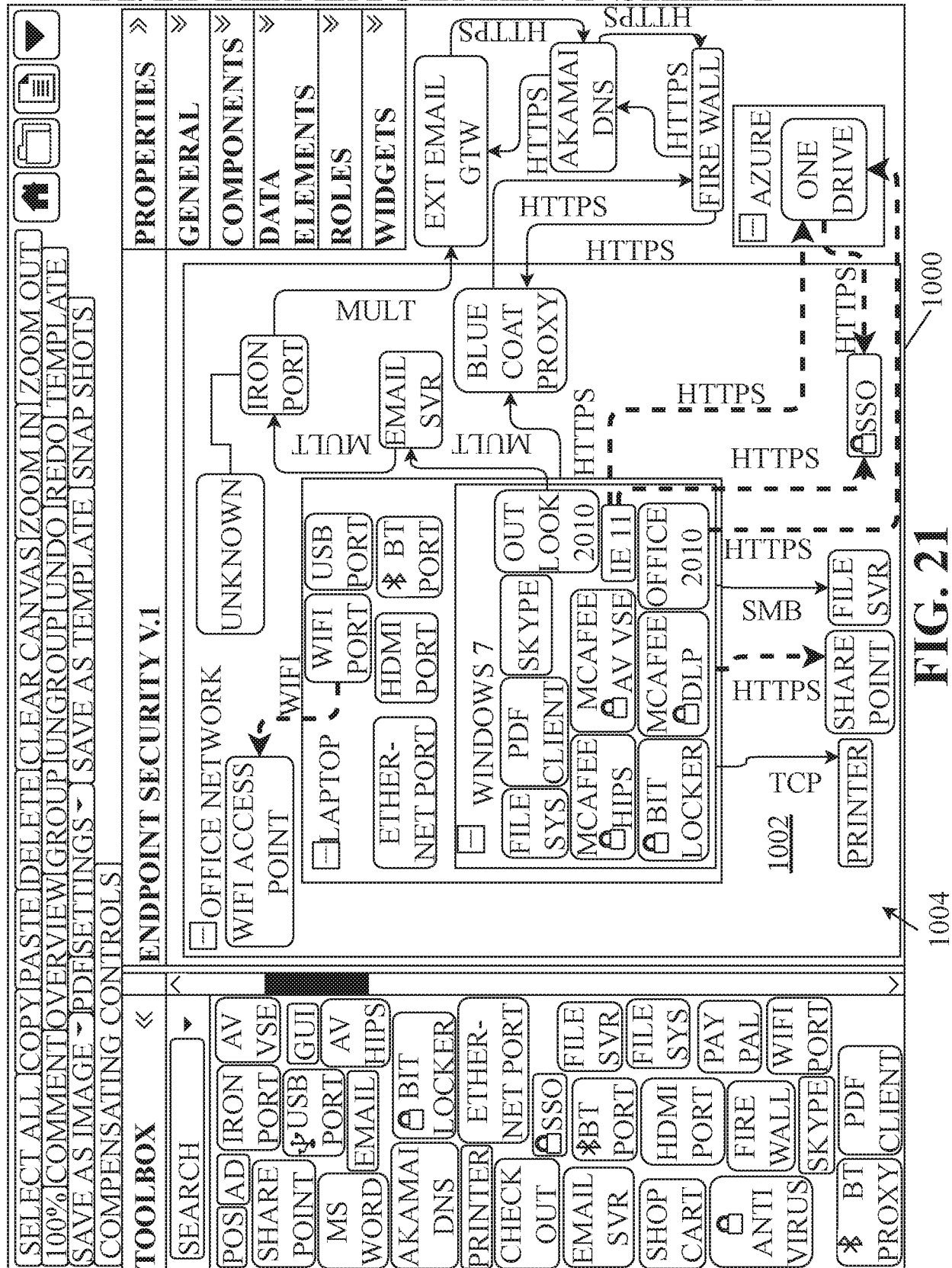


FIG. 21

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

Sep 21, 2020 03:39:21 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	COCOUT	09/21/2020	THREATM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

AMENDMENT/REPLY

Applicant: ThreatModeler Software Inc.

Docket No: THREATM008

Examiner: Song, Hosuk

Ser. No: 16228738

Filed: December 20, 2018

Group Art Unit: 2435

Title: Threat Model Chaining and Attack Simulation Systems and Related Methods

**RESPONSE TO CERTIFICATE OF CORRECTION BRANCH
COMMUNICATION**

Certificates of Correction Branch
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Examiner:

This is filed in response to the Certificate of Correction Branch communication dated 9/21/2020 requesting

Drawing Amendments begin on page 2.

