

**IriusRisk Inc. v. ThreatModeler
Software Inc.,**

**IPR2023-00656
(U.S. Patent No. 10,713,366)**

Petitioner's Demonstrative Exhibits

Oral Argument: July 10, 2024



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Overview

- Technology Overview
- ThreatModeler's U.S. Patent No. 10,713,366 (the '366 patent)
- Claim Construction
- Grounds:
 - **Ground 1:**
 - Keenan Anticipates Claims 1-20
 - **Ground 2:**
 - Zheng in View of Baker and Jones Renders Obvious Claims 1-4, 7-11, 15-18
 - **Ground 3:**
 - The References of Ground 2 in Further View of Galliano Render Obvious Claims 2, 9, and 17
 - **Ground 4:**
 - The References of Ground 2 in Further View of Keenan Render Obvious Claims 1-20
 - **Ground 5:**
 - The References of Ground 2 in Further View of the Knowledge of a POSITA Renders Obvious Claims 2, 5-6, 9, 12-14, 17, and 19-20

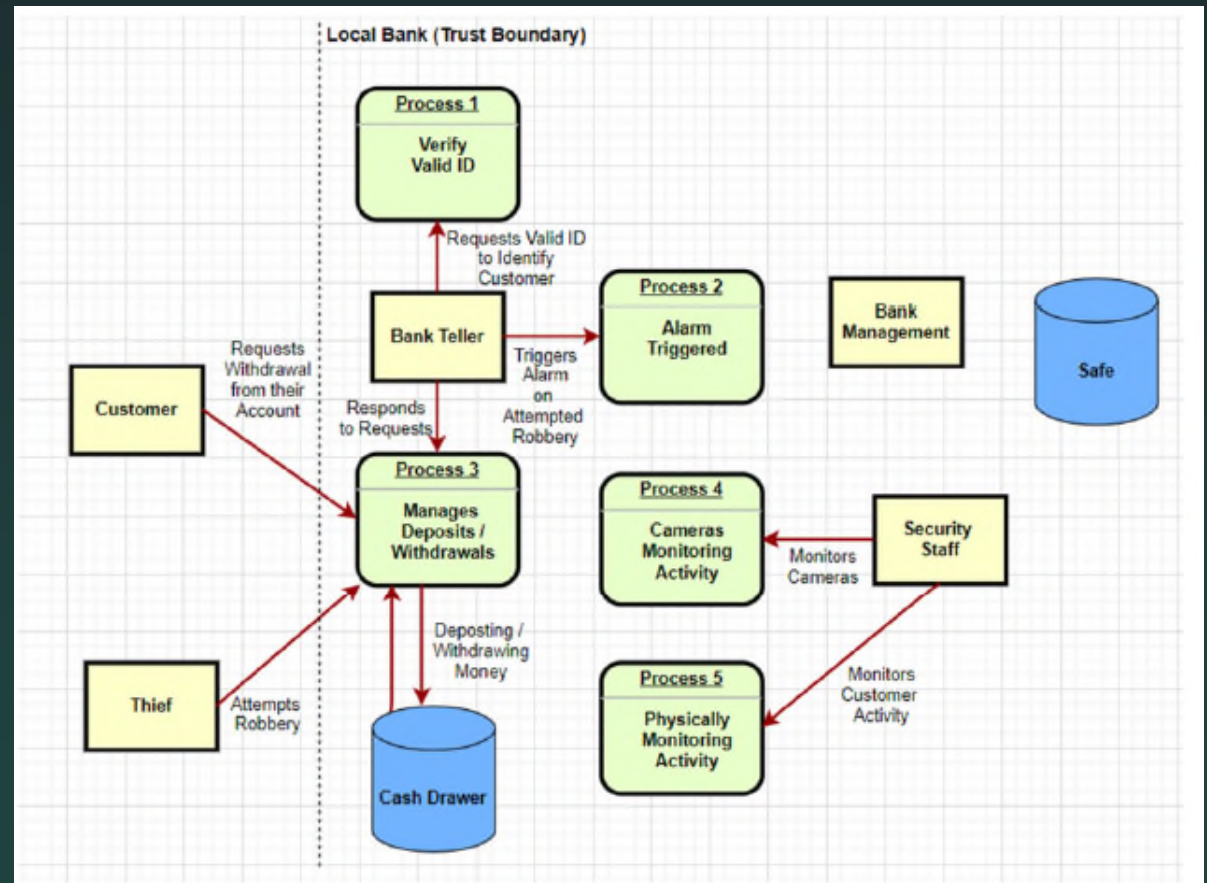
DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

The '366 Patent

Background: Threat Model

Threat modeling is a process by which potential threats to a system are identified. Petition at 4.

The Petition provides an example of a threat model showing potential threats to a physical branch of a bank:



Petition at 5.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

The '366 Patent

US10171336B2

(12) **United States Patent**
Agarwal

(10) **Patent No.:** US 10,713,366 B2
(45) **Date of Patent:** Jul. 14, 2020

(54) **SYSTEMS AND METHODS FOR AUTOMATED THREAT MODEL GENERATION FROM THIRD PARTY DIAGRAM FILES**

(71) Applicant: **ThreatModeler Software Inc.**, Jersey City, NJ (US)

(72) Inventor: **Anurag Agarwal**, Jersey City, NJ (US)

(73) Assignee: **ThreatModeler Software Inc.**, Jersey City, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **16/542,263**

(22) Filed: **Aug. 15, 2019**

(65) **Prior Publication Data**
US 2019/0370477 A1 Dec. 5, 2019

Related U.S. Application Data
(63) Continuation-in-part of application No. 16/228,738, filed on Dec. 20, 2018, which is a (Continued)

(51) Int. Cl. **G06F 21/57** (2013.01)
G06F 16/21 (2019.01)
(Continued)

(52) U.S. CL. **G06F 21/577** (2013.01); **G06F 9/451** (2018.02); **G06F 16/212** (2019.01);
(Continued)

(58) **Field of Classification Search**
CPC .. G06F 21/577; G06F 16/2282; G06F 16/248; G06F 9/451; G06F 16/212; G06F 2221/0833
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
4,999,015 A 9/1990 Rasinski et al.
6,952,779 B1 10/2003 Cohen et al.
(Continued)

OTHER PUBLICATIONS
Bruce Potter, Microsoft SDL Threat Modeling Tool, Network Security, vol. 2009, Issue 1, pp. 15-18 (Elsevier 2009) (Year: 2009).*

(Continued)

Primary Examiner — Theodore C Parsons
(74) Attorney, Agent, or Firm — Law Office of Paul B. Johnson, Paul B. Johnson

(57) **ABSTRACT**
Threat modeling systems include one or more computing devices communicatively coupled with one or more databases, the database(s) including threat model components and threats associated with one another. One or more mapping files coupled with the database(s) correlate the threat model components with visual diagram components of a third party software application. An import interface initiates reading of a third party generated data file by the computing device(s), the data file including a subset of the third party diagram components and relationships between the subset. An interface receiving input initiates a determination of threat model components correlated with the subset. A diagram interface displays a relational diagram using visual representations of threat model components correlated with the subset, the relational diagram defining a threat model. A threat report interface includes a threat report displaying each threat that is associated with one of the threat model components of the threat model.

20 Claims, 30 Drawing Sheets

IriusRisk
Ex. 1001 - Page 1

The alleged invention of the '366 patent is the ability to create diagrams in a “third party software application” such as Microsoft Visio and to import those diagrams into the threat model. '366 Patent at 24:26-29.

