

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE, INC.,
Patent Owner.

Case IPR2023-00656
Patent 10,713,366

PATENT OWNER RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	BACKGROUND	3
	A. Priority Date of the ‘366 Patent.....	3
	B. Overview of the ‘366 Patent.....	4
	C. File History of the ‘366 Patent	10
III.	SUMMARY OF REFERENCES	11
	A. U.S. Patent No. 11,200,228 (“Keenan”).....	11
	B. U.S. Patent No. 10,503,907 (“Zheng”).....	15
	C. U.S. Patent Pub. 2014/0236665 (“Baker”).....	16
	D. U.S. Patent No. 9,602,529 (“Jones”).....	17
	E. U.S. Patent No. 10,681,068 (“Galliano”)	17
IV.	CLAIM CONSTRUCTION.....	17
	A. “Threats”	18
	B. “Threat Model Components”	25
	C. “Visual Representations of the Threat Model Components”	26
	D. “Mapping Files”	28
V.	THE CHALLENGED CLAIMS ARE NOT UNPATENTABLE	29
	A. Ground 1: Keenan Does Not Anticipate the Challenged Claims	29
	1. Keenan Does Not Disclose the Claimed “Threats”	29
	2. Keenan Does Not Disclose the Other “Threat” Claim Terms Including “Threat Model,” “Threat Model Components,” “Visual Representations of the Threat Model Components,” or “Threat	

Report”	39
3. Keenan Does Not Disclose Dependent Claims 2, 3, 9, 10, 17, or 18	41
4. Keenan Does Not Disclose Dependent Claim 5	44
5. Keenan Does Not Disclose Claims 6 and 14	45
6. Keenan Itself Is Not Prior Art and the Petition Made No Attempt to Show that the Cited Portions of Keenan Qualify As Prior Art.....	47
B. Ground 2: Alleged Obviousness of Claims 1-4, 7-11, 15-18 over Zheng In View of Baker and Jones	49
C. Grounds 3-5: Alleged Obviousness of: (1) Claims 2, 9, and 17 over the Combination of Zheng, Baker, Jones, and Galliano (<i>i.e.</i> , Ground 3); (2) Claims 1–20 over the Combination of Zheng, Baker, Jones, and Keenan (<i>i.e.</i> , Ground 4); and (3) Claims 2, 5-6, 9, 12–14, 17, and 19-20 over the Combination of Zheng, Baker, Jones and “the knowledge of a POSITA” (<i>i.e.</i> , Ground 5).....	52
VI. CONCLUSION	54

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Ex parte Levy</i> , 17 USPQ2d 1461 (Bd. Pat. App. & Inter. 1990)	38
<i>In re Oelrich</i> , 666 F.2d 578, 212 USPQ 323 (CCPA 1981)	38
<i>In re Rijckaert</i> , 9 F.3d 1531, 28 USPQ2d 1955 (Fed. Cir. 1993)	38
Statutes	
35 U.S.C. §102	47
35 U.S.C. §102(d)	47
35 U.S.C. §102(d)(2).....	48
35 U.S.C. § 103	52
Regulations	
37 C.F.R. § 42.105	56
37 C.F.R. § 42.24(b), (c) and (d)	55
37 C.F.R. § 42.6	56

PATENT OWNER’S EXHIBIT LIST

Exhibit No.	Description
EX-2001	Patent Owner’s December 4, 2023 Power of Attorney
EX-2002	Transcript of Robert Hurlbut Deposition taken December 18, 2023
EX-2003	CIO Article dated August 23, 2016
EX-2004	Draft NIST Special Publication 800-154 entitled “Guide to Data-Centric System Threat Modeling,” March 2016
EX-2005	Excerpts from <i>Measuring and Managing Information Risk, A FAIR Approach</i> , by Jack Freund and Jack Jones, 2015
EX-2006	NIST Special Publication 800-30, Rev. 1, entitled “Guide for Conducting Risk Assessments, Sept. 2012
EX-2007	Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, April 6, 2015
EX-2008	Excerpts from <i>Threat Modeling</i> by Frank Swiderski and Window Snyder, 2004
EX-2009	Declaration of Seth James Nielson, Ph.D.

I. INTRODUCTION

The Board should deny IriusRisk Inc.’s (“IriusRisk” or “Petitioner”) Petition against Claims 1-20 (collectively, “the Challenged Claims”) of the ‘366 Patent (EX-1001). The ‘366 Patent discloses and claims a novel and non-obvious threat modeling system and method in which various threats are associated with one or more threat model components in a database. The system and method read a data file from a third party software application to discern the third party diagram components in the data file. The system and method correlate the third party diagram components with one or more threat model components and generate a threat report. IriusRisk’s Petition does not establish a reasonable likelihood that the Challenged Claims are anticipated or obvious, and that they should be cancelled.

Petitioner’s primary ground relies on U.S. Patent No. 11, 200,228 (“Keenan”) as an anticipatory reference against all Challenged Claims. Keenan is directed to risk analysis – not threat modeling. Keenan never discloses threats, or the use and storage of threats, as required by the claims of the ‘366 Patent. Petitioner argues that Keenan discloses risk and the threat can be determined from that risk – *i.e.*, Petitioner makes an inherency argument. Although there may be a relationship between threats and risk, threats and risk are distinct concepts. The

intrinsic and extrinsic evidence demonstrates the differences between risk and threats, and establishes that knowing the risk does not allow one to determine the threat that may have given rise to the risk. Figure 8 of the '366 Patent, for example, shows multiple threats having the same risk. Thus, knowing that the risk is “very high,” for example, does not determine which threat gave rise to the risk.

Patent Owner provides multiple, contemporaneous texts that show that those of skill in the art at the time of the '366 Patent recognized that risk and threats were distinct concepts. Even Petitioner's expert, Robert Hurlbut, admitted at his deposition that knowing risk does not allow one to determine the corresponding threat, if any. Because Keenan does not expressly or inherently disclose threat, or the storage and usage of threats, as recited in the Challenged Claims, Keenan does not anticipate any of the Challenged Claims.

Patent Owner provides additional reasons why Keenan does not anticipate at least dependent claims 2, 3, 5, 6, 9, 10, 14, 17, and 18.

Moreover, Petitioner failed to establish a *prima facie* case of anticipation. Keenan itself is not prior art against the '366 Patent. For Keenan to qualify as prior art, Petitioner was required to establish that the relevant teachings of Keenan were entitled to its provisional filing date. Petitioner made no effort to establish that foundation.

With respect to Grounds 2-5 of the Petition, the Board correctly found in its Institution Decision that there are deficiencies in the prior art references relied upon by Petitioner. For example, Zheng does not teach or suggest a “mapping file” that correlates threat model components to third party diagram components. Zheng uses the term “map” consistently in the context of cartography, *i.e.*, creating a digital view of components and their interconnections (like drawing a map of how computer network components are interconnected). Baker’s process has no need or use for any “mapping files” as claimed. Instead, Baker simply searches for a flowchart shape without disclosing any “mapping files” providing correlations as recited in the claims. Moreover, the combination of references relies on improper hindsight as the basis of the combination.

As further explained in the Institution Decision, for the remaining references relied upon in Grounds 2-5, none of those references are relied upon to remedy the deficiencies found in Zheng and Baker.

The Board should determine that Petitioner has not shown that any of the Challenged Claims are unpatentable.

II. BACKGROUND

A. Priority Date of the ‘366 Patent

The U.S. Patent Application No. 16/542,263 (“the ‘263 Application”) was

filed on August 15, 2019. The ‘263 Application issued as the ‘366 patent on July 14, 2020. The ‘263 Application claims priority to four U.S. Provisional Applications, the earliest of which was filed on May 17, 2017. EX-1001, 1-2.