Remarks/Arguments begin on page 3.

Drawing Amendments

The Certificate of Corrections Branch on Sep. 21, 2020 issued a request for a new set of drawings. It was unclear from this request whether only the drawings corrected by the certificate of correction were required, or whether all drawings were required. Accordingly, the following are submitted herewith:

1. A clean copy of the drawings, including the changes to FIGS. 10, 21 and 22 that were requested in the July 6, 2020 certificate of correction request.
2. A copy of just the replacement sheets each marked "Replacement Sheet" at the top.
3. A copy of Annotated Sheets highlighting the changes made, each marked "Annotated Sheet" at the top.

CONCLUSION

If it will in any way speed issuance of a certificate of correction, the examiner is invited to contact an attorney of record using the contact information listed below.

Respectfully submitted,

Date: September 21, 2020

By: /Paul B. Johnson/
Paul B. Johnson
Reg. No. 59375

Law Office of Paul B. Johnson
8483 S 1275 E
Sandy, UT 84094-1363
Ph: 801.719.5229
Fax: 801.317.8889
paul@pauljohnsonlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 10,699,008 B2
APPLICATION NO. : 16/228738
DATED : June 30, 2020
INVENTOR(S) : Anurag Agarwal

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

On the Title Page

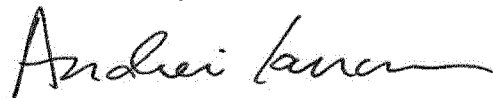
Column 2 in the abstract:

Line 2, change "including a threat model components" to -including threat model components-.
Line 5, change "associate with" to -associated with-.
Line 9, change "model include" to -model and include-.

In the Specification

Column 5, Line 55, change "compensated" to -compensating-.
Column 6, Line 30, change "compensatory" to -compensating-.
Column 15, Line 4, change "showing" to -shows-.
Column 16, Line 36, change "a cloud computing" to -cloud computing-.
Column 17, Line 35, change "popup threat" to -popup threat report-.
Column 18, Lines 2-3, change "a similar" to -an-.
Column 18, Line 3, change "to the" to -similar to the-.
Column 18, Line 39, change "list" to -lists-.
Column 20, Line 6, change "the component" to -component-.
Column 20, Line 12, change "ID a version" to -a CPE ID indicating a version-.
Column 23, Line 19, change "to" to -to/from-.
Column 23, Line 62, change "some sub-component" to -a sub-component-.
Column 23, Line 63, change "some element" to -an element-.
Column 27, Line 1, change "analyze" to -analyzing-.
Column 27, Line 3, change "analyze" to -analyzing-.
Column 27, Lines 4-5, change "measure and quantify" to -measuring and quantifying-.
Column 33, Line 50, change "functionality" to -the web page having functionality-.
Column 34, Line 33, change "is" to -includes-.

Signed and Sealed this
Sixth Day of October, 2020



Andrei Iancu
Director of the United States Patent and Trademark Office



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/228,738	12/20/2018	Anurag Agarwal	THREATM008	3702
145042	7590	11/17/2020	EXAMINER	
Law Office of Paul B. Johnson			SONG, HOSUK	
8483 S. 1275 E.				
Sandy, UT 84094-1363				
			ART UNIT	PAPER NUMBER
			2435	
			NOTIFICATION DATE	DELIVERY MODE
			11/17/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

paul@pauljohnsonlaw.com



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Patent No.: 10699008
Issue Date: 06/30/2020
Appl. No.: 16/228,738
Filed: 12/20/2018

PART (A) RESPONSE FOR CERTIFICATES OF CORRECTION

This is a decision on the Certificate of Correction request filed 21 September 2020.

The request for issuance of Certificate of Correction for the above-identified correction(s) under the provisions of 37 CFR 1.322 and/or 1.323 is hereby:

(Check one)

☒ Approved ☐ Approved in Part ☐ Denied

Comments: N/A

PART (B) PETITION UNDER 37 CFR 1.324 OR 37 CFR 1.48

☐ This is a decision on the petition filed _____ to correct inventorship under 37 CFR 1.324.

☐ This is a decision on the request under 37 CFR 1.48, petition filed _____. In view of the fact that the patent has already issued, the request under 37 CFR 1.48 has been treated as a petition to correct inventorship under 37 CFR 1.324.