2500

CREATE NEW THREAT MODEL

Test Proj 1 1.0 AWS Cloud App

Required Required

AWS; High Internal

C:\desktop\AWS_2.vsd BROWSE

Only .vsd & .vsdx formats are supported.
Please validate a file. VALIDATE

EMPTY TEMPLATE IMPORT WIZARD

X Cancel Submit

HEALTH THREAT	1.0	0%	Very High	BOB
ONLINE BANK	1	0%	Very High	ANN

FIG. 26

Petition at 6-8.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

'366 Patent Challenged Claim 1

CLAIM ELEMENT	CLAIM
1[p]	"A threat modeling method, comprising:"
1[a]	"providing one or more databases, the one or more databases comprising:"
1[b]	"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;"
1[c]	"providing one or more mapping files communicatively coupled with the one or more databases,"
1[d]	"the one or more mapping files correlating the threat model components with visual diagram components of a third party software application (hereinafter "third party diagram components"); and"
1[e]	"in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices communicatively coupled with the one or more databases:"
1[f]	"using the one or more computing devices, reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;"
1[g]	"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;"
1[h]	"displaying on the one or more user interfaces a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and"
1[i]	"generating, using the one or more computing devices, and displaying, on the one or more user interfaces, a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model."
	the remaining independent claims (8 and 16) are commensurate in scope with claim 1 (see Institution Decision at 23-24)

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

'366 Patent Challenged Claim 2-7, 12-13, and 15

CLAIM ELEMENT	CLAIM
2	"The method of claim 1, 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."
3	"The method of claim 1, wherein the one or more mapping files comprise one or more tables stored within the one or more databases."
4	"The method of claim 1, wherein the data file comprises one of a VSD file, a VSDX file, a TMT file, an XML file, a JSON file, a PNG file, and a JPEG file."
5	"The method of claim 1, wherein determining, for the subset of third party diagram components, correlated threat model 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 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."
6	"The method of claim 5, further comprising, 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."
7	"The method of claim 1, further comprising determining, for the one or more relationships defined by the data file, correlated threat model components as defined in the one or more mapping files."
12	"The system of claim 8, wherein the one or more mapping files includes a file correlating user-defined names of the third party diagram components with the threat model components."
13	"The system of claim 8, wherein the one or more mapping files includes a file correlating default titles of the third party diagram components with the threat model components."
15	"The system of claim 8, further comprising one or more mapping interfaces displayed on the one or more computing devices and configured to, in response to receiving user input, modify the one or more mapping files."
	the remaining dependent claims (9-11, 14, and 17-20) are commensurate in scope with the claims above.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Claim Construction

Claim Construction

CLAIM TERM	PETITIONER'S DEFINITION	PATENT OWNER'S DEFINITION
"Threat"	✓ an "undesirable event that may happen."	X "one or more potential events that, if they occur, can cause adverse effects to a target system."
"Mapping File"	✓ "a file or other representation that correlates data from a source to a target."	X "a file or one or more tables that correlate threat model components with visual diagram components of a third party software application."

Institution Decision at 12; POR at 18-25, 28-29; Reply at 3-5; Sur-Reply at 2-4

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Claim Construction

“Threat”

“Threat”	✓ an “undesirable event that may happen.”	X “one or more potential events that, if they occur, can cause adverse effects to a target system.”
----------	---	---

“Threat”

✓ an “undesirable event that may happen.”

X “one or more potential events that, if they occur, can cause adverse effects to a target system.”

CLAIM ELEMENT

CLAIM

1[p]	“A threat modeling method, comprising:”
1[a]	“providing one or more databases, the one or more databases comprising:”
1[b]	“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;”
1[c]	“providing one or more mapping files communicatively coupled with the one or more databases;”
1[d]	“the one or more mapping files correlating the threat model components with visual diagram components of a third party software application (hereinafter “third party diagram components”); and”
1[e]	“in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices communicatively coupled with the one or more databases;”
1[f]	“using the one or more computing devices, reading a data file generated by the third party software application, the data file comprising a subset of the third party diagram components, the data file defining one or more relationships between the subset of third party diagram components;”
1[g]	“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;”
1[h]	“displaying on the one or more user interfaces a relational diagram of one of a system, an application, and a process, using visual representations of the threat model components correlated with the subset of third party diagram components, the relational diagram defining a threat model; and”
1[i]	“generating, using the one or more computing devices, and displaying, on the one or more user interfaces, a threat report displaying each threat that is associated through the one or more databases with one of the threat model components included in the threat model.”
	“the remaining independent claims (8 and 16) are commensurate in scope with claim 1”

- The parties’ definitions are essentially the same.
- The asserted references (Keenan, Zheng) disclose threats under either parties’ definition.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Claim Construction

“Mapping File”

“Mapping File”	✓ “a file or other representation that correlates data from a source to a target.”	X “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application.”
----------------	--	---

“Mapping File”

✓ “a file or other representation that correlates data from a source to a target.”

X “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application.”

CLAIM ELEMENT	CLAIM
1[p]	“A threat modeling method, comprising:”
1[a]	“providing one or more databases, the one or more databases comprising:”
1[b]	“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;”
1[c]	“providing one or more mapping files communicatively coupled with the one or more databases,”
1[d]	“the one or more mapping files correlating the threat model components with visual diagram components of a third party software application (hereinafter “third party diagram components”); and”
1[e]	“in response to receiving one or more user inputs, using one or more user interfaces displayed on one or more computing devices communicatively coupled with the one or more databases:”

- PO’s definition imports claim language, which is improper.
- See *Robotic Vision Sys., Inc. v. View Eng’g, Inc.*, 189 F.3d 1370, 1376 (Fed. Cir. 1999) (rejecting a construction on the ground that it “would necessarily be redundant and would add no additional limitations.”)

Reply at 5-7

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Petitioner's Expert: Robert Hurlbut



Robert Hurlbut is a long-time software developer, software architect, and application security / threat modeling leader, working to help developers, software architects, project managers, and others on project teams to understand more about secure software design and architecture through threat modeling and other secure application initiatives. He is a strong advocate for creating, building, and sustaining Threat Modeling Programs in organizations as well as creating, building, and sustaining Security Champion Programs.

New since May, 2023:

Ph.D. in Space Cybersecurity student @ Capitol Technology University with a focus on Threat Modeling and Secure Software Design, Architecture, and Development for New Space Systems.

Robert Hurlbut is the Co-author of the Threat Modeling Manifesto (2020):

<https://threatmodelingmanifesto.org>

Robert Hurlbut is the Co-author of the Threat Modeling Capabilities Model (2024)

<https://threatmodelingmanifesto.org/capabilities>

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

“Mapping File”

✓ “a file or other representation that correlates data from a source to a target.”

X “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application.”

17 Q. All right. Let me ask you about
18 mapping files. As used in the '366 patent,
19 and again from the perspective of a person
20 of skill in the art in May of 2017, what
21 does the term mapping files mean?

22 A. A mapping file is actually a
23 general term that's well-known for those who
24 are skilled in the art at that time to
25 understand that you're mapping or

- PO did not act as its own lexicographer.
- The term must be construed according to its plain and ordinary meaning.
- A mapping file is a term of art

EX-2002, 26:22-24

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

“Mapping File”

✓ “a file or other representation that correlates data from a source to a target.”

X “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application.”

22 A. A mapping file is actually a
23 general term that's well-known for those who
24 are skilled in the art at that time to
25 understand that you're mapping or

2 correlating data from a source to a target,
3 and the mapping file itself is a
4 representation, it's not necessarily a file,
5 it could be contained within source code, it
6 could be contained within memory that you

- A mapping file is a term of art
- A POSITA would understand that a mapping file is “a file or other representation that correlates data from a source to a target.”

EX-2002, 26:22-27:6

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

“Mapping File”

✓ “a file or other representation that correlates data from a source to a target.”

X “a file or one or more tables that correlate threat model components with visual diagram components of a third party software application.”

19 Q. Okay.
20 And the purpose -- just again to
21 recap, I'm sorry, I'm just trying to make
22 notes -- but the purpose of the mapping file
23 is to correlate data from a source to a
24 destination --
25 A. That is correct.

EX-2002, 27:20-25

- A mapping file is a term of art
- A POSITA would understand that a mapping file is “a file or other representation that correlates data from a source to a target.”

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 1

Claims 1-20 Anticipated by Keenan

Overview: Keenan Discloses Claims 1-20

US011200228B2

(12) **United States Patent**
Keenan et al.

