

IriusRisk v. ThreatModeler

IPR2023-00656

Patent No. 10,713,366 B2

ThreatModeler Oral Argument

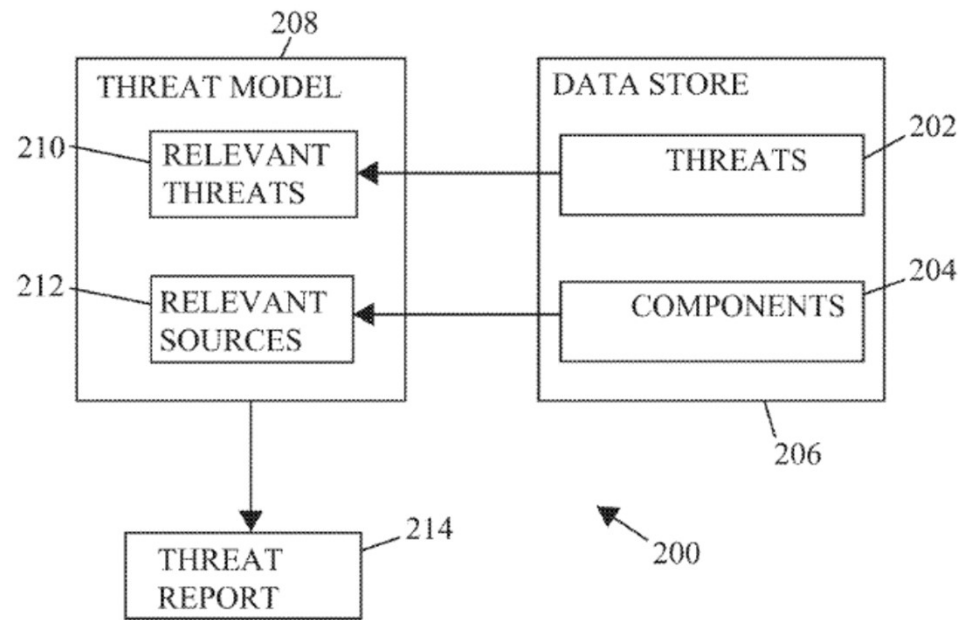
Claim Construction: “Threat”

“Threat” means:

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

EX-2009, ¶78.

“Threat”



EX-1001, Fig. 2.

Demonstrative Exhibit - Not Evidence

“Threat Model Components”

“Threat Model Components” means:

“a potential relevant source for one or more threats.”

Petition, 14; EX-1003, ¶¶40, 60; EX-2002 [Hurlbut depo. Tr.], 20:22-21:25; EX-2009, ¶93.

“Visual Representations of Threat Model Components”

“Visual Representations of the Threat Model Components”
means:

“representations of threat model components that can be
visually displayed on a diagram.”

EX-2009, ¶96.