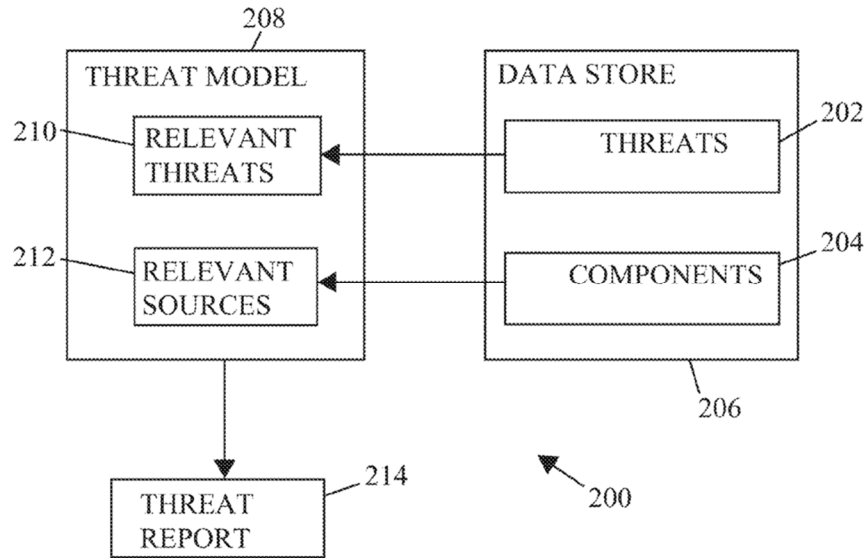
IriusRisk’s petition for *inter partes* review and Mr. Hurlbut’s expert opinions are based on the May 17, 2017 priority date of the ‘366 Patent. (Petition, 8; EX-1003, ¶45). Accordingly, this Patent Owner Response assumes the ‘366 Patent has a priority date of May 17, 2017.

B. Overview of the ‘366 Patent

The ‘366 Patent is entitled “Systems and Methods for Automated Threat Modell Generation from Third Party Diagram Files” and relates to threat modeling systems and processes. EX-1001, cover page. The ‘366 Patent explains that “[t]hreat modeling is a process by which vulnerabilities of a system or process may be detailed and prioritized.” EX-1001, 1:56-57.

Threat modeling can be applied to a broad range of environments or activities. EX-1001, 1:62-66. “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.” EX-1001, 2:3-7.

Figure 2 of the '366 Patent is one example of a threat modeling process of the invention that is applicable to any application, process, or system under consideration. EX-1001, 8:65-9:1.



The '366 Patent explains that threat models are created from defined threats and threat model components, which are stored within a database. *Id.*, 9:10-16 (“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.”). 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.” ’366 Pat., 10:8-12.

“[E]ach asset could have any number of threats that could threaten to compromise it. ... Some assets may be threatened by only a single threat, some may be threatened by two or three threats, or more, and so forth.” ’366 Pat., 24:26-32.

One obstacle to widespread use of threat modeling techniques and tools has been creation of the threat model objects and relationships between the objects within the context of a threat model, *i.e.* creation of the threat model itself, which can be a laborious project (especially within large and complicated systems, such as networked enterprise computing platforms. EX-2009, ¶57.

Typically, an enterprise will have some sort of model of their computing platforms, such as for inventory, troubleshooting, and the like. However, such reports lack information relating to threats and threat relationships between elements. As noted at ’366 Pat., 2:47-49 “[s]oftware exists for converting a diagram file of one type to another type of diagram file, though not into a threat model.” In other words, at the time of filing the ’366 patent there was a need for a tool to convert existing diagrams into threat models that include the necessary elements and relationships of threat models. The challenged claims are directed generally to a software-based threat modeling system or method that “may be able to take any diagram, in any file format, and convert it into a threat model.” ’366 Pat., 43:9-11; EX-2009, ¶58.

As noted by Petitioner, conventionally, specific diagrams, such as Data Flow Diagrams, were required to produce a threat model. The Data Flow Diagram at EX-1003, Paragraph 35, is specific to the use case and requires identifying Actors, Processes, Data Stores or Assets, and Data Flows of the specific use case. *See* Petition at pp. 5-6. Petitioner states that “[t]he Data Flow Diagram helps identify potential threat actors (Customer, Thief) and various countermeasures to create an initial threat model known in the art before the ’366 patent’s priority date. EX-2011-2014; EX-1003, ¶¶35-37.” While data flow diagrams do help identify potential threat actors, this statement overly simplifies the complex process required to create a threat model from a Data Flow Diagram. For example, threats, *i.e.*, potential events that, if they occurred, would have an adverse effect on a specified asset, must be identified and correlated with the assets. Then the threats must be considered within the context of the data flow of the Data Flow Diagram. EX-2009, ¶59.

The claimed invention leverages two novel data structures of: (1) threat model components stored in a database in association with “threats”; and (2) “a mapping file which correlate the threat model components with visual diagram components of a third-party software application. These two data structures, when used in the claimed manner, provide a mechanism for correlating a visual diagram

to threats to thereby allow creation of a threat model from existing visual diagrams (such as network architecture diagrams). Note that the threat model components, as stored in the database are not part of a threat model, but can be correlated to elements in a diagram, to define a threat model. EX-2009, ¶60.

Referring to Figure 2, a user selects from among the available components those components which are relevant to any given system, process or application being examined. This process is represented by the arrow between the components 204 and the relevant sources 212. The relevant sources are the sources determined by the system 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 databased where the threats and components are stored the threats that were previously correlated with the components to form the threat model 208. The threat model includes the relevant threats and the relevant sources of those threats. The threat model can be used to generate a threat report 214. EX-2009, ¶61.

The '366 Patent describes each "threat model component" as "a potential relevant source for one or more threats." EX-1001, 9:55-57. One example provided in the specification is that one threat may be "Bluejacking," in which a potential attacker may seek to gain improper access to a system via its Bluetooth

interface. In this example, the threat model component is the “Bluetooth port,” *i.e.*, the potential source of the threat. EX-1001, 9:55-59. As another example, an “online banking interface” may be stored as a threat model “component,” and “a threat may be a virus being introduced to the bank’s environment through a breach in the banking interface.” ’366 Pat., 24:64-25:1; EX-2009, ¶62.

The challenged claims of the ’366 Patent recite a “database,” and in claim 1, the database comprises, in relevant part, “a plurality of threat model components stored therein; and a plurality of threats stored therein, wherein each of the threats is associated with at least one of the threat model components through the one or more databases.” Independent claims 8 and 16 include substantially similar features. As claimed, the “database” does not simply store a numeric value as a property or characteristic of a component. Instead, the one or more databases expressly stores “a plurality of threats,” and associates each of the threats with “at least one of the threat model components through the one or more databases.” EX-2009, ¶63.

Further, the ’366 Patent expressly distinguishes between “threats” and the concept of “risk.” “[A]n 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.” ‘366 Pat., 25:8-12. As discussed further below, a “threat” may be associated with a risk level as disclosed in Figure 8 and the specification, but a risk level is different from a threat. Describing Figure 8, the ‘366 Patent explains, “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.” ‘366 Pat., 14:5-9. Exemplary risk levels are relative values, *i.e.*, very high, high, or medium, but risk levels do not disclose threats to the system’s components. ‘366 Pat., FIG. 8; 25:20-26; EX-2009, ¶¶64.

C. File History of the ‘366 Patent

The ‘366 Patent was filed as U.S. Patent Application No. 16/542,263 (“the ‘263 application”) on August 15, 2019. EX-1002. The ‘366 Patent issued on July 14, 2020 after the Examiner found that the cited prior art did not disclose “determining using the one or more computing devices, for the subset of third party diagram components, correlated threat model components as defined in the one or more mapping files,” as recited in the context of claim 1. EX-1002, p.516. The cited art also did not disclose “the one or more mapping files correlating the threat model components with visual diagram components of a third party software application,” as recited in the context of claim 1. EX-1002, p.517. The Examiner found that the cited art did not disclose the corresponding features of independent

claims 8 and 16, and that the dependent claims were patentable because of their dependence from the independent claims. EX-1002, p.517.

III. SUMMARY OF REFERENCES

The Petitioner requests review of the ‘366 Patent on the following grounds:

Ground	Claims	Statutory Basis	Alleged Prior Art
1	1-20	§102	Keenan
2	1-4, 7-11, 15-18	§103	Zheng in view of Baker and Jones
3	2, 9, 17	§103	The references of Ground 2 in further view of Galliano
4	1-20	§103	The references of Ground 2 in further view of Keenan
5	2, 5-6, 9, 12-14, 17, 19-20	§103	The references of Ground 2 in further view of the knowledge of a POSITA

Petition, 12.

A. U.S. Patent No. 11,200,228 (“Keenan”)

Keenan relates to risk management – not threat modeling. Keenan was filed by and assigned to an insurance company: American International Group, Inc. Keenan assigns a risk value to certain aspects of a system, but the threats underlying that risk value are neither determined by Keenan nor important to Keenan. The purpose of Keenan is to provide a view that allows a user to see (via

a “view”) an overall risk level associated with an infrastructure for business and insurance purposes, not to detail or prioritize vulnerabilities or threats. EX-2009,

¶67. Keenan makes this clear in the specification:

Design of object classifications is suited to capture the properties of the information assets in a way that associates the risk, cost, quality, accountability of the assets to the product chain that produces calc[ulation]s which the business utilizes *to set premiums and reserves, manage investment risk and produce financial reports and compliance reports.*

Keenan, 1:33-38 (emphasis added).