(10) Patent No.: **US 11,200,228 B2**
(45) Date of Patent: ***Dec. 14, 2021**

(54) **INTEGRATED OBJECT ENVIRONMENT SYSTEM AND METHOD**

(71) Applicant: **American International Group, Inc.**, New York, NY (US)

(72) Inventors: **Sean C. Keenan**, Reading, CT (US); **James G. Barrett**, New York, NY (US); **Gordon Cooper**, Spring, TX (US)

(73) Assignee: **AMERICAN INTERNATIONAL GROUP, INC.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 87 days. This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15957,828**
(22) Filed: **Apr. 19, 2018**

(65) **Prior Publication Data**
US 2018/0307780 A1 Oct. 25, 2018

Related U.S. Application Data
(60) Provisional application No. 62/487,370, filed on Apr. 19, 2017.

(51) **Int. Cl.**
G06F 16/242 (2019.01)
G06F 16/904 (2019.01)
(Continued)

(52) **U.S. Cl.**
CPC — **G06F 16/2443** (2019.01); **G06F 16/2445** (2019.01); **G06F 16/289** (2019.01); **G06F 16/904** (2019.01); **G06F 16/9024** (2019.01); **G06F 3/04842** (2013.01); **G06F 2203/04806** (2013.01)

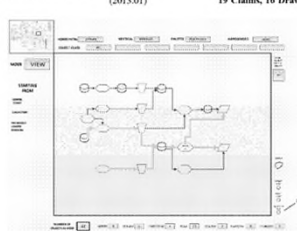
(58) **Field of Classification Search**
CPC: **G06F 3/0484**; **G06F 3/04842**; **G06F 3/0485**; **G06F 16/904**; **G06F 16/289**; **G06F 16/9024**; **G06F 2203/04806**; **G06F 2203/048**
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
6,889,309 B1 * 5/2005 Oliveira G06F 16/10 707/117/51
2004/0039745 A1 * 2/2004 Evans G06F 16/289 707/999.1
(Continued)

OTHER PUBLICATIONS
"AI shapes," Feb. 24, 2016, Microsoft, retrieved via Wayback Machine, pp. 1-5 (2016).
(Continued)

ABSTRACT
(57) A system and method are described to create and use an Integrated Object Environment (IOE) running in a graph database environment. Uses include storing, revealing and maintaining value and risk of information assets, such as the topology of an analytical infrastructure in query-driven, graph database. A graphical user interface is described to permit importation, viewing, modification and querying in the IOE.

19 Claims, 16 Drawing Sheets



IriusRisk
Ex. 1004 - Page 1

Overview:

- Keenan is Prior Art:
 - Keenan is supported by its provisional
 - The '366 is not entitled to its priority date
- Keenan Discloses Threats:
 - Keenan discloses the nature of a threat
 - Keenan does identify specific threats
 - Keenan's risk analysis includes threats
- Keenan Discloses Dependent Claims

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Overview: Keenan Discloses Claims 1-20

US011200228B2

(12) **United States Patent**
Keenan et al.

(10) **Patent No.:** **US 11,200,228 B2**
(45) **Date of Patent:** ***Dec. 14, 2021**

(54) **INTEGRATED OBJECT ENVIRONMENT SYSTEM AND METHOD**

(71) **Applicant:** American International Group, Inc., New York, NY (US)

(72) **Inventors:** Sean C. Keenan, Reading, CT (US); James G. Barrett, New York, NY (US); Gordon Cooper, Spring, TX (US)

(73) **Assignee:** AMERICAN INTERNATIONAL GROUP, INC., New York, NY (US)

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 87 days. This patent is subject to a terminal disclaimer.

(21) **Appl. No.:** 15957,828

(22) **Filed:** Apr. 19, 2018

(65) **Prior Pub.:** a son Data US 2018/0307780 A1 Oct. 25, 2018

Related U.S. Application Data

(60) Provisional application No. 62/487,370, filed on Apr. 19, 2017.

(51) **Int. Cl.** (2019.01)
G06F 16/242 (2019.01)
G06F 16/904 (2019.01)
(Continued)

(52) **U.S. Cl.** (2019.01); **G06F 16/243** (2019.01); **G06F 16/245** (2019.01); **G06F 16/289** (2019.01); **G06F 16/904** (2019.01); **G06F 16/9024** (2019.01); **G06F 3/04842** (2013.01); **G06F 2203/04806** (2013.01)

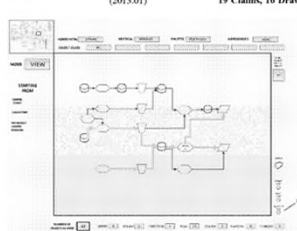
(58) **Field of Classification Search**
CPC: G06F 3/0484; G06F 3/04842; G06F 3/0485; G06F 16/904; G06F 16/289; G06F 16/9024; G06F 2203/04806; G06F 2203/048
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
6,889,309 B1 * 5/2005 Oliveira G06F 16/10 707/117/51
2004/0039745 A1 * 2/2004 Evans G06F 16/289 707/999.1
(Continued)

OTHER PUBLICATIONS
"AI shapes," Feb. 24, 2016, Microsoft, retrieved via Wayback Machine, pp. 1-5 (2016).
(Continued)

ABSTRACT
(57) A system and method are described to create and use an Integrated Object Environment (IOE) running in a graph database environment. Uses include storing, revealing and maintaining value and risk of information assets, such as the topology of an analytical infrastructure in query-driven, graph database. A graphical user interface is described to permit importation, viewing, modification and querying in the IOE.

19 Claims, 16 Drawing Sheets



IriusRisk
Ex. 1004 - Page 1

Overview:

- Keenan is Prior Art:
 - Keenan is supported by its provisional
 - The '366 is not entitled to its priority date
- Keenan Discloses Threats:
 - Keenan discloses the nature of a threat
 - Keenan does identify specific threats
 - Keenan's risk analysis includes threats
- Keenan Discloses Dependent Claims

DEMONSTRATIVE EXHIBIT - NOT EVIDENCE

Keenan is Prior Art

- PO's Sur-Reply does not dispute that Keenan is supported by its provisional.
- Petitioner was entitled to raise this argument in reply.
- *Innovative Growers Equip., Inc. v. Pipp Mobile Storage Sys., Inc.*, No. IPR2022-00893, 2023 WL 7107846, at *18 (P.T.A.B. Oct. 27, 2023)

*18 In order for Hutto to be accorded an August 4, 2017 filing date based on its provisional application, Petitioner must establish that the specification of the Hutto *provisional* application contains a written description of the invention and the manner and process of making and using it, in such full, clear, concise, and exact terms to enable an ordinarily skilled artisan to practice the invention *claimed* in the Hutto *non-provisional* application, which in this proceeding became the Hutto patent. *Dynamic Drinkware, LLC v. National Graphics, Inc.*, 800 F.3d 1375, 1378 (Fed. Cir. 2015) (citing *New Railhead Mfg., L.L.C. v. Vermeer Mfg. Co.*, 298 F.3d 1290, 1294 (Fed. Cir. 2002)). The burden is on Petitioner “to prove that the prior art [Hutto] patent was entitled to the filing date of its provisional application.”

Patent Owner asserts that Petitioner's effort to establish that the Hutto patent is a prior art reference was untimely because it was not included in the Petition. Sur-reply 4 (Petitioner “did not attempt to timely establish any disclosure of Hutto to be prior art until after institution”). We disagree.

Dynamic Drinkware is very clear on this point. The petitioner in an *inter partes* review does not have the burden of producing evidence that the effective date of an asserted reference patent relates back to its claimed provisional application until after a patentee challenges the prior art status of the asserted reference.

Keenan is Prior Art

Innovative Growers Equip., Inc. v. Pipp Mobile Storage Sys., Inc., No. IPR2022-00893, 2023 WL 7107846, at *18 (P.T.A.B. Oct. 27, 2023)

Dynamic Drinkware is very clear on this point. The petitioner in an *inter partes* review does not have the burden of producing evidence that the effective date of an asserted reference patent relates back to its claimed provisional application until after a patentee challenges the prior art status of the asserted reference.