The petition is hereby: ☐ Granted ☐ Dismissed

Comment: _____

The patented filed is being forwarded to Certificate of Corrections Branch for issuance of a certificate naming only the actual inventor or inventors.

/JOSEPH P HIRL/
Supervisory Patent Examiner, Art Unit 2435
Technology Center 2400
Phone: (571)272-3685

Certificates of Correction Branch email: CustomerServiceCoC@uspto.gov CoC Central Phone Number: (703) 756-1814



UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Patent No.: 10699008
Issue Date: 06/30/2020
Appl. No.: 16/228,738
Filed: 12/20/2018

PART (A) RESPONSE FOR CERTIFICATES OF CORRECTION

This is a decision on the Certificate of Correction request filed 21 September 2020.

The request for issuance of Certificate of Correction for the above-identified correction(s) under the provisions of 37 CFR 1.322 and/or 1.323 is hereby:

(Check one)

☒ Approved ☐ Approved in Part ☐ Denied

Comments: N/A

PART (B) PETITION UNDER 37 CFR 1.324 OR 37 CFR 1.48

☐ This is a decision on the petition filed _____ to correct inventorship under 37 CFR 1.324.

☐ This is a decision on the request under 37 CFR 1.48, petition filed _____. In view of the fact that the patent has already issued, the request under 37 CFR 1.48 has been treated as a petition to correct inventorship under 37 CFR 1.324.

The petition is hereby: ☐ Granted ☐ Dismissed

Comment: _____

The patented filed is being forwarded to Certificate of Corrections Branch for issuance of a certificate naming only the actual inventor or inventors.

/JOSEPH P HIRL/
Supervisory Patent Examiner, Art Unit 2435
Technology Center 2400
Phone: (571)272-3685

Certificates of Correction Branch email: CustomerServiceCoC@uspto.gov CoC Central Phone Number: (703) 756-1814

To: paul@pauljohnsonlaw.com,,
From: PAIR_eOfficeAction@uspto.gov
Cc: PAIR_eOfficeAction@uspto.gov
Subject: Private PAIR Correspondence Notification for Customer Number 145042

Nov 18, 2020 03:49:50 AM

Dear PAIR Customer:

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363
UNITED STATES

The following USPTO patent application(s) associated with your Customer Number, 145042 , have new outgoing correspondence. This correspondence is now available for viewing in Private PAIR.

The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

Disclaimer:

The list of documents shown below is provided as a courtesy and is not part of the official file wrapper. The content of the images shown in PAIR is the official record.

Application	Document	Mailroom Date	Attorney Docket No.
16228738	COCX	11/17/2020	THREATM008

To view your correspondence online or update your email addresses, please visit us anytime at <https://portal.uspto.gov/secure/myportal/privatepair>.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov with 'e-Office Action' on the subject line or call 1-866-217-9197 during the following hours:

Monday - Friday 6:00 a.m. to 12:00 a.m.

Thank you for prompt attention to this notice,

UNITED STATES PATENT AND TRADEMARK OFFICE
PATENT APPLICATION INFORMATION RETRIEVAL SYSTEM

UNITED STATES PATENT AND TRADEMARK OFFICE
COMMISSIONER FOR PATENTS
P.O.BOX 1450
ALEXANDRIA VA 22313-1451

PRESORTED
FIRST-CLASS MAIL
U.S. POSTAGE PAID
POSTEDIGITAL
NNNNN

Law Office of Paul B. Johnson
8483 S. 1275 E.
Sandy, UT 84094-1363



**Courtesy Reminder for
Application Serial No: 16/228,738**

Attorney Docket No: THREATM008

Customer Number: 145042

Date of Electronic Notification: 11/18/2020

This is a courtesy reminder that new correspondence is available for this application. If you have not done so already, please review the correspondence. The official date of notification of the outgoing correspondence will be indicated on the form PTOL-90 accompanying the correspondence.

An email notification regarding the correspondence was sent to the following email address(es) associated with your customer number:

paul@pauljohnsonlaw.com

To view your correspondence online or update your email addresses, please visit us anytime at **<https://ppair-my.uspto.gov/pair/PrivatePair>**.

If you have any questions, please email the Electronic Business Center (EBC) at EBC@uspto.gov or call 1-866-217-9197.