Keenan refers to the “risk” as a property. Keenan, 1:42 (“[t]hese properties (e.g. costs, risks and accountability)”). Keenan also refers to the risk as a “value.” For example, in Table 3 in its specification, Keenan discloses that the PALETTE view name includes an option called Model Risk. Keenan, 14:32-38. Under this view and option, an object shape’s color is “based on the *value* of the risk characteristics for the models in the view.” *Id.* (emphasis added). Keenan also refers to “risk” as a characteristic that is “preset.” Keenan, 16:4-5. Keenan views may “fill[] the object shapes based on the *value* of the technical risk ranking characteristics of that object.” Keenan, 16:21-23 (emphasis added). These disclosures support only that “risk” in Keenan is a preset value as property of an object, and does not identify any “threats” as claimed. EX-2009, ¶68.

Keenan further teaches that “risk” is a calculated value. Keenan teaches that:

The GUI also preferably includes an option for calculating and displaying the Riskiest Path. The user selects one of the risk metrics and the IOE computes based on pre-loaded formulae the path with the highest risk based on the metric selected by the user. The riskiest path will appear highlighted (e.g., in red) as seen in FIG. 11. A sample list of risk metrics include: Model Risk without exposure; Model Risk with exposure; Data Quality; Ops Risk; Tech Risk; and Aggregated Risk.

EX-1004, 17:44-52. Further, Keenan discloses that a user can “calculate the risk of the selected View,” and even the “Calculate Aggregate risk by View” report “depicts risk values of the objects of the View aggregated based on an *aggregation formula*.” Keenan, 18:6-8, 18:20-22 (emphasis added); EX-2009, ¶69.

Keenan teaches that different “views” can display colors according to different properties, including the risk level, associated with various objects. EX-2009, ¶70. Keenan teaches:

The system may permit user-defined dimensions in the case of special Views. For instance, a shape fill color may represent platform association in the default view, but represent model risk in a specific Palette View (see below). The number of characteristic or sub-class values possible for each visual

component is thus limited only by the differences the normal human eye can detect on today's screens.

EX-1004, 13:16-22. Keenan further states that “[a] shape’s fill color may depict model risk levels in model objects when selecting the model risk palette View.”

EX-1004, 13:41-42 (emphasis added). Similarly, the Technical Threat Vector palette View is described as “color fills the object shapes based on the value fo [sic: of] the technical risk ranking characteristic of that object.” EX-1004, 14:61-63 (emphasis added); also 16:21-23. The Operational Risk palette View is described as “colors fills the object shapes based on the value of operational risk characteristic of the object or its associated control.” EX-1004, 14:64-67 (emphasis added); also 16:27-29. Keenan’s “risk” is a risk value or risk level. EX-2009, ¶70.

Indeed, Keenan discloses using the risk values in formulas to calculate aggregate risk, thereby confirming that risk is simply a number, and neither discloses nor informs anything about any “threats” as claimed. As disclosed, Keenan allows a user to “calculate the risk of the selected View,” and even the “Calculate Aggregate risk by View” report “depicts risk values of the objects of the View aggregated based on an aggregation formula.” EX-1004, 18:6-8, 18:20-22 (emphasis added); EX-2009, ¶71.

Keenan’s alerts can inform an owner of a change in risk, but this is also

based on formulas and values, not “threats.” Keenan discloses that “[c]hanges to characteristics can also include formulas that calculate risk parameters based on new raw values put into ... characteristics of one object but flow downstream to other objects.” EX-1004, 20:34-37. “Entire paths are preferably monitored for changes to aggregate characteristics values.” EX-1004, 20:37-38. This disclosure indicates that a risk value or parameter can be changed by a user, *e.g.*, from 5 to 6, and that new value can require recalculations of the formulas using that value as an input. Keenan’s risk is a numeric value as a property or characteristic. EX-2009, ¶72.

B. U.S. Patent No. 10,503,907 (“Zheng”)

Although Zheng relates to threat modeling, the portions and teachings from Zheng relied upon in the Petition do not support the conclusion that Zheng discloses certain claim elements of the ‘366 Patent (*e.g.*, the “mapping files”). As stated in the Institution Decision, Zheng discloses a system comprising “a visualization module for *rendering, on a computer display, a map* with components representative of the suite of software applications and relationships among the software applications,” where “[t]he components are *displayed* in a base layer of *the map*.” EX-1005, 1:48–53 (emphases added). Zheng explains that, “by utilizing *a visualization approach like cartography*, application architecture can be

represented in a compressible view that enhances security and risk analysis,” and that “*mapping techniques* and concepts can be used *in the context of data visualization* to create a graphical representation of application connectivity and security.” *Id.* at 3:28–34 (emphases added). On its face, Zheng appears to use the term “map” consistently in the context of cartography, *i.e.*, creating a digital view of components and their interconnections (like drawing for someone a map of how computer network components are interconnected). Institution Decision, 25-26. Zheng does not disclose “mapping techniques” in the context of “correlating” component, specifically correlating claimed “threat model components with visual diagram components of a third party software application,” as recited, for example, in claims 1, 8, and 16 of the ‘366 Patent claims. EX-2009, ¶73.

C. U.S. Patent Pub. 2014/0236665 (“Baker”)

Baker is directed to an “automated risk management system.” EX-1006, ¶1. Baker does not disclose the use of “mapping files,” as argued in the Petition. Instead, Baker stores the “text and shape of each element of the flowchart . . . in the process database 30” and “automatically assign[s] or associate[s] predetermined objectives or controls according to the shapes of the imported flowcharts.” EX-1006, [0025]; *see also id.*, [0009]. Baker simply searches for a flowchart shape without disclosing any “mapping files” providing correlations as

recited in the claims. EX-2009, ¶74.

D. U.S. Patent No. 9,602,529 (“Jones”)

Jones discloses that “[t]he reporter may be configured to generate one or more reports from the threat analysis, at least one of which may include an organized arrangement of at least some of the attributes of at least some of the components, data flows or cybersecurity threat.” EX-1007, 6:59-63 (emphasis added). EX-2009, ¶75.

E. U.S. Patent No. 10,681,068 (“Galliano”)

The Petition relies on Galliano for allegedly disclosing the elements of Claims 2, 9, and 17. In essence those claims recite “wherein the one or more mapping files are not stored in the one or more databases but are stored in the one or more computing devices.” EX-1001, claim 2. The sole portion of Galliano cited by the Petition is Figure 3 which states that the “[m]odel is either stored in a back-end repository (ex. database) or in memory within a computing system.” EX-1008, Figure 3. No other portion of Galliano that elaborates further on this statement. The cited portion of Galliano does not disclose “mapping files” or where they may be stored. EX-2009, ¶76.

IV. CLAIM CONSTRUCTION

In the Institution Decision, the Board invited the parties to address the proper construction of the following claim terms: “threats”, “threat model

components,” “visual representations of the threat model components,” and “mapping files.” Institution Decision, 12. Each of those terms are addressed below. Because Keenan relates to “risk,” the different meanings of “threats” and “risk” are addressed in the “threats” section below.

A. “Threats”

The specification of the ‘366 Patent does not provide an express definition of the word “threat.” Nevertheless, “threat” is a term of art within the field of threat modeling. The term “threat” should be construed to mean “one or more potential events that, if they occur, can cause adverse effects to a target system.” EX-2009, ¶78.

The specification of the ‘366 Patent provides examples of “threats.” For example, Figure 6 shows a list of threat model components under the “components” heading. EX-1001, 11:54-12:26. When a user clicks on one of the components, such as the “login” component, its corresponding properties are shown in the panel on the right hand side. Under the properties heading, the section labeled “threat” shows each of the threats that correspond to the “login” component. In this case, the “login” threat model component has the following threats: inducing account lockout, session hacking, and click jacking. If any of those potential events occur, the event would have an adverse effect on the system.

EX-2009, ¶79.

Figure 8 shows a view of the “threats” sub-menu. The threats listed in this figure include buffer overflow, session hijacking, physical theft, etc. Again, if any of those potential threats occur, the threat would have an adverse effect on the system. Note that in Figure 8 that “threats” and “risk” are distinct concepts. A “threat” is a potential event. Whereas “risk” is the potential impact on a system due to a threat that occurs coupled with the likelihood that a threat will occur. The terms “risk” and “risk level” are used synonymously in the ‘366 Patent, as they are typically used in the threat modeling field. In Figure 8, the “risk” for the various threats are categorized as medium, high, or very high. There is not necessarily a one-to-one correspondence between “threats” and “risk.” Indeed, the same threat can have different risk levels depending on the system in which the threat may occur. Similarly, knowing the risk level does not identify a particular threat. In Figure 8, a “very high” risk could correspond to any one of six different threats.