Dynamic Drinkware, LLC v. Nat'l Graphics, Inc., 800 F.3d 1375, 1381 (Fed. Cir. 2015)

4 First, we find that Dynamic did not waive its argument that Raymond was entitled to an earlier effective date. As discussed *supra*, Dynamic did not have the burden of producing evidence relating to the Raymond provisional application until after National Graphics made its argument regarding reduction to practice. As a result, it was not necessary for Dynamic to prove in its petition that Raymond was entitled to the filing date of its provisional application. Thus, there was no waiver.

Overview: Keenan Discloses Claims 1-20

US011200228B2

(12) **United States Patent**
Keenan et al.

(10) **Patent No.:** **US 11,200,228 B2**
(45) **Date of Patent:** ***Dec. 14, 2021**

(54) **INTEGRATED OBJECT ENVIRONMENT SYSTEM AND METHOD**

(71) **Applicant:** American International Group, Inc., New York, NY (US)

(72) **Inventors:** Sean C. Keenan, Reading, CT (US); James G. Barrett, New York, NY (US); Gordon Cooper, Spring, TX (US)

(73) **Assignee:** AMERICAN INTERNATIONAL GROUP, INC., New York, NY (US)

(*) **Notice:** Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 87 days.
This patent is subject to a terminal disclaimer.

(21) **Appl. No.:** 15957,828
(22) **Filed:** Apr. 19, 2018
(65) **Prior Publication Data**
US 2018/0307780 A1 Oct. 25, 2018
Related U.S. Application Data
(60) Provisional application No. 62/487,370, filed on Apr. 19, 2017.

(51) **Int. Cl.**
G06F 16/242 (2019.01)
G06F 16/904 (2019.01)
(Continued)

(52) **U.S. Cl.**
CPC — **G06F 16/2443** (2019.01); **G06F 16/2445** (2019.01); **G06F 16/289** (2019.01); **G06F 16/904** (2019.01); **G06F 16/9024** (2019.01); **G06F 3/04842** (2013.01); **G06F 2203/04806** (2013.01)

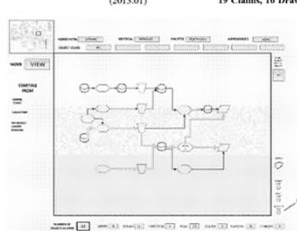
(58) **Field of Classification Search**
CPC: G06F 3/0484; G06F 3/04842; G06F 3/0485; G06F 16/904; G06F 16/289; G06F 16/9024; G06F 2203/04806; G06F 2203/048
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
6,889,309 B1 * 5/2005 Oliveira G06F 16/10 707/117/51
2004/0039745 A1 * 2/2004 Evans G06F 16/289 707/999.1
(Continued)

OTHER PUBLICATIONS
"AI shapes," Feb. 24, 2016, Microsoft, retrieved via Wayback Machine, pp. 1-5 (2016).
(Continued)

ABSTRACT
(57)
A system and method are described to create and use an Integrated Object Environment (IOE) running in a graph database environment. Uses include storing, revealing and maintaining value and risk of information assets, such as the topology of an analytical infrastructure in query-driven, graph database. A graphical user interface is described to permit importation, viewing, modification and querying in the IOE.

19 Claims, 16 Drawing Sheets



IriusRisk
Ex. 1004 - Page 1

Overview:

- Keenan is Prior Art:
 - Keenan is supported by its provisional
 - **The '366 is not entitled to its priority date**
- Keenan Discloses Threats:
 - Keenan discloses the nature of a threat
 - Keenan does identify specific threats
 - Keenan's risk analysis includes threats
- Keenan Discloses Dependent Claims

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Keenan is Prior Art

- PO's Sur-Reply does not dispute that the '366 Patent is not entitled to its priority date.
- Petitioner was entitled to raise this argument in reply
- *United Therapeutics Corp. v. Liquidia Techs., Inc.*, 2023 WL 8794633, at *3 (Fed. Cir. Dec. 20, 2023)

As the Board recognized, Liquidia's IPR petition asserted that each of the Voswinckel abstracts was publicly presented or published at least one year before the priority date of the '793 patent, making each of them printed publications within the meaning of § 102(b). See *Decision* at *4; see also Petition at 22, 24, J.A. 133, 135. UTC first challenged the sufficiency of those grounds in its post-institution Patent Owner Response. See Patent Owner Response at 11–18, J.A. 372–79. Thereafter, in its Reply, Liquidia asserted, with additional evidence, that both Voswinckel abstracts were publicly presented and sufficiently disseminated at conferences prior to the critical date such that they qualified as printed publications. See J.A. 471, 474–75.

The Board found that Liquidia's arguments and evidence raised in its Reply were not untimely as they were made in direct response to UTC's attack on the prior art status of the abstracts first raised in its post-institution Patent Owner Response. *Decision* at *4, J.A. 10. This conclusion was not an abuse of the Board's discretion. See *Anacor Pharms., Inc. v. lancu*, 889 F.3d 1372, 1380–82 (Fed. Cir. 2018) (explaining that the petitioner “may introduce new evidence after the petition stage if the evidence is a legitimate reply to evidence introduced by the patent owner”); see also *Axonics*, 75 F.4th at 1380 (explaining that a petitioner's entitlement to respond to new arguments made in a patent owner response is consistent with SAS). As the Board observed, Liquidia's arguments were not inconsistent with, and therefore not new over, the grounds raised in its IPR petition—that the Voswinckel abstracts were publicly accessible prior to the critical date. *Ericsson Inc. v. Intell. Ventures I LLC*, 901 F.3d 1374, 1380 (Fed. Cir. 2018) (“[T]he Board has discretion to determine whether a petition for *inter partes* review identified the specific evidence relied on in a reply and when a reply contention crosses the line from the responsive to the new.”). Accordingly, we conclude that the Board did not abuse its discretion in considering the arguments and evidence raised in Liquidia's Reply.

Petition at 10; POR 47-49; Reply at 10-12; Sur-Reply at 8-9

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Overview: Keenan Discloses Claims 1-20

US011200228B2

(12) **United States Patent**
Keenan et al.

(10) Patent No.: **US 11,200,228 B2**
(45) Date of Patent: ***Dec. 14, 2021**

(54) **INTEGRATED OBJECT ENVIRONMENT SYSTEM AND METHOD**

(71) Applicant: **American International Group, Inc.**, New York, NY (US)

(72) Inventors: **Sean C. Keenan**, Reading, CT (US); **James G. Barrett**, New York, NY (US); **Gordon Cooper**, Spring, TX (US)

(73) Assignee: **AMERICAN INTERNATIONAL GROUP, INC.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 87 days. This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15957,828**
(22) Filed: **Apr. 19, 2018**

(65) **Prior Publication Data**
US 2018/0307780 A1 Oct. 25, 2018

Related U.S. Application Data
(60) Provisional application No. 62/487,370, filed on Apr. 19, 2017.

(51) Int. Cl. (2019.01)
G06F 16/242
G06F 16/904
(Continued)

(52) U.S. Cl. (2019.01); **G06F 16/243**
CPC: **G06F 16/243** (2019.01); **G06F 16/245** (2019.01); **G06F 16/289** (2019.01); **G06F 16/904** (2019.01); **G06F 16/9024** (2019.01); **G06F 3/04842** (2013.01); **G06F 2203/04806** (2013.01)

(58) Field of Classification Search
CPC: **G06F 3/0484**; **G06F 3/04842**; **G06F 3/0485**; **G06F 16/904**; **G06F 16/289**; **G06F 16/9024**; **G06F 2203/04806**; **G06F 2203/048**
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
6,889,309 B1 * 5/2005 Oliveira **G06F 16/10**
707/117/51
2004/0039745 A1 * 2/2004 Evans **G06F 16/289**
707/999.1
(Continued)

OTHER PUBLICATIONS
"AI shapes," Feb. 24, 2016, Microsoft, retrieved via Wayback Machine, pp. 1-5 (2016).
(Continued)

ABSTRACT
(57)
A system and method are described to create and use an Integrated Object Environment (IOE) running in a graph database environment. Uses include storing, revealing and maintaining value and risk of information assets, such as the topology of an analytical infrastructure in query-driven, graph database. A graphical user interface is described to permit importation, viewing, modification and querying in the IOE.