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 10,699,008 B2
APPLICATION NO. : 16/228738
DATED : June 30, 2020
INVENTOR(S) : Anurag Agarwal

Page 1 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

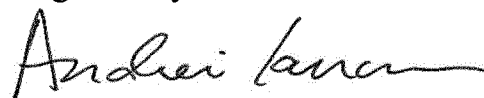
In the Drawings

In FIG. 10, the rightmost line connecting the “AKAMAI DNS” component with the “FIRE WALL” component should have the end arrow pointing at the “FIRE WALL” component as shown on the attached drawing sheet.

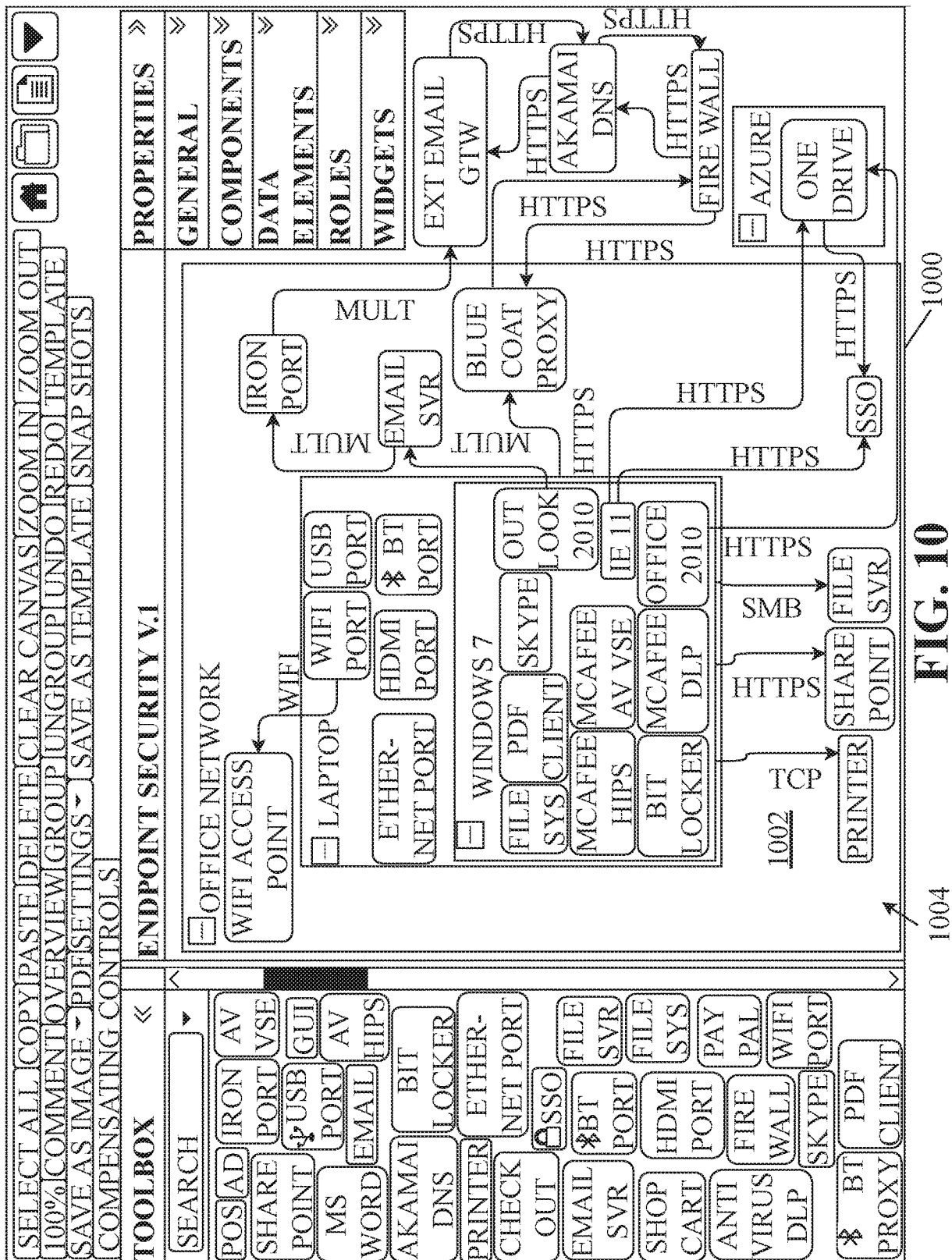
In FIG. 21, the rightmost line connecting the “AKAMAI DNS” component with the “FIRE WALL” component should have the end arrow pointing at the “FIRE WALL” component as shown on the attached drawing sheet.