EX-1001, Fig. 8; EX-2009, ¶80.

Petitioner’s expert agreed that knowing risk does not allow one to necessarily determine the threat that may have caused the risk and that there was not a one-to-one relationship between risk and threats. Mr. Hurlbut testified that:

Q. Okay.

But if you are just given the
risk, can you derive the threat from that?

MR. MIDDLETON: Objection.
Form.

A. You have -- well, some possible
threats. Some possible threats. And I gave
an example already. The example I gave was
unavailability. I have a risk of
unavailability. But what's the threat?
Well, the threat could be several things.
It could be a denial-of-service attack, it
could be the thing I'm relying on is not
available to me. So, therefore, I have that
risk, and so I don't have exactly a one to
one, but I certainly have a pretty good idea
of what it could be, so I've narrowed down
my possibilities.

EX-2002 [Hurlbut depo], 61:7-24; *see also* 64:14-25, 66:2-9; EX-2009, ¶81.

Figures 11 and 12 of the '366 Patent also show multiple threats, the potential
“source” of those threats (which correspond to the claimed “threat model

components”), and the risk associated with each threat in the context of the system being examined. Again, there is no one-to-one relationship between a threat and its associated risk. Knowing a particular risk (or risk level) does not identify or determine a particular threat. EX-2009, ¶82.

The article “Threat Modeling Approaches for Securing Cloud Computing” was submitted to the Patent Office during prosecution of the ‘366 Patent. EX-1002, 480-495. That article includes definitions of both “threat” and “risk.” “Threat” is defined as “harm or unauthorized access that might occur due to vulnerability and destroy organization assets, organization operations or system information.” EX-1002, 482. The article cites to the Open Web Application Security Project (“OWASP”) in which “risk” is defined as “Risk = Likelihood x Impact.” EX-1002, 493. “Likelihood” is the probability that a threat may occur, and “impact” is the damage that may occur to a system or organization if the threat occurs. EX-2009, ¶83.

The extrinsic evidence is consistent with Patent Owner’s construction of “threat” – *i.e.*, one or more potential events that, if they occur, can cause adverse effects to a target system. For example, the Draft National Institute of Standards and Technology (“NIST”) Special Publication 800-154, Guide to Data-Centric System Threat Modeling (hereafter, “NIST 800-154”), is a well-accepted and

widely-consulted standard in the field of threat modeling. EX-2004. NIST 800-154 references NIST Special Publication 800-30 (hereafter, “NIST 800-30”) which defines “threat” as:

any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

EX-2006, B-13 [NIST 800-30] (emphasis added); EX-2009, ¶84. NIST 800-30 also defines “risk” as:

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

EX-2006, B-9 [NIST 800-30]. Using these definitions, a “threat” is the “circumstance or event.” The “risk” is the “measure of the extent to which an entity is threatened” by the threat. “Risk” is a function of the impact of the potential threat (if it were to occur), and the likelihood that the threat may occur.

EX-2009, ¶84; *see also* EX-2007 at 109 and 127 [Committee on National Security Systems Instruction (CNSSI) 4009, National Information Assurance (IA)] (same

definition of “risk”).

Another well-known reference is “Measuring and Managing Information Risk: A FAIR Approach” by Jack Freund and Jack Jones (“FAIR”). This book relies on the Factor Analysis of Information Risk (FAIR) standard (<https://www.fairinstitute.org/>). FAIR notes that “[a] reasonable definition for threat is anything (e.g., object substance, human, etc.) that is capable of acting in a manner that can result in harm.” EX-2005 [FAIR], 4. FAIR defines “risk” as “[t]he probable frequency and probable magnitude of future loss.” EX-2005 [FAIR], 5; EX-2009, ¶85.

Similarly, an August 23, 2016 article in CIO magazine was entitled “Risk = Likelihood x Impact.” EX-2003 [CIO article]. That article explained that “the total amount of risk exposure is the probability of an unfortunate event occurring, multiplied by the potential impactor damage incurred by the event.” EX-2003 [CIO article], 2. The “event” corresponds to a “threat,” whereas the “risk” is a calculated value that may be derived from a threat assuming that the likelihood and impact of the threat can be determined. EX-2009, ¶86.

Many view the book “Threat Modeling” by Frank Swiderski and Window Snyder as the first authoritative book on the topic of threat modeling. EX-2008 [Threat Modeling Excerpt]. While “Threat Modeling” was written several years

before the invention of the '366 Patent, "Threat Modeling" defines "threat" and "risk" as two separate concepts. "Threat" is defined as "[t]he adversary's goals, or what an adversary might try to do to a system." EX-2008, 28. "Risk" is defined as "[a] characterization of the danger of a vulnerability or condition." EX-2008, 27. While these definitions are not identified for their accuracy in 2017 when the technology of the '366 Patent was developed, the definitions are consistent with those proffered by Patent Owner and demonstrate that "threat" and "risk" are distinct concepts. EX-2009, ¶87.

At deposition, Petitioner's expert, Mr. Hurlbut, testified a "threat" was different from a "risk." Specifically, Mr. Hurlbut testified that a good definition of "risk" was the likelihood of a threat occurring multiplied by the impact the threat would have if it occurred. EX-2002 [Hurlbut depo], 24:3-25:5, 31:5-33:2. Mr. Hurlbut also testified that knowing the risk does not determine the specific threat that gave rise to the risk. EX-2002 [Hurlbut depo], 61:8-24. Mr. Hurlbut testified that there was not a one-to-one correspondence between a threat and a risk. EX-2002 [Hurlbut depo], 61:8-24; EX-2009, ¶88.

Thus, the extrinsic evidence also supports Patent Owner's construction of "threat," and in addition demonstrates how "threat" and "risk" have different meanings. The term "threat" should be construed to mean "one or more potential

events that, if they occur, can cause adverse effects to a target system.” EX-2009, ¶89.

B. “Threat Model Components”

The ‘366 Patent describes each “threat model component” as “a potential relevant source for one or more threats.” EX-1001, 9:55-57. One example of a threat provided in the specification is “Bluejacking,” in which a potential attacker may seek to gain improper access to a system via its Bluetooth interface. In this example, the threat model component is the “Bluetooth port,” *i.e.*, the potential source of the threat. EX-1001, 9:55-59. As another example, an “online banking interface” may be stored as a threat model “component,” and “a threat may be a virus being introduced to the bank’s environment through a breach in the banking interface.” EX-1001, 24:64-25:1; EX-2009, ¶90.

Further, the ‘366 Patent explains that threat model components are not limited to physical components. Components can be steps, actions, or a physical component. EX-1001, 9:65-10:13. An example of a non-physical component/source is “merging onto freeway” when modeling the threats of commuting to work. “Merging onto freeway” is an action as opposed to a physical component that may be correlated to a threat such as a “freeway collision.” EX-1001, 9:66-10:7; EX-2009, ¶91.

Figure 10 of the '366 Patent and its associated description in the specification provide other examples of threat model components/sources including a USB port, SSO (single sign on), Bluetooth port, and Bluetooth proxy. EX-1001, 17:36-41; EX-2009, ¶92.

The term “threat model components” should be construed as “a potential relevant source for one or more threats.” Petitioner and its expert agree with this construction. Petition, 14; EX-1003, ¶¶40, 60; EX-2002 [Hurlbut depo. Tr.], 20:22-21:25; EX-2009, ¶93.

C. “Visual Representations of the Threat Model Components”

In the prosecution history of the '366 Patent, the Examiner issued an indefiniteness rejection based on the claim 1 recitation of “using visual representations of threat model components correlated with the subset of third party diagram components.” The Examiner stated that his understanding was that “third party diagram components” are visual representations. Thus, the Examiner alleged, a POSITA would not be able to determine how the claimed “visual representations” relate to the “third party diagram components.” EX-1002, 408. In essence, the Examiner argued that it was confusing as to how the claimed “visual representations of threat model components” were correlated with “third party diagram components” which the Examiner understood were also “visual

representations.” EX-2009, ¶94.