19 Claims, 16 Drawing Sheets

IriusRisk
Ex. 1004 - Page 1

Overview:

- Keenan is Prior Art:
 - Keenan is supported by its provisional
 - The '366 is not entitled to its priority date
- Keenan Discloses Threats:
 - Keenan discloses the nature of a threat
 - Keenan does identify specific threats
 - Keenan's risk analysis includes threats
- Keenan Discloses Dependent Claims

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Keenan Discloses Independent Claims 1, 8, 16

- The only dispute for the independent claims is whether Keenan discloses threats
- Keenan discloses using color to categorize risk based on the type of risk (i.e., cyber, environmental, accidental). These “types of risk” stem from the underlying threat—i.e., cyber threats, environmental threats, and accidental threats.
- There is no requirement in the claims of the '366 patent that a specific threat must be identified.
- PO presents no evidence to the contrary.

40 In the example of FIG. 7, a Model Risk view 702 uses color to represent a range of risk based on the risk characteristics for models in the view. A Business Affiliation view 704 uses color to represent differences in accountability for different business departments. A Business Unit view 706
45 uses color to represent business division accountability. A Technical Risk Measurement view 708 uses color to represent different types of risk (e.g., cyber, environmental, accidental, etc.). An Allocated Business Contribution view 710 uses color to represent aggregate attribution of business
50 value to production chains (e.g., to indicate objects contributing to multiple business uses).

EX-1004, 16:40- 51

Keenan Discloses Independent Claims 1, 8, 16

- The only dispute for the independent claims is whether Keenan discloses threats
- Keenan discloses using color to categorize risk based on the type of risk (i.e., cyber, environmental, accidental). These “types of risk” stem from the underlying threat—i.e., cyber threats, environmental threats, and accidental threats.
- There is no requirement in the claims of the '366 patent that a specific threat must be identified.
- PO presents no evidence to the contrary.

Keenan demonstrates that its risk measurement and display includes a determination of threats where Keenan discloses a risk measurement view that uses [] color to “represent different types of risk (e.g., cyber, environmental, accidental, etc.).” [Ex. 1004], 16:40–51. [The skilled artisan] 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 discloses threats within its risk analysis. Moreover, [the skilled artisan] would understand that risk is a function of threats exploiting vulnerabilities to obtain, damage, or destroy assets. In other words, threat modeling is used to identify risk.

Petition at 23-24, 28

Petition at 23-24, 28; EX-1003, ¶¶79, 82; Reply at 12-18; Institution Decision at 18-19

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Keenan Discloses Independent Claims 1, 8, 16

- Given risk, a POSITA knows that threats underlie that risk.
- There is no requirement in the claims of the '366 patent that a specific threat must be identified.

8 But if you are just given the
9 risk, can you derive the threat from that?
10 MR. MIDDLETON: Objection.
11 Form.
12 A. You have -- well, some possible
13 threats. Some possible threats. And I gave
14 an example already. The example I gave was
15 unavailability. I have a risk of
16 unavailability. But what's the threat?
17 Well, the threat could be several things.
18 It could be a denial-of-service attack, it
19 could be the thing I'm relying on is not
20 available to me. So, therefore, I have that
21 risk, and so I don't have exactly a one to

EX-2002, 61:8-21

Petition at 23-24, 28; EX-1003, ¶¶ 79, 82; Reply at 12-18; Institution Decision at 9

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Overview: Keenan Discloses Claims 1-20

US011200228B2

(12) **United States Patent**
Keenan et al.

(10) Patent No.: **US 11,200,228 B2**
(45) Date of Patent: ***Dec. 14, 2021**

(54) **INTEGRATED OBJECT ENVIRONMENT SYSTEM AND METHOD**

(71) Applicant: **American International Group, Inc.**,
New York, NY (US)

(72) Inventors: **Sean C. Keenan**, Reading, CT (US);
James G. Barrett, New York, NY (US);
Gordon Cooper, Spring, TX (US)

(73) Assignee: **AMERICAN INTERNATIONAL GROUP, INC.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 87 days.
This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15957,828**
(22) Filed: **Apr. 19, 2018**

(65) **Prior Publication Data**
US 2018/0307780 A1 Oct. 25, 2018

Related U.S. Application Data
(60) Provisional application No. 62/487,370, filed on Apr. 19, 2017.

(51) **Int. Cl.**
G06F 16/242 (2019.01)
G06F 16/904 (2019.01)
(Continued)

(52) **U.S. Cl.**
CPC: **G06F 16/2443** (2019.01); **G06F 16/2445** (2019.01); **G06F 16/289** (2019.01); **G06F 16/904** (2019.01); **G06F 16/9024** (2019.01); **G06F 3/04842** (2013.01); **G06F 2203/04806** (2013.01)

(58) **Field of Classification Search**
CPC: **G06F 3/0484**; **G06F 3/04842**; **G06F 3/0485**; **G06F 16/904**; **G06F 16/289**; **G06F 16/9024**; **G06F 2203/04806**; **G06F 2203/048**
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
6,889,309 B1 * 5/2005 Oliveira G06F 16/10
707/117/11
2004/0039745 A1 * 2/2004 Evans G06F 16/289
707/999.1
(Continued)

OTHER PUBLICATIONS
"AI shapes," Feb. 24, 2016, Microsoft, retrieved via Wayback Machine, pp. 1-5 (2016).
(Continued)

ABSTRACT
(57)
A system and method are described to create and use an Integrated Object Environment (IOE) running in a graph database environment. Uses include storing, revealing and maintaining value and risk of information assets, such as the topology of an analytical infrastructure in query-driven, graph database. A graphical user interface is described to permit importation, viewing, modification and querying in the IOE.

19 Claims, 16 Drawing Sheets

IriusRisk
Ex. 1004 - Page 1

Overview:

- Keenan is Prior Art:
 - Keenan is supported by its provisional
 - The '366 is not entitled to its priority date
- Keenan Discloses Threats:
 - Keenan discloses the nature of a threat
 - **Keenan does identify specific threats**
 - Keenan's risk analysis includes threats
- Keenan Discloses Dependent Claims

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Keenan Discloses Claims 1-20

- Keenan does identify specific threats
- For example, Keenan discloses an example of a model named “European Windstorm Model.” EX-1004, 9:42-47.
- A POSITA would understand that natural disasters are threats that could be included in a threat model.
- PO’s Sur-Reply does not address this argument

Q I mean, a natural disaster, that could be one or more potential events, right?

A It could be, yes.

Q And a natural disaster could cause adverse effects, right?

A There is the potential that an earthquake, for example, a natural disaster would have an adverse effect on the security of the system. So in that circumstance, yes, I would agree that could be part of a threat model.

EX-1015, 53:1-10, 84:3-20.

Petition at 23-24, 28; EX-1003, ¶¶79, 82; Reply at 12-18; EX-1004, 9:42-47

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Overview: Keenan Discloses Claims 1-20

US011200228B2

(12) **United States Patent**
Keenan et al.

(10) Patent No.: **US 11,200,228 B2**
(45) Date of Patent: ***Dec. 14, 2021**

(54) **INTEGRATED OBJECT ENVIRONMENT SYSTEM AND METHOD**

(71) Applicant: **American International Group, Inc.**,
New York, NY (US)

(72) Inventors: **Sean C. Keenan**, Reading, CT (US);
James G. Barrett, New York, NY (US);
Gordon Cooper, Spring, TX (US)

(73) Assignee: **AMERICAN INTERNATIONAL GROUP, INC.**, New York, NY (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 87 days.
This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15957,828**
(22) Filed: **Apr. 19, 2018**

(65) **Prior Publication Data**
US 2018/0307780 A1 Oct. 25, 2018

Related U.S. Application Data
(60) Provisional application No. 62/487,370, filed on Apr. 19, 2017.

(51) Int. Cl. (2019.01)
G06F 16/242 (2019.01)
G06F 16/904 (2019.01)
(Continued)

(52) U.S. Cl. (2019.01); **G06F 16/243** (2019.01); **G06F 16/245** (2019.01); **G06F 16/289** (2019.01); **G06F 16/904** (2019.01); **G06F 16/9024** (2019.01); **G06F 3/04842** (2013.01); **G06F 2203/04806** (2013.01)

(58) **Field of Classification Search**
CPC: **G06F 3/0484**; **G06F 3/04842**; **G06F 3/0485**; **G06F 16/904**; **G06F 16/289**; **G06F 16/9024**; **G06F 2203/04806**; **G06F 2203/048**
See application file for complete search history.

(56) **References Cited**
U.S. PATENT DOCUMENTS
6,889,309 B1 * 5/2005 Oliveira G06F 16/10
707/117/11
2004/0039745 A1 * 2/2004 Evans G06F 16/289
707/999.1
(Continued)

OTHER PUBLICATIONS
"AI shapes," Feb. 24, 2016, Microsoft, retrieved via Wayback Machine, pp. 1-5 (2016).
(Continued)

ABSTRACT
(57)
A system and method are described to create and use an Integrated Object Environment (IOE) running in a graph database environment. Uses include storing, revealing and maintaining value and risk of information assets, such as the topology of an analytical infrastructure in query-driven, graph database. A graphical user interface is described to permit importation, viewing, modification and querying in the IOE.

19 Claims, 16 Drawing Sheets

IriusRisk
Ex. 1004 - Page 1

Overview:

- Keenan is Prior Art:
 - Keenan is supported by its provisional
 - The '366 is not entitled to its priority date
- Keenan Discloses Threats:
 - Keenan discloses the nature of a threat
 - Keenan does identify specific threats
 - **Keenan's risk analysis includes threats**
- Keenan Discloses Dependent Claims

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Keenan's Risk Analysis Includes Threats

- There is no dispute that a POSITA would understand that “a risk analysis requires some form of threat analysis.”
- The definition of “risk” that PO’s expert Dr. Nielson applied in his report is “the potential impact on a system due to a threat that occurs coupled with the likelihood that a threat will occur.” EX-1015, 61:8-62:12 (“likelihood times impact is the way I’ve been using ‘risk,’ both in my career and in this patent.”)

Q And how do you perform a risk analysis?

A Again, that can be somewhat context-specific, but typically a risk analysis requires some form of threat analysis, and then based on the threat analysis, you assess risk that's either quantitative, or it can be qualitative, as in you can prioritize the risks. But it's based on assessment of threats.

EX-1015, 9:22-10:7.

The Definition of “Risk” Includes Threats

- Both parties experts agree that the definition of “risk” is “the potential impact on a system due to a threat that occurs coupled with the likelihood that a threat will occur.”

Q. And how would you define risk from the perspective of person of skill in the art in May of 2017? How would you define risk?

A. Sure. Risk is a -- essentially a product or in general relation to threat modeling is a product of probability, the possibility, probability of a threat being realized as well as the impact of that threat. If it's a major threat that's going

EX-2002, 24:11-20

Q And this Paragraph 80, you write, "Whereas, risk is the potential impact on a system due to a threat that occurs coupled with the likelihood that a threat will occur"; is that right?

A Correct.

Q Is this the definition of risk that the '366 patent uses?

A The '366 patent does not provide a definition, but this definition is compatible with how it is used.

EX-1015, 61:8-62:12

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Dr. Nielson Attempted to Change His Definition

Q So you agree with this definition?

A The definition of -- I just want to -- risk likelihood times impact is the way I've been using "risk," both in my career and in this patent.

Q And that's the definition you applied in your report?

A Yes.

EX-1015, 61:8-62:12

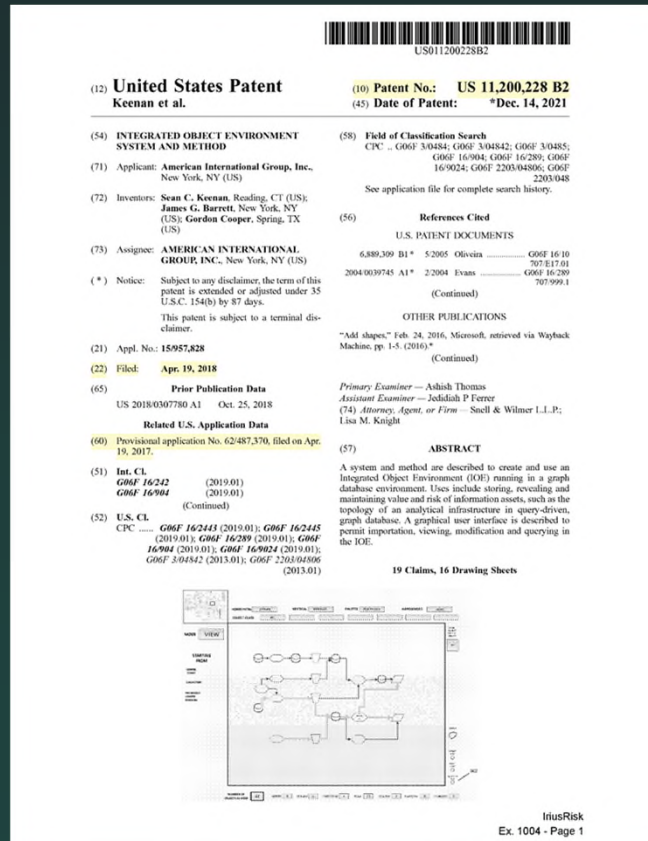
Q Dr. Nielson, just to go back to your definition of risk and just to confirm again, your definition of risk is the likelihood of a threat by the impact of that threat; is that correct?

A No.

EX-1015, 88:9-13

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Overview: Keenan Discloses Claims 1-20



Overview:

- Keenan is Prior Art:
 - Keenan is supported by its provisional
 - The '366 is not entitled to its priority date
- Keenan Discloses Threats:
 - Keenan discloses the nature of a threat
 - Keenan does identify specific threats
 - Keenan's risk analysis includes threats
- Keenan Discloses Dependent Claims

Keenan Discloses Dependent Claims 2-3, 9-10, 17-18

- Claims 2, 9, and 17 require that the mapping file is stored on “the one or more computing devices.”

It is understandable to those skilled in the art that all or a part of steps of the processes in the preceding embodiments is preferably implemented by relevant 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; EX-1003, ¶109; Petition, 41-42.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Keenan Discloses Dependent Claims 2-3, 9-10, 17-18

3. The method of claim 1, wherein the one or more mapping files comprise one or more tables stored within the one or more databases.

- For Claims 3, 10, and 18 PO does not address that Petition's argument that Keenan teaches a "characteristics table" with "Flow Objects" that allow a user to make connections on the screen of the GUI. Petition, 42; POR, 41-44.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Keenan Discloses Dependent Claim 5

5. The method of claim 1, wherein determining, for the subset of third party diagram components, correlated threat model 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 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.

- PO wholly ignores the Petition's argument that "a POSITA would further understand that Keenan discloses a system that checks for default titles or user-defined name matches in either order." Petition, 43-44

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Keenan Discloses Dependent Claims 6 and 14

6. The method of claim 5, further comprising, 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.

- PO again ignores the Petition's actual arguments
 - (1) that “[a] POSITA would understand that Keenan’s system creates a placeholder component where no exact match is found for the third party component object the user adds to Keenan’s IOE, and then displays that placeholder in the IOE, indicating no match was found”; and
 - (2) that a POSITA would understand Keenan’s disclosure of temporary topology in memory discloses this claims. Petition, 45-47.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 2: Zheng in Combination With Baker and Jones Render the Challenged Claims Obvious

Zheng In Combination With Baker Discloses Claims

US010503907B2

(12) **United States Patent**
Zheng et al.

(10) **Patent No.:** US 10,503,907 B2
(45) **Date of Patent:** Dec. 10, 2019

(54) **INTELLIGENT THREAT MODELING AND VISUALIZATION**

(71) Applicant: FMR LLC, Boston, MA (US)
(72) Inventors: Erkang Zheng, Cary, NC (US); Jason Kao, Cary, NC (US)
(73) Assignee: FMR LLC, Boston, MA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 499 days.

(21) Appl. No.: 15/979,129
(22) Filed: Dec. 14, 2016

(65) **Prior Publication Data**
US 2017/0169230 A1 Jun. 15, 2017

Related U.S. Application Data
(60) Provisional application No. 62/266,827, filed on Dec. 14, 2015.

(51) **Int. Cl.**
G06F 11/00 (2006.01)
G06F 21/57 (2013.01)
G06F 17/50 (2006.01)
G06N 20/00 (2019.01)

(52) **U.S. Cl.**
CPC — G06F 21/577 (2013.01); G06F 17/5009 (2013.01); G06N 20/00 (2019.01)

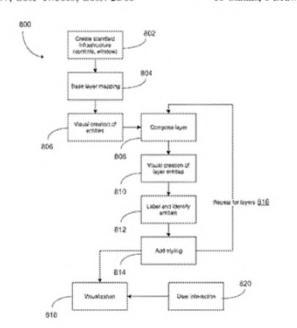
(58) **Field of Classification Search**
CPC — G06F 21/577; G06F 17/5009; G06N 20/00

(56) **References Cited**
U.S. PATENT DOCUMENTS
2007/0186284 A1 * 8/2007 McConnell G06F 21/55
2017/0060572 A1 * 3/2017 Sripathan G06F 8/70
* cited by examiner

Primary Examiner — Mohammad W Rem
(74) **Attorney, Agent, or Firm** — Proskauer Rose LLP

(57) **ABSTRACT**
A computer-implemented system is provided for visualizing and analyzing security threats in a suite of software applications. The system includes 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. The components are displayed in a base layer of the map. The system also includes a threat modeling module configured to automatically identify one or more security threats in the suite of software applications. The threat modeling module is adapted to interact with the visualization module to graphically depict on the computer display the one or more security threats on the map in a threat modeling layer. The system further includes a security controls module configured to implement security controls for mitigating the one or more security threats identified by the threat modeling module.

16 Claims, 6 Drawing Sheets

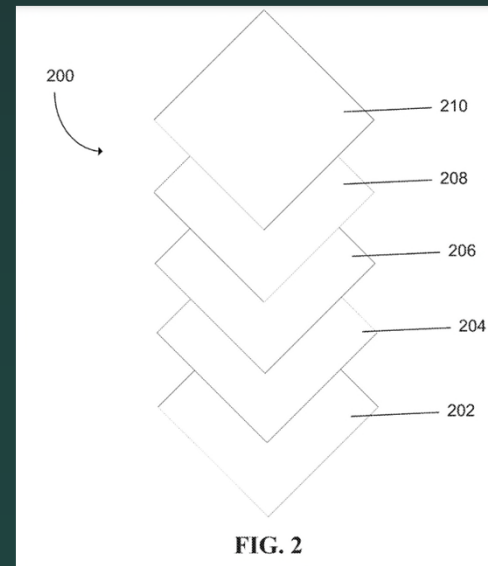


The flowchart illustrates the process of threat modeling and visualization. It begins with a box labeled 'Create/refresh visualization, controls, entities' (802), which leads to 'Threat modeling' (804). From 'Threat modeling', the process flows to 'Visual inspection of entities' (806), then to 'Computer layer' (808), and finally to 'Visual inspection of threat entities' (810). From 'Visual inspection of threat entities', the process flows to 'Layer and security entities' (812), then to 'Add policy' (814), and finally to 'User interaction' (820). A feedback loop labeled 'Review for errors' (816) connects 'Visual inspection of threat entities' back to 'Threat modeling'. The process concludes with 'Visualization' (910).

IirusRisk
Ex. 1005 - Page 1

Overview:

- Zheng Discloses a Mapping File
- It would have been obvious to combine Zheng and Baker



DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Zheng Discloses a Mapping File

- Zheng's disclosure goes beyond mere cartography. Zheng's cartographic mapping is within the base layer only:
 - EX-1005, 3:28-31 (“by utilizing a visualization approach like cartography, application architecture can be represented.”).
 - EX-1005, 3:66-4:2 (“the multilayered structure 200 includes four different overlaying layers, with the base layer 202 representing at least a portion of a company's application architecture.”).

Q So doesn't that mean it's adding more than basic cartographical details?

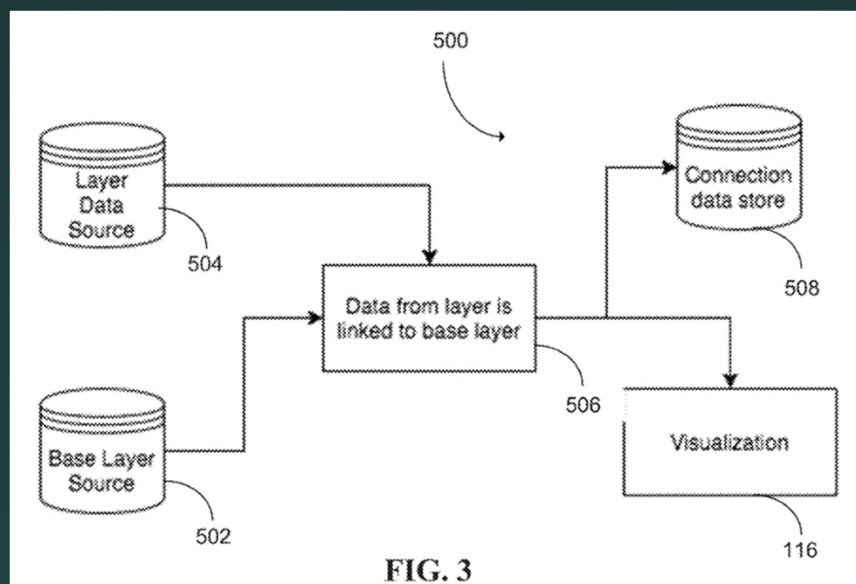
A It identifies traffic, for example, as something beyond basic cartographical details. And, I mean, if we're going back to what we talked about a few minutes ago, this is just the analogy of overlaying the active attacks on top of the system architecture.

EX-1015, 128:14-21

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Zheng Discloses a Mapping File

- Layers are linked or mapped together to provide additional details that overlay on the architecture of the base layer—and this linkage goes far beyond simple cartography.



EX-1005, Fig. 3

Petition, 63 (citing, e.g., 5:18-24); EX1003, ¶160 (discussing threat modeling layer's visualizations).

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Zheng Discloses a Mapping File

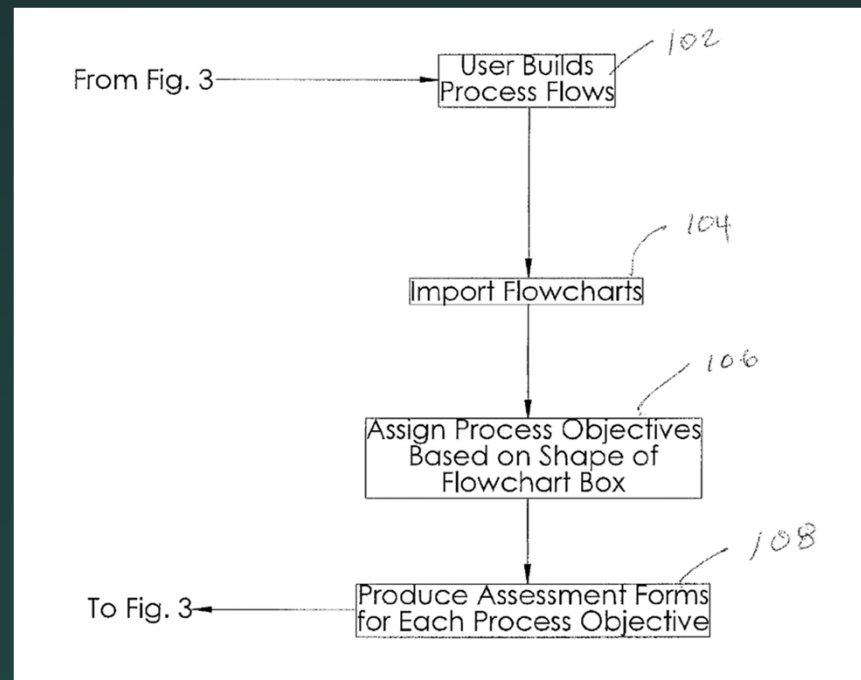
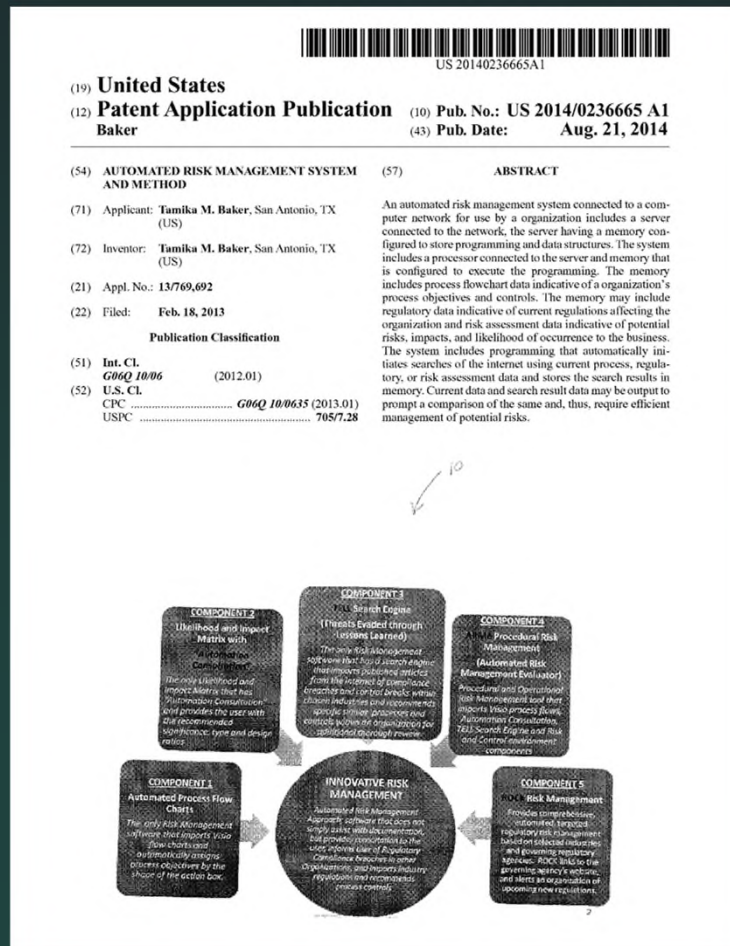
- Zheng discloses the use of a mapping file for interactions between the layers.
- Zheng discloses that a database table may be used to store data for each layer and for each possible combination and interaction of the layers. EX-1005, 8:25-38
- The '366 patent explicitly acknowledges that a database table is a type of mapping file. EX-1001, 38:33-42 (where “one or more tables of the database are used for the mapping file(s), each table is, for the purposes of this disclosure, a “file.”).

In some embodiments, **at least one database table** is used to store data for each layer and for each possible combination/interaction of the layers. As shown in FIG. 3, data for the base layer 202 can be stored in a base layer database table 502. Data for one or more additional layers can be stored in their corresponding database tables 504. Further, data representing various combinations/interactions of the layers can be stored in their corresponding database tables 504. For example, given 3 layers A (e.g., representing the threat modeling layer 204), B (e.g., representing the security controls layer 206), and C (e.g., representing the threat update layer 208), six database tables can be generated to represent the combinations {A, B, C, AB, AC, BC, ABC} that are stored in the database tables 504.

EX-1005, 8:25-38

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

It would have been obvious to combine Zheng and Baker



DEMONSTRATIVE EXHIBIT - NOT EVIDENCE

It would have been obvious to combine Zheng and Baker

- Baker's system also discloses a mapping file. Baker discloses using shapes to represent components of its native system. EX-1006, ¶[0025] ("As are understood by persons involved in risk management processes, a risk management flowchart utilizes symbols of various shapes to indicate actions, determinations, or other elements of an activity or evaluation").
- Baker then discloses importing third party visual diagram components (i.e., Visio shapes and flowcharts) into its system, which are used in place of Baker's native shapes and formats. *Id.* ("At step 106, the processor 20 acts to automatically assign or associate predetermined objectives or controls according to the shapes of the imported flowcharts.").

Software exists for converting a diagram file of one type to another type of diagram file, though not into a threat model. For example, LUCIDCHART, SMARTDRAW, and EDRAWSOFT are programs which will convert a MICROSOFT VISIO file into another file type (for example importing the visual elements and retaining some diagram features of the original VISIO file) but without creating an associated threat model.

EX-1001, 2:47-54

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 3: The References of Ground 2 In Further View of Galliano

Galliano Discloses Claim 2

US 10,681,068 B1

(12) **United States Patent**
Galliano et al.

(10) Patent No.: **US 10,681,068 B1**
(45) Date of Patent: **Jun. 9, 2020**

(54) **SYSTEM AND METHOD FOR ANALYZING DATA AND USING ANALYZED DATA TO DETECT CYBER THREATS AND DEFEND AGAINST CYBER THREATS**

(71) Applicant: Christopher Galliano, New Orleans, LA (US); Raed Alshaiwet, Louisville, TX (US); Kent Laureen, Slidell, LA (US)

(72) Inventors: Christopher Galliano, New Orleans, LA (US); Raed Alshaiwet, Louisville, TX (US); Kent Laureen, Slidell, LA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 199 days.

(21) Appl. No.: 15/398,367
(22) Filed: Jan. 4, 2017

Related U.S. Application Data
(60) Provisional application No. 62/566,947, filed on Jul. 26, 2016.

(51) Int. Cl. **H04L 29/06** (2006.01); **G06F 30/20** (2020.01)
(52) U.S. Cl. **H04L 63/1425** (2013.01); **G06F 30/20** (2020.01); **H04L 63/1433** (2013.01)
(57) Field of Classification Search CPC: H04L 63/1416; H04L 63/1408; H04L 63/1441; H04L 63/1438; G06F 21/552

References Cited
U.S. PATENT DOCUMENTS
2016/0191559 A1* 6/2016 Mhase H04L 63/1416 726/23
2017/0126727 A1* 5/2017 Beam H04L 63/20 726/23
2017/0237752 A1* 8/2017 Gompaly H04L 63/1416 726/23
* cited by examiner

ABSTRACT
(57) A system and method for joining various cyber security threat data sources into a single threat data model, analyzing this threat data and storing the data in a specific data model, processing the data to standardize, minimize, interpret and catalogue the threat data, creating a meta-model based on the cyber threat data model, creating executable models based on this cyber threat data enabling simulations of this cyber threat's behavior, enabling execution of these simulations to capture quantifiable data observations of cyber threat behavior in the context of logical configurations of networks, devices and systems which may be specified as models of information environments and IT infrastructures, interpreting the results of the simulations, and generating output based on the results of the simulations.

1 Claim, 7 Drawing Sheets

IriusRisk
Ex. 1008 - Page 1

U.S. Patent
Jun. 9, 2020
Sheet 3 of 7
US 10,681,068 B1

FIGURE 3

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 4: The References of Ground 2 In Further View of Keenan

Keenan Discloses Default Names and Titles

- Claims 5-6, 12-14, and 19-20 describe the use of certain names and titles for third-party components in the threat model.
- These claims are rendered obvious by the references of Ground 2 in further view of Keenan. EX-1003, ¶¶ 221-223. As shown in Ground 1, Keenan expressly discloses the use of certain names and titles for third-party elements as recited in these claims.



EX-1003, ¶¶ 221-23.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Ground 5: The References of Ground 2 In View of the Knowledge of a POSITA

A POSITA's Knowledge

- A POSITA would have understood that mapping files can be stored in a database or in a computing device without using a database as specified in claims 2, 9, and 17.
- A POSITA would have understood that third-party components can be named or titled in a certain way as specified in claims 5, 6, 12-14, and 19-20 as a matter of mere design choice. EX-1003, ¶226.



EX-1003, ¶¶ 224-27.

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

Thank you

DEMONSTRATIVE EXHIBIT – NOT EVIDENCE

53