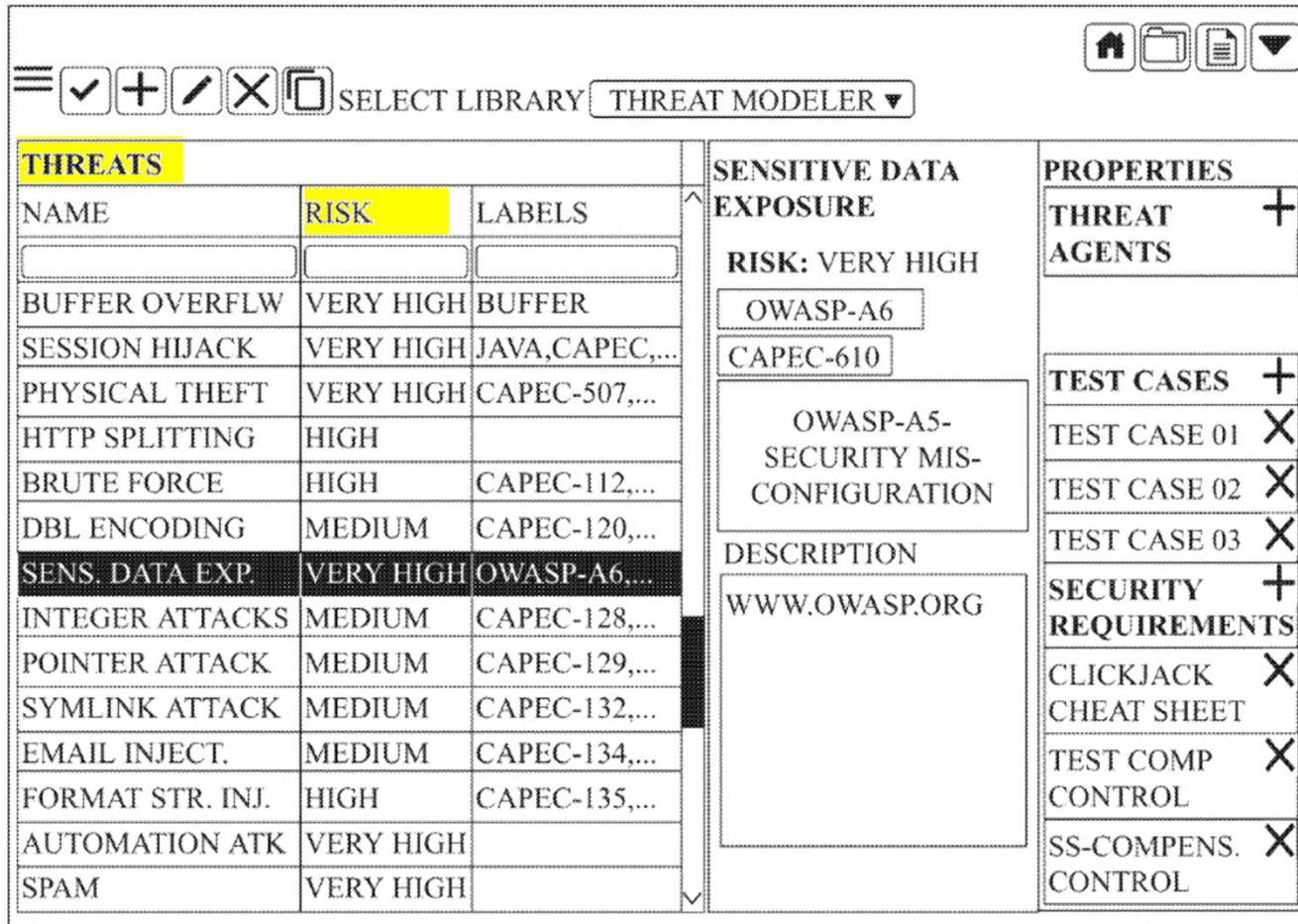
“Mapping File”

“Mapping File” means:

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

EX-2009, ¶¶97, 99; EX-1002, 506.

Risk vs. Threat



THREATS		
NAME	RISK	LABELS
BUFFER OVERFLW	VERY HIGH	BUFFER
SESSION HIJACK	VERY HIGH	JAVA, CAPEC, ...
PHYSICAL THEFT	VERY HIGH	CAPEC-507, ...
HTTP SPLITTING	HIGH	
BRUTE FORCE	HIGH	CAPEC-112, ...
DBL ENCODING	MEDIUM	CAPEC-120, ...
SENS. DATA EXP.	VERY HIGH	OWASP-A6, ...
INTEGER ATTACKS	MEDIUM	CAPEC-128, ...
POINTER ATTACK	MEDIUM	CAPEC-129, ...
SYMLINK ATTACK	MEDIUM	CAPEC-132, ...
EMAIL INJECT.	MEDIUM	CAPEC-134, ...
FORMAT STR. INJ.	HIGH	CAPEC-135, ...
AUTOMATION ATK	VERY HIGH	
SPAM	VERY HIGH	