In response and after an interview, the applicant explained that the “third party components” were distinct elements from the “visual representations of the threat model components.” The “third party diagram components” (or third party components) were components of an independent (*i.e.*, “third party”) software application (*e.g.*, used, for example, in some other system that does not necessarily have anything to do with threat modeling and is not related to the software performing the steps of the claim). The “visual representations of the threat model components” were elements of the “native” software that is performing the steps of the claim. These elements of the “native” software are used to visually represent potential components of a target system being analyzed as part of the threat model analysis. EX-1002, 505 and 462; EX-2009, ¶95.

One of ordinary skill in the art would have readily recognized this based on the disclosure of the ‘366 patent. For example, Figure 21 of the ‘366 Patent illustrates a user interface in which threat model components (such as ETHERNET PORT) are represented visually for manipulation. EX-2009, ¶96.

The term “visual representations of the threat model components” means “representations of threat model components that can be visually displayed on a diagram.” EX-2009, ¶96.

D. “Mapping Files”

In the context of the claims of the ‘366 Patent, a “mapping file” is “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application.” During prosecution of the ‘366 Patent, the applicant explained that “[t]he mapping file correlates the internal threat model components with the external third party diagram components so that the system can read a file created with the third party software program and generate its own diagram using internal components that are, through the mapping file, correlated to the external third party components.” EX-1002, 506; EX-2009, ¶97.

The ‘366 Patent gives examples of “mapping files.” For example, Figures 28 and 29 show comma separated value (“CSV”) files that are each “mapping files.” EX-1001, 37:14-18. While these mapping files are CSV files, the claimed mapping files can be in a file format other than CSV. EX-1001, 38:33-34. In addition, the “mapping files” can also be one or more tables in a database or multiple databases. EX-1001, 38:34-36. If the mapping file is not stored in the database, the file can be stored in one of the computing devices (*e.g.*, computers, servers, etc.) that make up the threat modeling system. EX-1001, 38:36-40; EX-2009, ¶98.

The term “mapping file” should be construed to mean “a file or one or more

tables that correlate threat model components with visual diagram components of a third party software application.” EX-2009, ¶99.

V. THE CHALLENGED CLAIMS ARE NOT UNPATENTABLE

A. Ground 1: Keenan Does Not Anticipate the Challenged Claims

1. Keenan Does Not Disclose the Claimed “Threats”

All claims of the ‘366 Patent include various recitations of “threats.” The preambles of independent claims 1, 8 and 16 each recite a “threat modeling system” or a “threat modeling method.” Each of these claims recites “a plurality of threats” stored in a database. EX-1001, 43:26, 44:29, 45:29. Additionally, “each of the threats is associated with at least one of the threat model components through the one or more databases.” EX-1001, 43:26-29, 44:29-33, 45:29-33. Further, each independent claim recites “a threat report displaying each threat.” EX-1001, 43:57-58, 44:61-62, 45:20-21. The term “threat” is obviously an aspect of other claim terms including “threat model,” “threat model components,” and “threat report” which appear in each of independent claims 1, 8, and 16. EX-2009, ¶102.

Keenan does not disclose threats at all. EX-2009, ¶103. Keenan is directed to viewing and analyzing risk. This makes sense since the assignee of Keenan is the well-known insurance company, American International Group, Inc. or “AIG” for short. As Keenan explains, the purpose of the Keenan system in part is to

“capture the properties of the information assets in a way that associates the risk, cost, quality, accountability of the assets to the product [sic: production] chain that produces calcs [*i.e.*, calculated outputs] which the business utilizes to set premiums and reserves, manage investment risk and produce financial reports and compliance reports.” EX-1004, 1:33-38 (emphasis added). It is immaterial to Keenan’s system whether a threat (or group of threats) gave rise to the risk. Keenan is focused on assessing the risk, cost, quality, etc. so that the business can make business decisions such as setting premiums, and determining asset reserves. EX-2009, ¶103.

Keenan also does not expressly or inherently determine a threat that may be associated with the risk. EX-2009, ¶104. As explained above, risk is a calculated value based on properties (likelihood of occurrence and impact) that may be associated with a threat. Thus, to the extent that one or more threats gave rise to a risk, the risk is a *downstream* product of properties associated with the one or more threats. As explained above, in the context of a threat, risk is equal to the likelihood of the threat occurring multiplied by the impact that the threat may have if it occurs. Keenan starts with the risk and thus, has no need to determine or otherwise know what, if any, threat(s) gave rise to the risk. EX-2009, ¶104.

Keenan only mentions the word “threat” two times. In Keenan’s “palette”

view, Keenan lists “technical threat vector” as one of the view options. EX-1004, 14:61-63. The “technical threat vector” is described as a view in which “color fills the object shapes based on the value fo [sic: of] the technical risk ranking characteristic of that object.” EX-1004, 14:61-63.¹ “Risk ranking” refers to one of two things. “Risk ranking” either means a risk value, such as a value between 0 and 100. Alternatively (and less likely), “risk ranking” refers to the amount of risk for a particular object relative to the amount of risk for other objects in the view. In either case, the “technical threat vector” is just a risk ranking and has nothing to do with the identification or determination of a threat associated with the risk. EX-2009, ¶105; *see* EX-2002 [Hurlbut depo], 77:5-11 (“technical risk ranking is actually equivalent to a risk level”).

In many circumstances (such as those described in Keenan), the risk of a loss can be known without ever determining the threat or threats that may have contributed to the risk. For example, if a company were selling life insurance to individuals who live in a particular county, the insurance company may know that the risk of a person in that county dying in a particular year is one out of one thousand. The insurance company does not care what the causes of death are (*i.e.*,

¹ The second occurrence of “technical threat vector” has the same explanation of what a “technical threat vector” is. EX-1004, 16:21-23.

the threats). It does not matter that some people died from car accidents, murder, heart disease, cancer, or freak accidents. Each of those threats to life is immaterial to the insurance company who is setting the premium for the life insurance. The company merely needs to know the risk level. That is the point of Keenan. EX-2009, ¶106.

Moreover, knowing the risk to a system alone does not allow one to determine the threat that may have given rise to the risk. EX-2009, ¶107. There is not a one-to-one correspondence between a risk and a threat. Many different threats can lead to the same risk. Figure 8 of the '366 Patent shows that six different threats have the same “very high” risk level. If one only knew that the risk to the system was “very high,” one could not determine which of the six threats led to that risk. Similarly, the same threat can have different risk levels depending on its context. If the threat is physical theft of an automated teller machine (“ATM”), the risk associated with that threat varies depending on where the ATM is located. If the ATM is located in a sparsely populated area of a city, the risk of the theft occurring can be high compared to the risk of the same ATM being physically stolen from inside a bank lobby that is only open during business hours. EX-2009, ¶107.

When asked about certain texts related to threats and risk, Petitioner’s expert

said that threats and risk were different concepts. For example, at his deposition, Petitioner's expert, Mr. Hurlbut, downplayed the relevance of the definition of "risk" contained in Exhibit 2005,² Mr. Hurlbut testified that FAIR was "not considered to be a threat modeling book because it looks at risks." EX-2002 [Hurlbut depo.], 44:6-22. Mr. Hurlbut testified that "FAIR is an approach to do risk management, which is a whole other area of security, so, again, I would understand this definition [of risk] in that context as opposed to in relation to threat modeling to somebody with skill in the art in May of 2017." EX-2002 [Hurlbut depo.], 45:6-14; EX-2009, ¶108.

The Petitioner makes an inherency argument that Keenan discloses threats. The Petition states that "[a] POSITA would understand that Keenan's 'risk' includes threats because measuring risk includes a determination of threats." Petition, 23. The Petition cites Keenan at 16:40-51 for support. But that portion of Keenan relates to different palette view that show risk levels, including the "technical risk measurement" view. Indeed, the word "threat" does not even appear in that passage. Substantively, that passage relates to different views of risk. The Petition also cites to paragraph 79 of Mr. Hurlbut's declaration. In that

² Exhibit 2005 is an excerpt from the book entitled "Measuring and Managing Risk, A FAIR Approach" by Jack Freund published in 2015 ("FAIR").

paragraph, Petitioner's expert makes the point that allegedly a "POSITA would understand that a determination of threats is included within a risk analysis." EX-1003, ¶79. But as explained above, that is not correct. Knowing risk does not mean that any threat determination occurred, much less knowing what the specific threat was. Neither Petitioner nor its expert provide any reasoned explanation allegedly why "measuring risk includes a determination of threats." EX-2009, ¶109.

The claims of the '366 Patent require that "a plurality of threats [are] stored" in one or more databases.³ Not only does Keenan not disclose a determination of threats, Keenan certainly does not disclose storing a plurality of threats in a database. EX-2009, ¶110.

The Petition and Petitioner's expert state that "[a] POSITA would understand that Keenan discloses a threat modeling system and method." Petition, 23, EX-1003, ¶79. That too is incorrect. EX-2009, ¶111. A POSITA would understand that, at best, Keenan discloses a *risk* modeling system/method. See EX-2002 [Hurlbut depo], 89:22-90:5; 90:11-23. Keenan's system allows a business to assess system-level risk to determine insurance premiums and asset

³ This same language appears in all three independent claims – namely, claims 1, 8, and 16.

reserve levels. EX-1004, 1:33-38. Keenan does not disclose threat modeling to a POSITA. EX-2009, ¶111. That is consistent with Mr. Hurlbut's testimony where he described a threat model as a tool to allow someone deal with threats, not risk. EX-2002 [Hurlbut depo.], 19:8-15.

Mr. Hurlbut's declaration states that:

Keenan discloses methods and system of measuring risk through threat modeling by providing "visual depictions" and models of the risk (which includes threats), *i.e.*, through visually depicting threats against IOE objects and creating "Views" through threat vectors, which may be combined with other Views, such as "model risk."

EX-1003, ¶79 (p.40). The Petition contains virtually the same sentence. Petition, 24. Parts of this sentence are correct, and other parts are incorrect. Keenan does disclose a method and system of storing and viewing risk. EX-1004, Abstract. Keenan does not disclose a system for measuring risk. The risk for objects is determined before the objects are imported into the IOE. Keenan does not make that measurement. Keenan discloses "models of the risk" or risk modeling. But Keenan does not disclose threat modeling. Contrary to Mr. Hurlbut's declaration, "the risk" does not "includes threats." Neither generally nor in the context of Keenan does risk "include threats." Risk might be based on a threat. But risk does not include a threat and determining risk does not require identifying or

determining a threat. Contrary to Mr. Hurlbut, Keenan does not “depict threat against IOE objects.” Risk and other characteristics of IOE objects are depicted, but a threat is not depicted. EX-2009, ¶112.

While Mr. Hurlbut states that the “model risk” option and the “technical threat vector” option can be combined in a single view, Keenan teaches otherwise. Model Risk is described as “color fills the object shapes based on the value of the risk characteristics for the models in the view.” EX1004, 14:36-39. Technical Threat Vector is described as a view in which “color fills the object shapes based on the value [of] the technical risk ranking characteristic of that object.” For Model Risk, the color is based on the “risk characteristics for the models in the view,” whereas for Technical Threat Vector, each object is filled with color based on risk ranking of that object. These descriptions run contrary to each other, thus leading to the conclusion that those two options cannot be combined in a single view. EX-2009, ¶112.

The Petition and Mr. Hurlbut both cite to exhibits other than Keenan to support the assertion that there is a close connection between risk analysis and threat modeling. Petition, 23-24, EX-1003, ¶79. Ground 1 is an anticipation ground based on Keenan. Thus, it is improper to rely on references other than Keenan to assert that Keenan discloses threats.

Petitioner relies on Keenan’s disclosure of “risk” as satisfying the claimed “threat” features of the ’366 Patent. Specifically, Petitioner contends that a “POSITA would understand that Keenan’s ‘risk’ includes threats because measuring risk includes a determination of threats.” Pet., 23 (citing EX-1003, ¶79). However, Petitioner’s reliance on its expert for disclosure of “threats” is improper under an anticipation theory. A “petitioner asserting anticipation cannot rely on its expert to supply disclosure of a claim element that is not expressly or inherently present in the reference.” *See Consolidated Trial Practice Guide*, at 36 (November 2019) (<https://www.uspto.gov/TrialPracticeGuideConsolidated>).

Petitioner argues that “the assets/objects in Keenan are ‘relevant sources of threats’ and thus threat model components, as defined by the ’366 patent, because the assets/objects in Keenan are subject to risks that Keenan’s system measures.” Pet. 28 (citing EX-1003 ¶82). However, nothing in Keenan describes threats and the fact that the assets are subject to risk that is displayed does not teach, or even suggest a threat determination. EX-2009, ¶114.

In the Institution Decision, the Board stated that “Patent Owner then merely concludes, without citing any factual support, that use of a color identifying the generic nature of a risk still fails to disclose any threats associated with the risk.” Institution Decision, p. 18. However, the use of color identifying risk levels is not

the same as teaching the presence of threats. Patent Owner's expert agrees. EX-2009, ¶115.

Petitioner essentially admits that threats are not expressly disclosed in Keenan. Therefore, while Petitioner and its expert do not expressly argue “inherency,” in order for Petitioner's argument to succeed, threat determination and the storage of threats in the claimed manner would have to be inherent in the disclosure of Keenan. This is not the case. The fact that a certain result or characteristic may occur or may be present in the prior art is not sufficient to establish the inherency of that result or characteristic. *In re Rijckaert*, 9 F.3d 1531, 1534, 28 USPQ2d 1955, 1957 (Fed. Cir. 1993); *In re Oelrich*, 666 F.2d 578, 581-82, 212 USPQ 323, 326 (CCPA 1981). When relying on inherency, the party challenging the claims “must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art.” *Ex parte Levy*, 17 USPQ2d 1461, 1464 (Bd. Pat. App. & Inter. 1990). Keenan does not inherently disclose threat or the storage and use of threats. EX-2009, ¶116.

When measuring risk (or displaying risk, in the case of Keenan), it does not necessarily follow that there has been a determination of a threat. Keenan fails to disclose or suggest any “threat” or any database storing threats, as claimed.

Rather, Keenan discloses a risk value, which is a number, without identifying or storing any threat as claimed. EX-2009, ¶117. Further, Keenan fails to disclose storing any threats in a database, as storing a value for a degree of risk is not what is claimed by the '366 Patent. Even if one were to assume, for the sake of argument, that the Petitioner's assertion that "measuring risk includes a determination of threats" is correct, such determination does not result in storing or using a threat in the claimed manner. EX-2009, ¶117.

Keenan does not anticipate any of the claims of the '366 Patent. Keenan does not disclose threats explicitly or inherently. Keenan relates to analysis of risk. Knowing a particular risk does not determine what threat, if any, gave rise to the risk. Keenan certainly does not disclose the storing of threats in one or more databases or the use of threats to generate a threat model. EX-2009, ¶118.

2. Keenan Does Not Disclose the Other "Threat" Claim Terms Including "Threat Model," "Threat Model Components," "Visual Representations of the Threat Model Components," or "Threat Report"

Because Keenan does not disclose "threats" or the storing of multiple threats, Keenan does not disclose a "threat model," "threat model components," "visual representations of the threat model components," or a "threat report." EX-2009, ¶119.

Throughout the analysis of Keenan in the Petition and in Mr. Hurlbut's

declaration, Petitioner and Mr. Hurlbut essentially conflate the concepts of “risk” and “threats” to argue that Keenan disclosed the claims of the ‘366 Patent. For example, with respect to Element 1[b], Mr. Hurlbut states that:

A POSITA would understand that the assets/objects in Keenan are “relevant sources of threats” and thus threat model components because the assets/objects in Keenan are subject to risks that Keenan’s system measures. A POSITA would further understand that “risk” as disclosed in Keenan includes threats because measuring risk includes a determination of threats.

EX-1003, ¶82. Mr. Hurlbut’s conclusion is necessarily based on the incorrect premise that risk somehow determines threats. At best, Mr. Hurlbut’s analysis is conclusory. As explained above, knowing risk does not determine the threat, if any, that caused the risk. The same conclusory analysis is contained in Mr. Hurlbut’s paragraph 83 (and elsewhere in his declaration, *e.g.* ¶106). EX-2009, ¶120.

In his analysis of the preamble, Mr. Hurlbut states that:

A POSITA would understand that “types of risk,” as disclosed in Keenan are threats because the described examples are all types of threats (cyber, environmental, accidental). Thus, Keenan disclosed threats within its risk analysis.

EX-1003, ¶79 (p.38). But Mr. Hurlbut’s conclusion ignores the plain language in

Keenan. The cited portion of Keenan expressly says that “cyber, environmental, accidental, etc.” are all different types of *risk* – not threats. EX-1004, 16:45-48. Again, Mr. Hurlbut simply assumes that knowing risk determines a threat or that “risk” is synonymous with “threat.” That is incorrect, as explained above. EX-2009, ¶121.

Keenan does not disclose a “threat model,” “threat model components,” “visual representations of the threat model components,” or a “threat report.” One or more of these terms are used throughout independent claims 1, 8, and 16, and in dependent claims 5, 7, 12-14, and 19-20. EX-2009, ¶122.

3. Keenan Does Not Disclose Dependent Claims 2, 3, 9, 10, 17, or 18

Claim 2 depends from independent claim 1 and recites “wherein the one or more mapping files are not stored in the one or more databases but are stored on the one or more computing devices.” Claim 3 depends from independent claim 1 and recites “wherein the one or more mapping files comprise one or more tables stored within the one or more databases.” EX-1001, 43:62-67.⁴ Thus, for claim 2, the mapping files cannot be stored in the database(s). But for claim 3, the mapping files’ tables must be stored in the database(s). To the extent these claims recite

⁴ Dependent claims 9 and 17, and claims 10 and 18 recite the same limitations as claims 2 and 3, respectively.

where the mapping files are stored, these claims are mutually exclusive. EX-2009, ¶123.

Before analyzing claims 2 and 3 themselves, it is useful to go back to the Petition's and Petitioner's expert's analysis of the "mapping files" in claim 1. For Elements 1[c] and 1[d], Petitioner and its expert relied upon two distinct teachings for the "mapping files." First, the Petition relied on the lone statement in Keenan that "[a] map is preset that maps Visio shapes and formats to IOE shapes and formats." Petition, 29-30; EX-1003, ¶¶84-88. Second, the Petition relies on "diagrams and 'Views' on a Graphical User Interface." *Id.*; EX-2009, ¶124.

It is important to understand that the second aspect of Keenan relied upon in the Petition (*i.e.*, the diagrams and Views) relates to the *topological* relationship among various objects. EX-2009, ¶125. The diagrams and "View" are different ways of visually looking at objects within a system, their interconnections among the objects, and various information about the objects, such as their risk level. *E.g.*, EX-1004, Abstract.

Keenan contains a set of definitions. "View" is defined as "[d]epiction of topology in the IOE via GUI. A view that is exported or printed from the IOE is a 'Diagram.'" EX-1004, 5:24-25. Keenan defines "topology" as "[r]epresentation of the relationships between objects in an analytical infrastructure." EX-1004, 5:5-

6. Examples of various topological “Views” are shown in Keenan’s Figures 4-11. Each figure shows the relationships among the objects in the View. These “Views” do not show any correlations between “threat model components” and “third party diagram components.” Thus, the various citations to “Views” and diagrams cannot relate to the claimed “mapping files.” EX-2009, ¶126.

Views cannot correspond to the mapping files because dependent claims 2 and 3 are directed to where the mapping files (or their tables) are stored. Keenan describes the IOE as residing in a graph database and the Views on the GUI are generated based on information in the IOE. EX-1004, 5:45-49, 1:53-57, 5:24-25. Keenan also says the “all or part of [the] steps of the processes in the preceding embodiments” may be implemented by “computing hardware instructed by a program. The program may be stored in a computer readable storage medium. The storage medium may include a ROM, A RAM, a magnetic disk or a compact disk.” EX-1004, 21:27-33. A POSITA would understand this passage to refer to the application program that implements the IOE. EX-2009, ¶127. But Keenan does not describe the location of the “map [that] is preset that maps Visio shapes and formats to IOE shapes and formats,” which is the first Keenan teaching relied upon for the “mapping files.” EX-2009, ¶127.

For Keenan to anticipate any of the challenged claims, Keenan must

disclose, expressly or inherently, the location of the claimed “mapping files.”

Keenan does not disclose that location. Keenan certainly does not indicate whether the alleged mapping files (or their tables) are stored in a file on a computing device and not in the claimed databases (claim 2), whether the mapping files’ tables are stored in the databases (claim 3), or whether the preset map is stored elsewhere such as in a cloud server. EX-2009, ¶128.

4. Keenan Does Not Disclose Dependent Claim 5

Dependent claim 5 recites that the determination of the threat model components correlated to the third party diagram components comprises “first determining whether a user-defined name for one of the subset of third party diagram components has a match in the one or more mapping files and, if no such match is found, then determining whether a default title for the third party diagram component, as defined by the third party software application, has a match in the one or more mapping files.” EX-1001, 44:4-13 (emphasis added). Thus, claim 5 has a distinct order. The system first checks to see if the user-defined name has a match, and if not, then the system determines whether a default title has a match. EX-2009, ¶129.

Claim 1 introduces the “subset of the third party diagram components” as being included in the “data file” that is read by the threat modeling system, where

the “data file” is “generated by the third party software application,” and “defin[es] one or more relationships between the subset of third party diagram components.”

EX-1001, 43:40-45. According to claim 1, reading the “data file” is how the system obtains the “subset of the third party diagram components.” Claim 5 then requires that the system first check for “user-defined name” match, and if no match is found, the system checks for a “default title” match. EX-2009, ¶130.

Keenan works in the opposite order. When importing a file into the Keenan system, the IOE “first checks to see if [the] object already exists in IOE based on external ID number first, then name match.” EX-1004, 18:36-50; EX-2009, ¶131.

Petitioner and its expert argue that Keenan also discloses the opposite order. But that is not true when importing and reading data files from third party applications. The portion of Keenan cited by Petitioner relates to a user manually adding individual objects. EX-1004, 18:36-50. This passage does not relate to “reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components,” as recited in claim 1. EX-2009, ¶132.

5. Keenan Does Not Disclose Claims 6 and 14

Claim 6 depends from claim 5 and recites that “if no match is found for the default title, matching the third party diagram component with a placeholder

component and displaying the placeholder component on the relational diagram to indicate that no match was found.” EX-1001, 44:13-17. Claim 14 depends from claim 8 and recites that “for each of the subset of third party diagram components for which no correlated threat model component is found in the one or more mapping files, the diagram interface displays a placeholder component indicative of a match not being found.” EX-1001, 45:15-19; EX-2009, ¶133.

The Petition and its expert cite to Keenan at 13:53-65, 11:7-11, 19:9-16, and Figures 12 and 13. Keenan at 13:53-65, 19:9-16, and Figures 12 and 13 all relate to a user modifying a “typology” and the system categorizing and saving it as a temporary typology. Keenan’s column 11:7-11 relates to searching the IOE and the results being returned and stored in temporary memory. EX-2009, ¶134. None of these citations relate to displaying a placeholder component showing that one of the subset of third party diagram components did not have a matching threat modeling component in the mapping file. The cited passages from Keenan have nothing to do with the subject matter of claims 6 and 14. It appears that Petitioner simply searched Keenan for the word “temporary” and then cited those passages. EX-2009, ¶134.

6. Keenan Itself Is Not Prior Art and the Petition Made No Attempt to Show that the Cited Portions of Keenan Qualify As Prior Art

Initially, Patent Owner notes that Petitioner has failed to establish that the disclosure of Keenan, on which the Grounds for Opposition are based qualifies as prior art pursuant to 35 U.S.C. §102. Title 35 U.S.C. §102(d) states:

(d) PATENTS AND PUBLISHED APPLICATIONS
EFFECTIVE AS PRIOR ART.—For purposes of determining whether a patent or application for patent is prior art to a claimed invention under subsection (a)(2), such patent or application shall be considered to have been effectively filed, with respect to any subject matter described in the patent or application—

(1) if paragraph (2) does not apply, as of the actual filing date of the patent or the application for patent; or

(2) if the patent or application for patent is entitled to claim a right of priority under section 119, 365(a), 365(b), 386(a), or 386(b), or to claim the benefit of an earlier filing date under section 120, 121, 365(c), or 386(c) based upon 1 or more prior filed applications for patent, as of the filing date of the earliest such application that describes the subject matter.

Title 35 U.S.C. §102(d) (emphasis added).

Petitioner states, the “[f]or the purposes of this IPR only, Petitioner applies a priority date of May 17, 2017.” Petition, 8. For purposes of this IPR, Patent

Owner does not dispute this date. Keenan was filed on April 19, 2018 and claims priority to a Provisional Application Ser. No. 62/487,370 filed on April 19, 2017 (“Keenan Provisional Filing”). Petitioner’s assertions based on the content of the U.S. Patent 11,200,228 (the Keenan Patent) do not demonstrate that the asserted subject matter was known prior to the May 17, 2017, the effective filing date of the ‘366 patent applied by Petitioner. For Keenan to be considered as prior art with respect to the ‘228 patent, Petitioner must demonstrate that the alleged disclosure relied on by Petitioner was present in the Keenan Provisional Filing. 35 USC §102(d)(2). Petitioner has made no such showing (or even an allegation thereof).

Moreover, it would be improper for Petitioner to supplement the record by trying to show that the relevant portions of Keenan are entitled to Keenan’s provisional filing date because establishing entitled to that provisional filing date is part of Petitioner’s alleged prima facie case of unpatentability. PTAB Consolidated Trial Practice Guide, Nov. 2019 (“CTPG”), 73 (“Petitioner may not submit new evidence or argument in reply that it could have presented earlier, e.g. to make out a prima facie case of unpatentability.”); *see Hulu, LLC v. Sound View Innovations, LLC*, Case IPR2018-01039 (PTAB Dec. 20, 2019) (Paper 29) (Precedential Opinion) at 7.

The Petition fails to establish that any claim of the ‘366 Patent is

unpatentable for this reason alone.

B. Ground 2: Alleged Obviousness of Claims 1-4, 7-11, 15-18 over Zheng In View of Baker and Jones

Zheng discloses a system comprising “a visualization module for rendering, on a computer display, a map with components representative of the suite of software applications and relationships among the software applications,” where “[t]he components are displayed in a base layer of the map.” Ex. 1005, 1:48–53. Zheng explains that “by utilizing a visualization approach like cartography, application architecture can be represented in a compressible view that enhances security and risk analysis,” and that “mapping techniques and concepts can be used in the context of data visualization to create a graphical representation of application connectivity and security.” *Id.* at 3:28–34. Zheng uses the term “map” consistently in the context of cartography, *i.e.*, creating a digital view of components and their interconnections (like drawing a map of how computer network components are interconnected). EX-2009, ¶135.

Petitioner argues, *inter alia*, “Zheng’s ‘mapping techniques’ and its ‘map’ convey, and necessarily include, a ‘mapping file’ as claimed because a mapping file would be required to perform mapping techniques.” Pet. 63 (citing EX-1003 ¶162). However, Zheng’s ‘mapping techniques’ are related to visualization of the application architecture, ‘like cartography,’ and have nothing to do with

‘correlating the threat model components with visual diagram components of a third party software application’ as recited in the claims. Additionally, Zheng’s generic disclosure of ‘mapping techniques . . . in the context of data visualization’ does not necessarily require any ‘mapping files’ as claimed. EX-2009, ¶136.

Petitioner then turns to Baker (EX-1006) for allegedly disclosing limitation 1[d], namely, “the one or more mapping files correlating the threat model components with visual diagram components of a third party software application.” Pet. 64–65. Baker discloses an “automated risk management system,” where a user is able to build a risk management flowchart (or multiple flowcharts) that “utilizes symbols of various shapes to indicate actions, determinations, or other elements of an activity or evaluation so that respective personnel of an organization can understand actions to be taken to successfully manage an activity or avoid a negative outcome.” EX-1006, ¶¶5, 20, 25. “Importantly, risk management or control flowcharts may be imported . . . from third party software such as that marketed as Microsoft Office Visio®.” *Id.* ¶25. By relying on Baker for the “correlating” feature, Petitioner implicitly acknowledges that Zheng itself does not disclose “mapping techniques” in the context of “correlating” components in the claimed manner. EX-2009, ¶137.

Petitioner argues Baker discloses “visual diagram components of a third

party software application” based on its disclosure of importing flowcharts from Visio, discussed above. Pet. 64. Petitioner further alleges that the skilled artisan would have been motivated to combine these teachings from Baker with the system of Zheng “to enable the importation of diagrams from Microsoft Visio into the threat modeling software of Zheng such that the mapping file of Zheng would correlate the threat model components with visual diagram components from the Visio diagrams.” Pet. 65 (citing EX-1003, ¶166); *see* Pet. 83–85 (alleged reasons to combine Zheng and Baker). EX-2009, ¶138.

However, Zheng does not disclose any mapping file, either expressly or inherently, and even considered in view of Baker, fails to disclose or suggest the claimed correlations based on mapping files. EX-2009, ¶139. Baker’s process has no need or use for any “mapping files” as recited in the claims. Baker stores the “text and shape of each element of the flowchart . . . in the process database 30” and “automatically assign[s] or associate[s] predetermined objectives or controls according to the shapes of the imported flowcharts.” Baker, [0025]; *see also id.*, [0009]. Baker simply searches for a flowchart shape without disclosing any “mapping files” providing correlations as recited in the claims. EX-2009, ¶139.

To reach the claimed correlations recited in claim 1, Petitioner first has to create a mapping file to capture the threat actor/threat target association of Zheng,

and then has to create a modification to repurpose the associations. EX-2009,

¶140. The motivations for these additions are hindsight-based creations of features not disclosed or suggested by the art. Neither Baker nor Zheng teaches “correlating” (a) threat model components with (b) visual diagram components of a third party software application, let alone doing so using “mapping files.” Further, one of skill in the art would not have been motivated to combine the alleged teachings of Zheng and Baker to arrive at limitations 1[c] and 1[d], but for hindsight, *i.e.*, using claim 1 and the teachings of the ’366 patent as a roadmap. EX-2009, ¶140.

C. Grounds 3-5: Alleged Obviousness of: (1) Claims 2, 9, and 17 over the Combination of Zheng, Baker, Jones, and Galliano (*i.e.*, Ground 3); (2) Claims 1–20 over the Combination of Zheng, Baker, Jones, and Keenan (*i.e.*, Ground 4); and (3) Claims 2, 5-6, 9, 12–14, 17, and 19-20 over the Combination of Zheng, Baker, Jones and “the knowledge of a POSITA” (*i.e.*, Ground 5)

Petitioner also contends certain claims are unpatentable under 35 U.S.C. § 103 as obvious over the following combinations:

- (1) claims 2, 9, and 17 over the combination of Zheng (Ex. 1005), Baker (Ex. 1006), Jones (Ex. 1007), and Galliano (Ex. 1008);
- (2) claims 1–20 over the combination of Zheng, Baker, Jones, and Keenan (Ex. 1004); and
- (3) claims 2, 5-6, 9, 12-14, 17, and 19-20 over the combination of Zheng, Baker, Jones and “the knowledge of a POSITA.”

Pet. 12, 85–89.

As for combination (1) above, Petitioner applies this combination only to dependent claims 2, 9, and 17, and does not appear to apply Galliano in any manner that would cure any deficiencies identified above, particularly with respect to independent claims 1, 8, and 16. EX-2009, ¶142.

As for combination (2) above, Petitioner applies this combination to claims 1-20, and does not apply Keenan, in this obviousness context, in any manner that would cure any deficiencies identified above, particularly with respect to independent claims 1, 8, and 16. Further, while Keenan is cited as a basis for invalidity based on Combination (2), Petitioner has not presented any allegations as to how Keenan is applied in conjunction with teachings of Zheng, Baker, and Jones to arrive at claims 1-4, 7-11, and 15-18. EX-2009, ¶143.

As for combination (3) above, Petitioner applies this combination only to dependent claims 2, 5-6, 9, 12-14, 17, and 19-20, and does not appear to apply any alleged “knowledge” of the skilled artisan, in this obviousness context, in any manner that would cure any deficiencies identified above in Section V.A, particularly with respect to independent claims 1, 8, and 16. *See* Pet. 88–89; EX-2009, ¶144.

Because none of the references relied upon in Grounds 3-5 cure the

underlying deficiencies identified in my analysis of Grounds 1 and 2, the Petition fails to establish obviousness under any of Grounds 3-5. EX-2009, ¶145.

VI. CONCLUSION

For the reasons discussed above, the challenged claims are not anticipated and/or rendered obvious over the references relied upon in the Petition.

Dated: January 12, 2024

Respectfully submitted,

/s/ Donald L. Jackson
Donald L. Jackson

CERTIFICATION OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(b), (c) and (d), Patent Owner certifies that the word count of Patent Owner's Response (exclusive of any table of contents, table of authorities, mandatory notices under § 42.8, certificates of service and word count, and list of exhibits or claim listing) as measured by Microsoft Word is 11,577 words.

By: /s/ Donald L. Jackson
Donald L. Jackson

CERTIFICATE OF SERVICE ON PETITION UNDER 37 C.F.R. § 42.105

Pursuant to 37 C.F.R. § 42.6(e) and 42.105(b), the undersigned certifies that, on January 12, 2023, a complete and entire copy of this Patent Owner Response, together with all supporting exhibits, were served on Petitioner electronically, by agreement, by emailing a copy of the same to the following attorneys for Petitioner:

brent.yamashita@us.dlapiper.com
blake.jackson@us.dlapiper.com
matthew.middleton@us.dlapiper.com

By: /s/ Donald L. Jackson
Donald L. Jackson