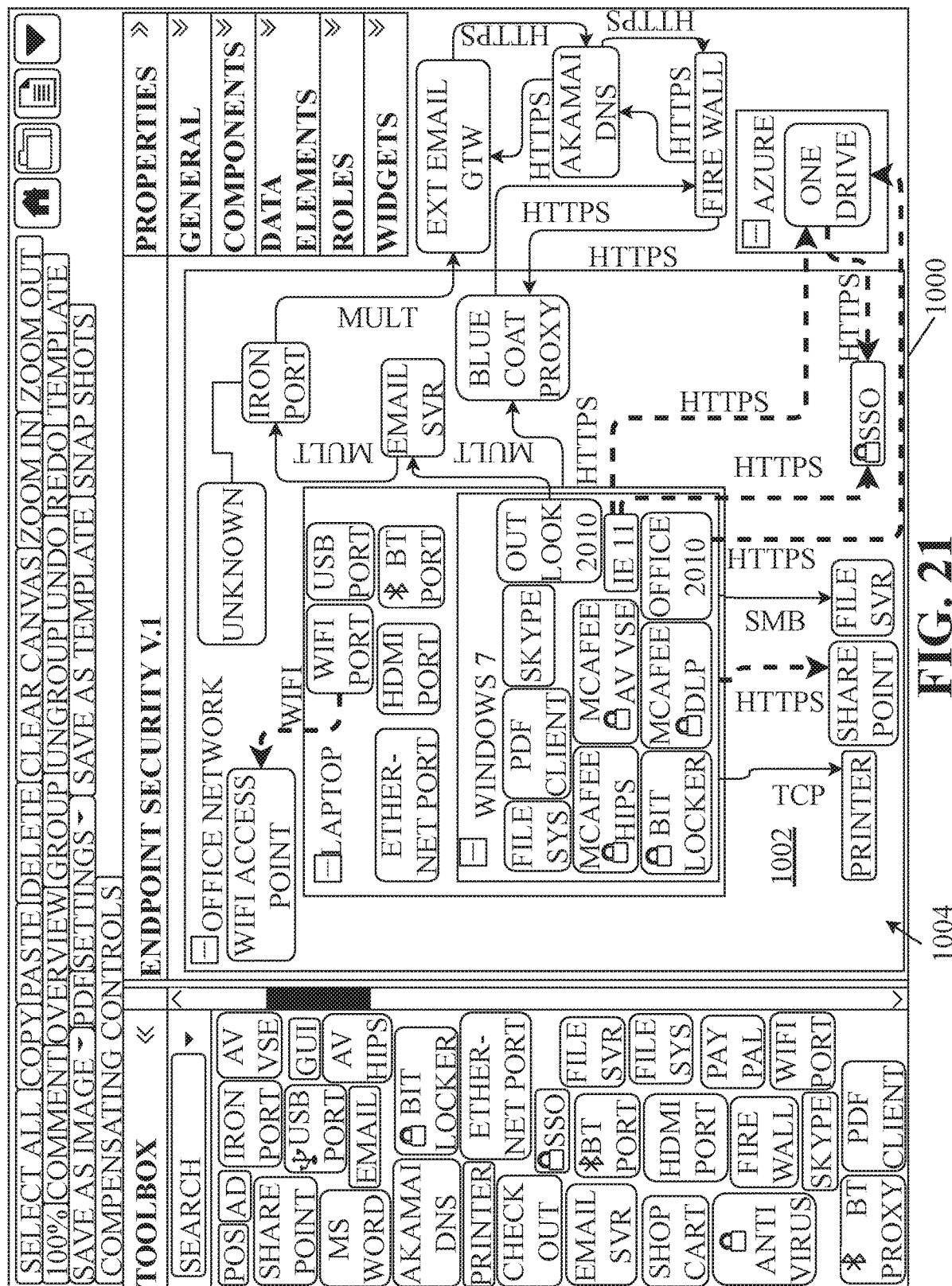
In FIG. 22, the rightmost line connecting the “AKAMAI DNS” component with the “FIRE WALL” component should have the end arrow pointing at the “FIRE WALL” component as shown on the attached drawing sheet.