SENSITIVE DATA EXPOSURE

RISK: VERY HIGH

OWASP-A6

CAPEC-610

OWASP-A5- SECURITY MIS- CONFIGURATION

DESCRIPTION

WWW.OWASP.ORG

PROPERTIES

THREAT AGENTS

TEST CASES

TEST CASE 01

TEST CASE 02

TEST CASE 03

SECURITY REQUIREMENTS

CLICKJACK CHEAT SHEET

TEST COMP CONTROL

SS-COMPENS. CONTROL

FIG. 8

800

The '366 Patent Specification (EX-1001, Fig. 8)

Demonstrative Exhibit - Not Evidence

Risk vs. Threat

7 Q. Okay.

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

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
22 one, but I certainly have a pretty good idea
23 of what it could be, so I've narrowed down
24 my possibilities.

Mr. Hurlbut Testimony (EX-2002, 61:7-24)

Risk vs. Threat

But this was never in dispute—IriusRisk’s Petition acknowledges *threats* *and risks are different* and instead argues that a POSITA would understand that Keenan discloses threats as well as risks (Petition, 21-24 (“A POSITA would understand that Keenan’s ‘risk’ includes threats because measuring risk includes a determination of threats”), 26-28 (same))—a fact that the POR hardly addresses.

No *Prima Facie* Case of Anticipation

The petition “guide[s] the life of the litigation.”

SAS Institute Inc. v. Iancu, 138 S. Ct. 1348, 1356 (2018).

No *Prima Facie* Case of Anticipation

“[T]he statute tells us that the petitioner's contentions, not the Director's discretion, define the scope of the litigation all the way from institution through to conclusion.”

SAS Institute Inc. v. Iancu, 138 S. Ct. 1348, 1356 (2018).

No *Prima Facie* Case of Anticipation

“the petition identifies, in writing and with particularity, each claim challenged, the grounds on which the challenge to each claim is based, and the evidence that supports the grounds for the challenge to each claim, ...”

35 U.S.C. §312(a)(3) (emphasis added).

No *Prima Facie* Case of Anticipation

“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.”

Consolidated Trial Practice Guide, Nov. 2019 (“CTPG”), 73.

No *Prima Facie* Case of Anticipation

The current version of the CTPG states that it was modified to include “[r]evisions to reconcile updates and to reflect the Board’s current practices relate to institution of trial after *SAS Institute Inc. v. Iancu*, 138 S. Ct. 1348 (2018);”

Consolidated Trial Practice Guide, Nov. 2019 (“CTPG”), 1.

No Inherency Argument

The Petition stated that “Keenan *discloses* threats within its risk analysis.”

Petition, 28 (emphasis added).

No Inherency Argument

“Petitioner argues that, although Keenan may not use the identical terminology as the ‘366 patent, Keenan nevertheless **explicitly** discloses limitation 1[b] *to the skilled artisan.*”

Institution Decision, 16 (citing Petition, 28) (some emphasis added).

Dependent Claims 2-3, 9-10, and 17-18

Claim 2:

“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:

“wherein the one or more mapping files comprise one or more tables ***stored*** within the one or more databases.”

EX-1001, 43:62-67 (emphasis added).

Dependent Claim 5

Claim 1:

“*reading a data file* generated by the third party software application, *the data file comprising a subset of the third party diagram components, ...*”

Claim 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.”

EX-1001, 43:40-43, 44:4-13 (emphasis added).

Dependent Claims 6 and 14

Claim 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.”

Claim 14:

“The system of claim 8, wherein, 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, 44:13-17, 45:15-19 (emphasis added).

Grounds 2-5: Zheng

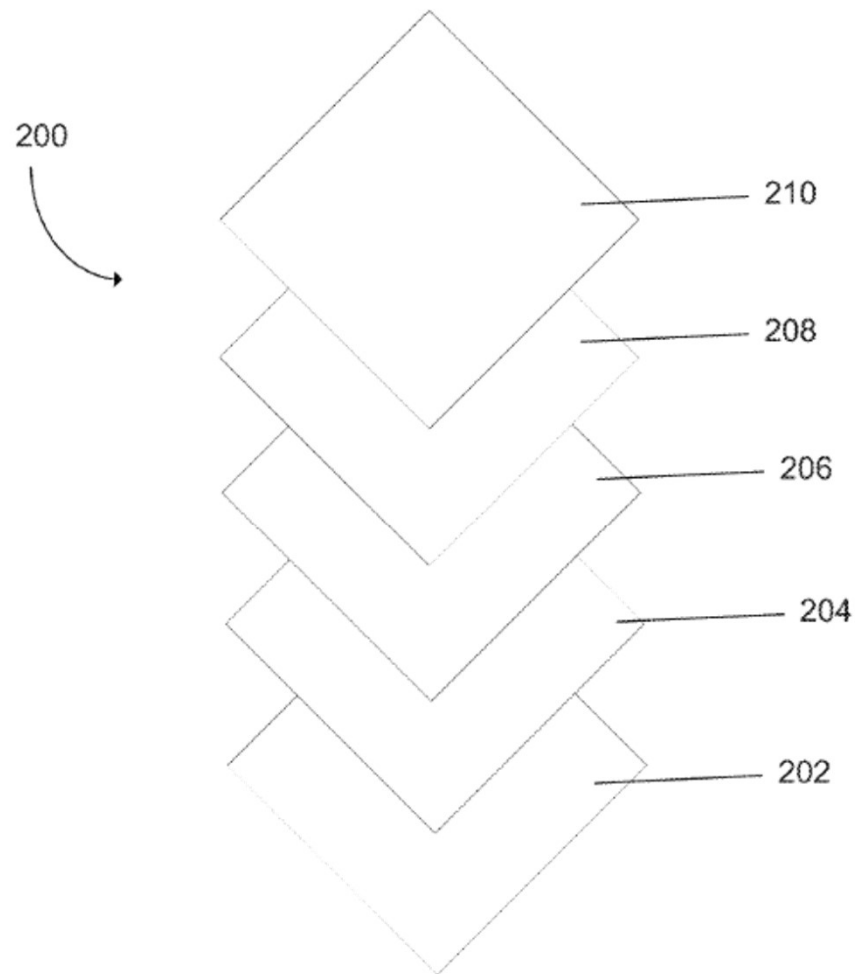


FIG. 2

EX-1005, Fig. 2.

Grounds 2-5: Zheng

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.

Grounds 2-5: Motivation to Combine Zheng and Baker

“It [*i.e.*, the motivation to combine evidence] also fails to explain why a person of ordinary skill in the art would have combined elements from specific references *in the way the claimed invention does.*”

ActiveVideo Networks, Inc. v. Verizon Comm’s, Inc., 694 F.3d 1312, 1328 (Fed. Cir. 2012) (emphasis in original).

Grounds 2-5: Motivation to Combine Zheng and Baker

“[I]t can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements *in the way the claimed new invention does* ... because inventions in most, if not all, instances rely upon building blocks long since uncovered, and claimed discoveries almost of necessity will be combinations of what, in some sense, is already known.”

KSR Int’l Co. v. Teleflex Inc., 550 U.S. 398, 419-20 (2007)
(emphasis added).

Grounds 2-5: Motivation to Combine Zheng and Baker

“Rather, ‘generic’ or ‘conclusory’ analysis is insufficient when it bears ‘no relation to any specific combination of prior art elements . . . from specific references’ and [does]n’t explain why a skilled artisan would have combined them ‘*in the way the claimed invention does.*’”

Intel Corp. v. Qualcomm Inc., 21 Fed. 4th 784, 797 (Fed. Cir. 2021) (emphasis in original) (quoting *ActiveVideo Networks, Inc. v. Verizon Commc’ns, Inc.*, 694 F.3d 1312, 1328 (Fed. Cir. 2012)).

End