Signed and Sealed this
Eighth Day of December, 2020



Andrei Iancu
Director of the United States Patent and Trademark Office





U.S. Patent

Jun. 30, 2020

Sheet 22 of 22

10,699,008 B2

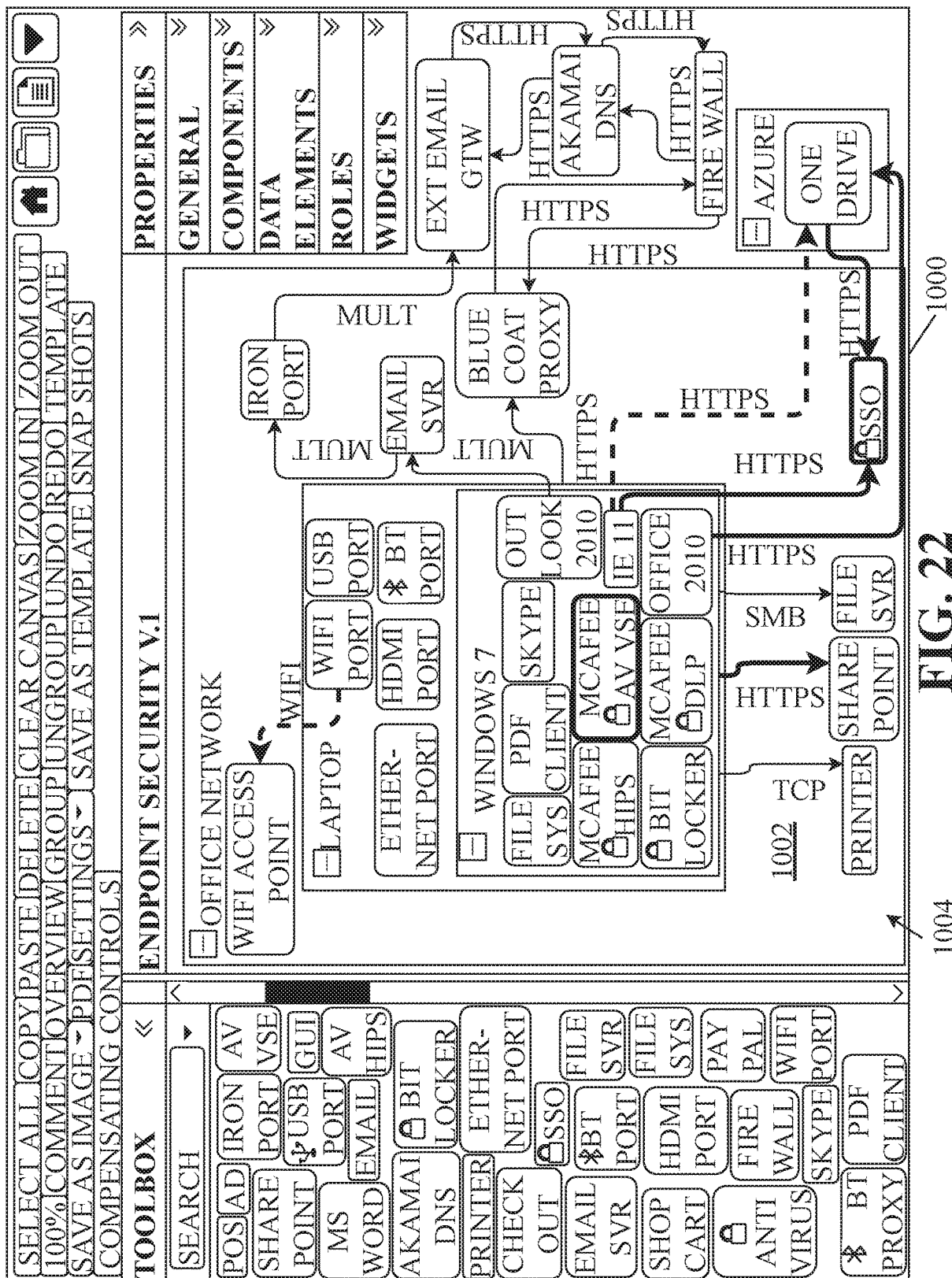


FIG. 22

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
---	---

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been
filed in the U.S. District Court _____ for the District of Delaware _____ on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292);

DOCKET NO.	DATE FILED 7/8/2022	U.S. DISTRICT COURT for the District of Delaware
PLAINTIFF THREATMODELER SOFTWARE INC.		DEFENDANT IRIUSRISK, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 US 10,699,008 B2	6/30/2020	ThreatModeler Software Inc.
2 US 10,713,366 B2	7/14/2020	ThreatModeler Software Inc.
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE
-------	-------------------	------

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy