

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE INC.,
Patent Owner.

IPR2023-00821
Patent 10,699,008 B2

Record of Oral Hearing
Held: August 14, 2024

Before KEVIN F. TURNER, JOHN D. HAMANN, and
STEPHEN E. BELISLE, *Administrative Patent Judges*.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

BRENT YAMASHITA, ESQ.
BLAKE JACKSON, ESQ.
MATTHEW MIDDLETON, ESQ.
DLA Piper LLP (US)
3203 Hanover Street Suite 100
Palo Alto, California 94304-1123

ON BEHALF OF THE PATENT OWNER:

DONALD JACKSON, ESQ.
MARC KAUFMAN, ESQ.
Rimon P.C.
8300 Greensboro Dr., Suite 500
McLean, Virginia 22102

The above-entitled matter came on for hearing on Wednesday, August 14, 2024, commencing at 1:30 p.m. (Eastern time), by video.

P R O C E E D I N G S

- - - - -

JUDGE BELISLE: Good afternoon and welcome to the Patent Trial and Appeal Board. I am Judge Belisle and I am joined today remotely by Judges Turner and Hamann. This is the oral hearing in IPR2023-00821 involving U.S. Patent Number 10,699,008 B2. Petitioner is IriusRisk, Inc. Patent Owner is ThreatModeler Software, Inc. The court reporter will prepare the transcript for this hearing.

Counsel, please introduce yourselves beginning with counsel for Petitioner.

MR. YAMASHITA: Good afternoon, Your Honor. Brent Yamashita from DLA Piper for the Petitioners. Also with me are Blake Jackson and Matt Middleton from DLA Piper, as well as Stephen de Vries, who is the CEO and founder of the Petitioner, IriusRisk.

JUDGE BELISLE: Thank you.

Patent Owner? You're muted.

MR. JACKSON: Can you hear me now?

JUDGE BELISLE: Yes.

MR. JACKSON: All right, great, thank you. For Patent Owner, Your Honor, this is Don Jackson and I'm also here with the client representative Nikunj Nagalia.

JUDGE BELISLE: Thank you. We are conducting this hearing by video today, as you know, and we'll begin with some general guidance. First, if you encounter technical difficulties during the hearing please let us know and contact our hearing team members who provided you with the connection information if you completely disconnect.

1 Second, for the benefit of the panel and the court reporter, please
2 speak clearly into your microphone and identify yourself each time you
3 speak. Please do not speak when others are speaking and mute yourself
4 when you are not speaking.

5 Third, we have the entire record, including the parties' demonstratives.
6 We would remind counsel that demonstratives are not evidence and are not -
7 - well, and are used only as visual aids. Any arguments and evidence that
8 are not in the record will not be considered by the panel in rendering the
9 final decision.

10 When referring to demonstratives, papers, or exhibits please do so
11 clearly and explicitly by slide or page number. Please pause a few seconds
12 after identifying the page you want us to go to provide us time to find it.
13 This is particularly important if you direct us to a paper that is not part of the
14 demonstratives. Once you identify it please give us a moment to locate it
15 ourselves in the record.

16 Finally, please do not interrupt the other party while that party is
17 presenting its arguments. If you have an objection, please raise it during
18 your argument.

19 Pursuant to our hearing order, each party has 60 minutes total to
20 present its argument.

21 Each party may reserve time solely to rebut the opposing party's
22 arguments. You may not use rebuttal to address an issue for the first time
23 during the hearing. The Petitioner will proceed first because it bears the
24 burden of proving unpatentability.

1 I will keep time and I will try to provide updates on the remaining
2 time during the hearing, but please feel free to ask about your remaining
3 time if you have any questions about that.

4 Petitioner, how much time, if any, do you wish to reserve for rebuttal?

5 MR. YAMASHITA: I'd like to reserve 15 minutes, Your Honor.

6 JUDGE BELISLE: Okay. You may begin when ready.

7 MR. YAMASHITA: Okay. Thank you, Your Honor. I will share my
8 screen which should show our demonstrative.

9 JUDGE BELISLE: Yes, I see it.

10 MR. YAMASHITA: Okay, wonderful. The demonstratives for
11 Petitioner are Exhibit 1017, and for the court reporter's reference this is
12 Brent Yamashita for Petitioner speaking.

13 Okay. So this is the '008 patent. First, on slide 2, this is just an
14 overview of what I'll be covering today. Of course, if the Court has
15 questions or other topics you wish me to address just take it out of order and
16 I'll address your concerns first.

17 But summary of the patent, claim construction is not really dispositive
18 in this matter so I won't spend much time at all on that, and then I'll go to the
19 grounds. Ground 1 is an interpretation of two of the claims. Ground 2
20 builds on Ground 1 and adds in the Zheng and Keenan references, Zheng for
21 this concept of the threat path (phonetic sp.) and Keenan for the concept of
22 toggling of features on and off on the screen.

23 Between Grounds 1 and 2 that covers all of the claims, Claims 1
24 through 20. Under Grounds 3, 4 and 5 are more like a belt and suspenders
25 approach. We think Grounds 1 and 2 cover everything and leads to
26 invalidity so that if I'm not able to convince the Board of something and you

1 disagree with me, then Ground 3 and 4 and 5 provide additional reasons why
2 the claims are invalid.

3 Specifically, Yu in Ground 3 supplies additional disclosure of
4 computation controls and the visualization of the controls on the screen.

5 Ground 4 and Reith provide additional disclosure of this notion of
6 nesting one threat model in another, and Ground 5 relies on the knowledge
7 of a POSITA who is well-aware of toggling feature that is the independent
8 claim.

9 So with that, I will proceed to just summarize the patent. Your
10 Honors, you heard the hearing involving the same parties for the '366 patent.
11 There are many similarities conceptually between the two patents, the '008 at
12 issue here and the '366 from last time.

13 There are three main concepts, and I'm on slide 4 now of the
14 presentation, three main concepts that are relevant to today's hearing. First,
15 the concept of the threat model we covered that last time as well.

16 The second and third concepts are different from last time. Number
17 two is this notion of compensating controls. And the third one is the idea of
18 nesting one threat model inside of another. So let me spend a little bit of
19 time on each of these.

20 So threat model we already know this from last time, but it's basically
21 a way to conceptualize the real world in terms of threat and sources for those
22 threats and components that are associated with this. So the patent gives a
23 nice example of a component in your computer, maybe a Bluetooth port, and
24 a threat that could be related to that component is the fiber hack known as
25 bluejacking where someone tries to commandeer that port.

1 So the component is the Bluetooth port. The threat is bluejacking that
2 could affect that port, and these combine to make a threat model. So a threat
3 model is simply this collection of component and threat and the relationship
4 among those things. And, you know, traditionally this is often just done on
5 a whiteboard. It's a way for people to analyze through real world and to just
6 brainstorm about things that could go wrong, things that could lead to
7 problems. And while (unintelligible) compensating controls. It's just a
8 (unintelligible) to mitigate these threats.

9 So on slide 6, compensating controls, the patent plus compensating
10 controls and these are just, as I mentioned, things they can do to mitigate
11 against the threat. So the '008 patent (unintelligible) is just an example of
12 the compensating controls. So in the private security context maybe you add
13 a firewall. A firewall can provide some network security and from that
14 network threat. And that's all it is. It's the way to just, you know, hedge
15 against a threat or mitigate the threat.

16 Then we get to the last concept relevant to today, which is that the
17 '008 patent talks about integrating one threat model in another. And they
18 give this nice example of say you're modeling a computer system, you might
19 have the model for Windows 7, your operating system, and associated
20 threats that might arise from that operating system.

21 And then you also have a model for a laptop and various threats that
22 could arise involving that laptop. And this part of the patent talks about
23 simply grabbing one of those threat models and putting it into the other.
24 Let's go to slide 8 now, such that when you do that -- so the finished hold
25 (phonetic sp.) has both threat models in it. So the threats that were
26 associated with the laptop and the threats that were associated with Windows

1 basically merge into one. It's the way to just basically shorthand to threat
2 modeling experience and just say, like, instead of lifting all the threats, you
3 know, every time I can just simply grab an existing threat model, stick it into
4 my new threat model and all of those threats will become integrated into one
5 model (phonetic sp.)

6 JUDGE BELISLE: Counsel, this is Judge Belisle. May we go back
7 one slide from where you were just a moment ago, one more slide?

8 MR. YAMASHITA: Sure.

9 JUDGE BELISLE: So on the text on the right in talking about the
10 Windows 7 threat model, it says, "When a user later adds this element."
11 What is the timing that -- how do you understand this language here in
12 connection with the timing of when this is added? Is it already there and you
13 just reveal it or is it literally added in at a later time?

14 MR. YAMASHITA: So in this particular paragraph when it says
15 "later" it is talking about, you know, you can set up your laptop model and
16 then at some later time you use it by simply grabbing it and dragging it onto
17 the screen, which is a simple whiteboard. I think this notion of temporal
18 relationship does arise in the claim and, you know, I'll also address them
19 when we get to the claims.

20 But here when it says later here it's simply just talking about the
21 sequence of the operations that a user would go through as he or she is
22 dragging things on the screen and building their threat model.

23 JUDGE BELISLE: So in that -- what's being revealed on, I don't see
24 the slide -- oh, slide 7 is that there was a Windows laptop threat model that
25 existed and then a user identified perhaps a shorthand or a, you know, an
26 icon-type component that would represent a Windows 7 threat model and

1 added that in to then make or redefine this original threat model? Is that
2 what's going on here?

3 MR. YAMASHITA: Yes. So, yes. The answer is yes. This talks
4 about these are stepped up. There's a Windows 7 print model. There is the
5 laptop that model. The user adds Windows 7 to the laptop and then later the
6 user uses that laptop in some larger threat model and in doing so the laptop
7 has within it the Windows 7 threat model. That's just something described
8 here in this application.

9 JUDGE BELISLE: Okay. And I guess the idea here is that you don't
10 want to reinvent the wheel every time for all the various threats associated
11 with Windows 7 so you can, sort of, identify those and then create a package
12 and then you just can bring that package in as a set of threats as opposed to
13 having to each time go through and identify those?

14 MR. YAMASHITA: That's correct, Your Honor.

15 JUDGE BELISLE: Okay. All right. I understand, thank you.

16 MR. YAMASHITA: Okay. All right, next slide 9, as I mentioned the
17 parties do have a couple of disputes on claim construction, but in our view
18 the patent is invalid under either construction offered so I won't, I won't
19 dwell on this other than to just note that there's a dispute as to certain -- it
20 really just adds to the first phrase. It's redefining the parties have a dispute,
21 but again, I don't think it is dispositive of the invalidity issue.

22 So let me now go to Ground 1 and Jones. Jones, in our view on
23 Claims 1 and 3 and have everything from those claims in it. Now I'm on
24 slide 14, which is Claim 1, and I'll just note that most of Claim 1 is not
25 disputed by Patent Owner. In other words, you know, we made our showing
26 that Jones has each of these things and Patent Owner is only disputing two

1 of those things. So I'm going to spend my time addressing those. You
2 know, and for the others I just will rest on our brief. And, again, Patent
3 Owner doesn't see those other limitations.

4 So on slide 19 we get to the first disputed issue, and on the left side
5 highlighted in orange is the relevant claim language. But this claim
6 language is talking about you create a visual interface and you depict a threat
7 model component, as well as visual representations of one or more
8 compensating controls.

9 So here on the right we have Jones, and Jones in Figure 9 depicts
10 visually a threat model. It tells us, Jones tells us that there are components
11 shown such as the big rectangle 804 are servers. To the left is the little
12 laptop icons. Those are also components, threat model components, and
13 Jones tells us that threats are depicted with little circles labeled with 904. So
14 in Figure 9, you can see a number of components and a number of threats in
15 the threat model depicted in Figure 9.

16 Figure 9 also shows this window, popup window 814, and Jones
17 explains that for any of the items in the tree you can click on it and it may
18 create this window, popup window 814, that gives you more information
19 about whatever it is you clicked on.

20 And in the particular example shown in Figure 9, Jones tells us that
21 this window has popped up based on the selection of one of the threats,
22 which is the threat called buffer overflow. So we see in the box 814 the
23 threat buffer overflow.

24 Jones also tells us that this box that I've highlighted, current controls,
25 are controls that are in place regarding that threat. And that is this box 814,
26 which shows entries for current controls. And that is the visual

1 representation of one or more of these compensating controls, and it's shown
2 in this relational diagram of Figure 9 of Jones.

3 JUDGE BELISLE: So that's -- so this is Judge Belisle again. What
4 are you calling the relation or the relational diagram in Figure 9? What part
5 of that is the relational diagram in Figure 9?

6 MR. YAMASHITA: It's the bulk of Figure 9 so it's the grid that you
7 see. It's all the icons, so 804, 904 and including the window, including 814,
8 which is not just something that randomly appeared on the screen. It's
9 related to the threat 904 for buffer overflow in this example. So it is still
10 related to the threat from which it was selected and so all of those things are
11 part of a relational diagram. And there is a relationship between the
12 compensating controls shown in 814 and the server icon was used to cause
13 that popup to occur.

14 JUDGE BELISLE: Does Figure 9 of Jones, does it show where that
15 compensating control is relative to the other components in this relation with
16 a relational diagram? Does it show where the compensating control is in
17 relation to the other components?

18 Mr. Yamashita: It shows that related to the threat of buffer overflow
19 in this example. It doesn't -- if you're asking if it has, like, a visual depiction
20 beyond that it does not, but there is a relationship between the current
21 controls that I've highlighted as well and the threat from which -- that it
22 relates to. So there is the relationship there in the same visual so in our view
23 it's practically the same depiction (phonetic sp.).

24 Okay. I'll move on to the second disputed issue in Ground 1. And
25 this is basically the ending of the claim. So this talks about configuring your
26 interface in response to user input, and this is where we get to the nesting.

1 You add a component proof to the first threat model thereby redefining that
2 threat model to include within a second threat model with the stated
3 components you just added. And those components that we added have a
4 predefined -- are predefined in a related group.

5 So let me show you what Jones says on these. All right. So first, on
6 slide 20, we have an excerpt from Jones, and Jones for the record is Exhibit
7 1004. This is from column 5, lines 4 through 19. Jones tells us expressly
8 that the threat model system can include nested components, nested
9 components.

10 And on the next slide, slide 21, Jones give us more detail on what this
11 means. So this is coming from Jones column 6, lines 12 through 34.

12 JUDGE BELISLE: Counsel, this is Judge Belisle again. I'm probably
13 going to have a lot of questions on this point because I think this is a
14 significant point of contention between the parties as to what it means, the
15 "add this component group." And Jones speaks in terms of nesting, but the
16 nested components in Jones, is it correct that those components already exist
17 at a nested state? They're already there but they're just in, sort of, layers that
18 you have to reveal to see all those components. Is that correct?

19 MR. YAMASHITA: Yes, Your Honor. No, Your Honor, that's not
20 how I read Jones. And that is how Patent Owner has described Jones, but if
21 we look at Jones carefully I don't think that's what's happening.

22 JUDGE BELISLE: Okay, let's do that.

23 MR. YAMASHITA: Oh, okay, let me explain, and it's actually we
24 start with this paragraph right here. So let me just step back and say that,
25 you know, Jones has this concept of level n and level n+1 threat model and
26 this is where the nesting comes into play. And Jones explains that the

1 operator can choose the level to be depicted and a level n will have one level
2 of detail and a level $n+1$ will have additional detail.

3 And I think Your Honor's question is, well, was that additional detail
4 already part of the level n diagram and this is simply just displaying it now?
5 In this portion of Jones that I have on the screen that's not what's going on.
6 And let me get a little more specific.

7 So starting with the yellow highlighted portion, this is saying that --
8 well, let me back up actually. At the very beginning of this paragraph it says
9 it may be desirable to basically show more details, and this is what is
10 prompting us to go from level n to level $n+1$.

11 Then it says the decomposer is configured to basically do the work to
12 figure out what the wrong thing -- the components that contains nested
13 (unintelligible). So it's not -- what's being described here it's not simply, sort
14 of, doing a visual review of something that's already there. It's just saying
15 the decomposer is configured to decompose the component in the level n
16 diagram to figure out what should be there in the nesting space.

17 And then it says, "The decomposer provides feedback of its
18 decomposition to the DFD creator," and in a moment I'll put up Figure 1 of
19 Jones which, kind of, puts those two pieces together.

20 And that DFD creator does more work. It modifies the original threat
21 model to include the nested components that it was polled about by the
22 decomposer and then it creates this new threat model, the level $n+1$ threat
23 model.

24 And then on top of that, then the threat indicator 108 is just another,
25 you know, functional block, figures out what threats are associated with

1 those nested components and it adds an appropriate secondary node
2 representing those threats.

3 And then Jones in the same paragraph tells us instead of modifying
4 the existing threat model, in some cases we can just simply create a new one
5 that has all of this in it. So my point in going through this is simply that
6 Jones tells us that when you want to go from level n to level $n+1$, the
7 decomposer and the DFD creator 106 each have to do a certain amount of
8 work. And then once those are done, the threat indicator 108 has to apply
9 the threats that go along with those nested components.

10 So what Jones is telling us is that this information is not already
11 present in your level and threat model. This information has to be added to
12 the level n threat model (unintelligible) to create this level $n+1$ threat model.

13 So the components of --

14 JUDGE BELISLE: Counsel, this is Judge Belisle. So let me just take
15 a step back. Earlier we were talking with respect to the patent that's
16 challenged. The introduction of those (inaudible) threats into a laptop says
17 Jones disclosed that technique of taking, sort of, an off-the-shelf icon
18 package of a Windows 7 threat and adding that into an existing threat model.

19 MR. YAMASHITA: It's done right here in this paragraph, Your
20 Honor. It uses different language, but when it says you take a component
21 and then decompose the figures out and nested components that are part of
22 that and then we add the threats that's associated with that. That's the
23 equivalent of with that -- no. Let's figure out what Windows 7 is all about in
24 the '008 patent.

25 JUDGE BELISLE: But were not all those components already there?
26 They're all part of the system. They're already part of the platform. Isn't

1 Jones simply asking you what level you'd like me to show you a threat
2 diagram for?

3 MR. YAMASHITA: So this information is known by the system of
4 Jones, and I think I will, I guess, exit this presentation and go to Jones for a
5 moment because I do think it would be helpful to see Jones' Figure 1.
6 (unintelligible). Okay.

7 So hopefully you can see Jones Figure 1.

8 JUDGE BELISLE: Yes.

9 MR. YAMASHITA: So, okay. So some of the words that I was
10 talking about earlier, the DFD creator, the threat indicator, the decomposer,
11 these are the things that are doing that work that gets us from level n to $n+1$.
12 Now, so the system of Jones that is running all of this has knowledge of lots
13 of components and threats and that's the components and threats, but the
14 important point is that Jones tells us that the threat model you start off with,
15 the level n threat model, doesn't have that information. And that's really the
16 key.

17 That threat model which is, you know, in existence, threat that
18 someone has created of threats and components, that threat model doesn't
19 have the nested component information in it already. And the reason we
20 know that is because Jones tells us when we want to make the switch if the
21 creator, the threat indicator and the decomposer in Figure 1 each have to do
22 stuff to make that happen.

23 So I guess I will close out this spot and this is not -- let me go back to
24 my slides. One second. I figured that out.

25 So going back to slide 21, which is what we were looking at earlier,
26 the components we've said is being added in Jones are those nested

1 components, such as decomposer, is figuring out and adding. So the first
2 threat model is the existing level n threat model that exists at the beginning
3 of this paragraph.

4 That threat model is being modified to include some new stuff, the
5 new nested components such as DFD is figuring out, as well as to include
6 the threat such as threat indicator 108 is adding, and the resulting threat
7 model will then be level n+1 threat model that is modified, a modified
8 version of the original threat model.

9 The second threat model is, in fact, the nested component and the
10 threats that are associated with those. And I'll consider that Jones does not
11 call out to us that, hey, by the way, that stuff that I'm adding is a separate
12 threat model. But if we consider, you know, what is a threat model, a threat
13 model is simply components and threats associated with those components.
14 And that's clearly what's been added here. So nested components are being
15 added and threats that are associated with those components are being added
16 and that is -- those are the components that are in the claim language.

17 There's a second threat model associated with that component use and
18 that would be added to the first threat model. And the threat model has been
19 modified to include those things. And we know those components have a
20 predefined interrelationship because they are, they are together. They are
21 nested components of the larger components that, you know, that they have
22 a relationship with.

23 JUDGE BELISLE: Counsel, Judge Belisle again. In your argument
24 are you essentially arguing that the claim language of "add a component
25 group to the first threat model," that's not talking about just simply adding
26 components into your system? That all that requires is that you're adding

1 those component groups to the threat model, i.e., threat model components
2 are being added to the threat model.

3 And it doesn't matter that you might -- whether or not you actually are
4 adding things into the system as a whole as far as adding components, it's
5 about whether you're adding the threat model components into the threat
6 model. Now, if that question made any sense then I'd like to hear your
7 response to it.

8 MR. YAMASHITA: Yeah. And as I understand it, I think you're
9 asking can this be satisfied by adding any component? And is that Your
10 Honor's question?

11 JUDGE BELISLE: So my question is you have a, you have a system
12 and the system has components but you also have a threat model modeling
13 those components. And so, for example, in Jones, Jones already has a
14 system with components. And in the patent when we were talking about
15 Windows 7 it appears that Windows 7 was actually being added as a
16 component to a system, but the claim language refers to adding the threat
17 model components to the threat model.

18 So even here if you were to add components to the other like, i.e., add
19 Windows 7 into your system, the claim isn't talking about whether or not
20 you're adding it into the system itself -- adding the threat model component
21 into the threat model, which I understand you to argue that that's what Jones
22 is doing. Jones has the threat model. It goes to another tier, identifies
23 additional components, threat model components, and then adds those to the
24 threat model.

25 So my question is are we drawing a distinction between adding threat
26 model components to a threat model versus whether you're adding

1 components to the system itself, just adding components versus adding the
2 threat model components?

3 MR. YAMASHITA: I see. Yeah, I think this portion of the claim is
4 talking about adding a threat model component to a threat model, and that's
5 also what's being discussed in this portion of Jones. It's not -- the
6 components you're adding are the nested components and you're adding
7 those to the existing threat model for the level n DFD. And DFD just stands
8 for data flow diagrams in Jones.

9 So those are components. Then the threat indicator is adding threats
10 to the DFD that are associated with those nested components. Once you do
11 that, together those represent the second threat line because the threat model
12 contains components and threats. It's from, you know, the relationship
13 between them. And that's what the decomposer and the threat indicator are
14 adding when they are making sense of what the nested components are.

15 JUDGE BELISLE: Just for your timing purposes, counsel, we're at
16 roughly 31 minutes so I'm going to lay off on questions on adding to let you
17 move on (simultaneous speaking)

18 MR. YAMASHITA: All right. Thank you, Your Honor. All right.
19 So next I want to move to Claim 3. In our view, Jones anticipates Claim 1
20 and Claim 3. Claim 2 depends on Claim 1.

21 So Claim 3 is long but it it's actually a very simple concept. So it's
22 saying, okay, so we've already done Claim 1. (Unintelligible) in Claim 1,
23 you also have to have the ability to receive user input to store one or more
24 additional threat model components, one or more additional threats, and one
25 or more additional compensating controls and put those in the database.

1 So, again, threat model components, threats, compensating controls,
2 these have to be received from the, from the user and then store in a
3 database.

4 And I'm going to flip again back to Jones to show you, I guess,
5 additional parts of Jones that are not on our slides. But so we're looking at
6 Jones at Exhibit 1004 and let me make sure I'm sharing. I think I'm sharing
7 (unintelligible).

8 Okay. So now I'm sharing Jones and I just want to show you portions
9 that talk about components, threats and controls since there's nice symmetry
10 (unintelligible) I'll talk about each of them. And for each of those things it
11 talks about the information for those things coming from the operator and
12 then storing it in the database, which is what Claim 3 requires.

13 So first in Jones column 7, around line 49 through 52, it's talking
14 about components, threat model components and it says, "In some examples
15 the components of data flows to the information system may be identified to
16 collected information from an operator," so the security architecture for
17 example. So that's receiving the information about a component.

18 And then shortly after that in column 8 beginning around lines 10
19 through 22, Jones explicitly tells us that the data regarding components is
20 stored and it can be stored in any number of different ways. And then if you
21 look at the very ending of the highlight it says, for example, file storage
22 database storage, cloud storage.

23 So this portion of Jones is saying I can get confirming information
24 from the user and operator and I can store information in the database. This
25 is components. There's similar language for threats and for compensating
26 controls. So for threats you have very similar language in paragraph -- I'm

1 sorry, column 12 around lines 22 through 25. This is some examples of
2 cybersecurity threats, (unintelligible) threats may be identified to the
3 collection of information from the operator.

4 And then further down around lines 49 through 55, it says that you
5 can store information in any number of different ways, including database
6 for later retrieval.

7 And then finally, there's similar language in column 15 regarding
8 compensating controls. Here Jones is talking about mitigation measures
9 which are one type of compensating control. And again, column 15, lines 10
10 through 13 it's saying that suggested mitigation of threats can be identified
11 through the collection of information from the operator.

12 And then in the next paragraph it again says that to store this
13 information in any number of different ways, including in a database.

14 So I apologize for the CD (phonetic sp.) walk through Jones, but I'll
15 go back to my slide now. You know, it's just put it all together what we see
16 is that Claim 3 requires, you know, in addition to whatever happened in
17 Claim 1 you also need the ability in response to the CD user input to store
18 threat model components, threats, and compensating controls in the one or
19 more databases.

20 And, hopefully, I just showed you those portions of Jones talk about
21 that for each of those things, about receiving input from an operator, that's
22 the user input, and storing it in the database. And Jones said that for threat
23 model components threats and controls as required by Claim 3.

24 So next, and I know I'm running short on time and I realize I won't
25 finish but I'll just get as far as I can, so Ground 2 builds on Jones and covers
26 basically the rest of the claims. And then I'll focus first on Zheng, so some

1 of the claims talked about visually displaying the (unintelligible). And I'm
2 sorry, I'm on slide 24 of Exhibit 1017 in our presentation. And so this slide
3 shows the language of Claim 2. Claim 2 talks about visually displaying
4 attack paths of all threats associated with the threat model components. And
5 the '008 patent talks about doing this by drawing a line, a graphical line from
6 the threat to the component.

7 And so this concept, which appears in many of the claims, need to
8 rely on Zheng. Zheng is also in the field of threat modeling and Zheng in a
9 couple of places talked about visually displaying attack paths between
10 threats and components.

11 So we see these are the steps in what I have on the screen, Zheng at
12 Exhibit 1005, column 2, lines 36 through 42. It also appears in Zheng
13 column 5, lines 14 through 18 where it again talks about visually displaying
14 a vector between a threat and a component. This is exactly what Claim 2 is
15 talking about when it says visually displaying attack paths of threats
16 involving components.

17 JUDGE BELISLE: Counsel, this is Judge Belisle. If it may help with
18 your time management, a concern of mine is you claim, for example -- well,
19 actually I'm looking at Claim 4 right now but I believe this also is Dependent
20 Claim 2. All right.

21 And the claim recites, this is Claim 4, in response to receiving a user
22 selection of one, of one of the diagram components, the system then says
23 that it will visually display attack path of all threats associated with the
24 diagrammed threat model components that comprise that selective threat
25 model component.

1 So the claim wants you to select one and then have the system show
2 you all the threats associated or that evolve around that one component. So
3 that's what I'd like to hear from you as to how this combination teaches that.

4 MR. YAMASHITA: Sure. So, let me switch to Zheng and address
5 Your Honor's point. So if we go to Zheng, I'm going to look at column 11,
6 column 11 around lines 41 through 48, here Zheng, to address Your Honor's
7 point, Zheng says that when you have this visualization up on the screen the
8 user can interact with it in any number of different ways, essentially toggling
9 enabling or disabling various things.

10 It says, "For example, a particular type of threat in the threat modeling
11 (unintelligible) can be toggled on or off to provide more focused
12 visualization. So taken together with the other piece of Zheng that I
13 mentioned earlier, Zheng is saying you can visually display attack path.
14 And then this portion of Zheng is saying the user can select or deselect
15 anything they want to be able to see the things he or she wants to on the
16 screen because as we know, sometimes the screens get complicated and we
17 want to just focus on something and it help to get rid of stuff on the screen if
18 you want to just focus on something that's of interest.

19 So these two pieces together tell us that you could look at every single
20 attack path or only some of them. And a person of ordinary skill in the art,
21 from Mr. Hurlburt, our expert, taking this all together would say that, okay, I
22 understand that, you know, Claim 2 basically is taught by Zheng when you
23 put these two pieces together.

24 JUDGE BELISLE: So is it -- counsel, this is Judge Belisle again. Is
25 it fair to say that while Zheng may not explicitly disclose or, you know, or
26 recite verbatim selecting one component and then seeing all the threats, that

1 the cited material that you've recited here in your presentation provided
2 enough information for the skilled artisan such that it would have taught or
3 at least suggested being able to select one and seeing all the threats
4 associated with it?

5 MR. YAMASHITA: That's correct, Your Honor. So it's a more
6 succinct way of saying it then whatever I said, so yes. That's exactly our
7 view of Zheng.

8 JUDGE BELISLE: Continue, please.

9 MR. YAMASHITA: Okay. Let's go back to the slides. I have lost
10 track of my own timers. Your Honor, do you happen to know how much
11 time I have left?

12 JUDGE BELISLE: You're at 43 minutes, counsel.

13 MR. YAMASHITA: Okay.

14 JUDGE BELISLE: As you know, you can use your rebuttal time if
15 you wish.

16 MR. YAMASHITA: Yes. Okay. So I'll just spend a moment talking
17 about Keenan and I will have to rely largely on our brief for that because I
18 do want to save time for rebuttal.

19 But we're relying on Keenan here for very narrow things, which is just
20 this notion of toggling on and something on the screen that, you know, a
21 graphic on the screen. And Keenan, here I'm on slide -- I'm actually not sure
22 what slide I'm on. Slide 25 of our presentation has an excerpt of Keenan,
23 column 12, lines 29 to 35. Keenan teaches this idea of toggling something
24 on the screen to make it appear or disappear.

25 It's not just in Keenan. We just saw a portion of Zheng itself that talks
26 about toggling something so that it visually appears or disappears. Also in

1 our Ground 5 Mr. Hurlbut explains the toggling graphic feature was
2 notoriously well-known in the art. And I would that each of us as users also
3 has done that before in various computer applications.

4 But that's what we're relying on Keenan for. And some of the
5 dependent claims, not all of them, require this notion of toggling either the
6 attack path or toggling the compensating control and just the user toggles
7 and then visually something changes on the screen, something appears or
8 something disappears.

9 And Keenan tells about and when you combine it with Zheng and
10 Zheng's teaching of attack path plus the base system of Jones, and I'll just
11 add that combining Jones and Zheng someone could simply just move two
12 arrows from those threats in Figure 9 of Jones to the components in Jones,
13 that's all that's required to visually show an attack path.

14 And after reading Zheng someone working with the Jones system
15 would say, like, oh, Zheng teaches how to visually show attack paths and
16 that might be useful to our customers. So in the next version of my Jones
17 system I'll just add that feature where I'll show a graphical arrow from threat
18 to component.

19 And then with Keenan, Keenan is just simply adding that you can
20 toggle things on and off. And why would you do this? It's for the ease of
21 the user to understand what he or she is looking at on the screen or if you
22 want to focus on one particular threat or one particular attack path or
23 compensating control, you know, why not turn off all the other stuff so you
24 don't see it when you look at only what's of interest at that time.

25 You know, we've all done something similar in meetings where we
26 want to focus the, you know, the meeting's attention on certain things so that

1 we can all talk about it. This is just saying the same thing but in a threat
2 modeling context, you know,.

3 So I, kind of, in this slide explanation I've, kind of, touched on the
4 motivation to combine, which Patent Owner has also taken issue with, but,
5 you know, what motivates each of these modifications that I've mentioned is
6 simply the realization that in the end threat modeling is used by people to
7 understand -- to abstract and understand these real-world threats and what
8 they can do to minimize those threats.

9 And so the idea of visually showing attack paths or being able to
10 toggle something on and off, one would be motivated to do those features
11 because they're useful to people and people are the ones who are using these
12 threat models. These threat models the whole point of it is to help people
13 understand the threats in the real world.

14 And so with that, I will stop and reserve my time for rebuttal unless
15 Your Honors have any questions.

16 JUDGE BELISLE: It does not look like the panel has any additional
17 questions at this time. That's at 47 minutes so you still basically have your
18 rebuttal time, 13 minutes of rebuttal time. Thank you.

19 Counsel for Patent Owner, how much would you like to reserve for
20 your surrebuttal?

21 MR. JACKSON: Thank you, Your Honor. This is Mr. Jackson. I'd
22 like to reserve 15 minutes.

23 JUDGE BELISLE: Okay, you may begin.

24 MR. JACKSON: Thank you. Let me try to share my screen. I'm not
25 familiar with the Webex interface so hopefully I'll get this correct. Just let
26 me know if you see the --

1 JUDGE BELISLE: We do.

2 MR. JACKSON: Okay, great. So I wanted to start here on Figure 10.
3 This is Figure 10 from the '008 patent, and this goes back to a question that
4 Your Honor Judge Belisle had for Petitioner's counsel when we were
5 talking. He gave the example of the laptop and the Windows 7 component
6 that was, that was added as an example of how the nesting invention of the
7 '008 patent works. And I just wanted to reiterate that.

8 So the -- what I've done is I've highlighted there in the box in Figure
9 10 the Windows 7 component that was added to this laptop. And the way
10 this invention works or envisions this working is over in the toolbox, which
11 is on the left, again just for the record, this is slide number 2 of our
12 presentation.

13 Over on the left you have this toolbox work area where you have
14 individual components that could be added to a threat model or in the
15 context of this particular feature you can predefine a group of components to
16 make up a particular subcomponent, if you will, of a larger system.

17 So as I think was elicited earlier from the description -- discussion,
18 this Windows 7 component can itself have other components within it. For
19 example there's a file system, a PDF client, Skype, et cetera, et cetera that's
20 shown here in Figure 10. And what the user does is if they want -- if they
21 have just a basic laptop, in the case of this particular figure here the laptop
22 would not have an operating system, so the laptop has the, sort of, the
23 hardware interface, if you will. It has the Ethernet port, the Wi-Fi port,
24 USB, HDMI, and Bluetooth.

25 And so the user can go to the toolbox and find -- and say, well, this
26 laptop is a Windows 7 laptop so I want to instead of rebuilding the Windows

1 7 aspect of the laptop from scratch I've done that previously. I can click and
2 drag this Windows 7 group into the laptop and thereby convert my laptop,
3 which is really just basic hardware at that point into a Windows 7 laptop,
4 which itself has its own set of vulnerabilities. And the components
5 associated with those vulnerabilities are shown there in the figure.

6 The advantage is not only just that a user doesn't have to redefine it
7 each time, but the way the patent describes it also is that the user can go to
8 the toolbox area, if you will, and work on the Windows 7 component there
9 and not have to go back to all of the threat models where the Windows 7
10 component was used individually.

11 So in other words, they can update it in one place and have those
12 changes ripple through the other threat models. So that's additional benefit
13 of the invention.

14 Oh, we talked about attack paths. I'm trying to get to the real issues
15 here. I did want to highlight one thing with this, this is on our slide 4
16 relating to claim construction. This is claim construction for the phrase that
17 says, "redefine the first threat model by including in it a second threat model
18 associated with the component group."

19 I think there is a difference, a significant difference which was
20 touched on by Judge Belisle's questions earlier today, which is we seem to
21 differ, at least my read of it is, the parties differ on this last phrase in Patent
22 Owner's construction where we said, "Where the added component group
23 was not a part of the first threat model before being added."

24 And we put that in there. It's really a little bit, I think, redundant of
25 the other part of the claim construction because we do talk about adding and

1 that comes right out of the claim. This component group and the threat
2 model associated with the components that have to be added.

3 And necessarily implied in that, I think, is the fact that it wasn't there
4 previously. So I tend to disagree with Petitioner's counsel a little bit on that
5 there. I think there is a significant difference on claim construction.

6 JUDGE BELISLE: Counsel, this is Judge Belisle. I just want to
7 touch on the same, sort of, line of questioning as Petitioner. Could you go
8 back to your slides to where it shows Figure 10 from the Jones patent?

9 MR. JACKSON: Yes, Your Honor, I'm there.

10 JUDGE BELISLE: Is Figure 10, is that showing us simply an
11 implementation of an interface or of a system or is it showing us the actual
12 threat model?

13 MR. JACKSON: It's showing us both, actually., It's showing us the threat
14 model because the threat model, as Your Honors are aware, conveys
15 information in addition to the system itself, right? So you're -- it's not just
16 the system but you're also looking at what threats are associated with the
17 different pieces of that system.

18 So what Figure 10 is showing is not just the system, such as, for
19 example, a laptop connected to a Wi-Fi access point connected to a
20 SharePoint server or a file server, but it's also showing us vulnerabilities that
21 may be present in that system. So it's actually showing us both.

22 JUDGE BELISLE: So where is an example where both of those are
23 shown in this figure, in Figure 10?

24 MR. JACKSON: So the vulnerability, to take the example that was
25 discussed earlier and was discussed in the '008 patent, the BT port is a
26 reference to the Bluetooth port. That's in the block labeled laptop. So that's

1 a threat model component. And threat model components, I think the parties
2 agreed, in particular in the prior art, are sources of threats.

3 So when I say vulnerability I'm not using claim language, obviously.
4 I'm just, sort of, paraphrasing here. That Bluetooth port represents a
5 vulnerability which is that it can be exploited potentially by someone
6 implementing a blue-jacking attack on that port. Does that make sense,
7 Your Honor?

8 JUDGE BELISLE: Well, not in connection with what is actually
9 shown in this drawing. I mean, I understand that there's threats associated
10 with a Bluetooth port, but what I -- my question is what is Figure 10
11 showing me? And it looks like it's just showing me the components of the
12 system. It seems like we haven't got to the threats yet, you know, like threat
13 vectors or where the threats are coming from or where this blue-jacking is
14 infecting this system.

15 It looks like -- and according to the patent itself it just says Figure 10
16 is an implementation of an interface of the system in Figure 1. So I'm just --
17 I just want to make sure I appreciate what Figure 10 is showing me. Is it
18 showing me bringing together and identifying the components of the system
19 that we will then do a threat model for? Or is it somehow also showing me
20 that this is a threat model somehow?

21 MR. JACKSON: Right. Your Honor, I think you're -- I'm sorry, I
22 missed that in your question earlier. So you're right. So what -- this is only
23 one of the interfaces that can be displayed from the system and you're right.
24 Almost all of these as I'm looking at them are components in one dimension,
25 although I will say that there are other -- so I can see controls also displayed,
26 for example, with firewall.

1 But I think the way the system works is that you can select one of the
2 components and then on another one on the screen look at the particular
3 threats that might be associated with that particular component. So I'm not
4 sure I have the best figure here, but --

5 JUDGE BELISLE: All right. And so before we move off, I guess
6 now I'll come to my question.

7 MR. JACKSON: Sure.

8 JUDGE BELISLE: Here, or at least what's revealed in Figure 10, the
9 adding of Windows 7 into this system, what I'm seeing is the adding of the
10 component of Windows 7 actually to the overall system. It's adding
11 Windows 7 into the system.

12 And I have -- this isn't yet showing me how that then impacts the
13 threat modeling but it's just showing me I'm piecing together my system by
14 being able to pull from this toolbox various items to create my overall
15 system. And then from there we're going to move on and have our threat
16 model. Is that correct?

17 MR. JACKSON: Right, right. And I think that's right, Your Honor,
18 but again, inherent in each of these because it was -- recall that even though
19 it might be in the toolbox, let's just talk about the Windows 7 block in the
20 context of being by itself in the toolbox, it has a threat model for it that's
21 been created.

22 And you can look in, I think, figure -- I was looking in Figure 6 but I
23 think also Figure 8 of the '008 patent shows how in a more tabular format
24 you can select. Well, actually, let me go back. I think Figure 6 is a better
25 figure.

1 So Figure 6 you can look at, you know, it'll list on the left-hand side
2 components. Yeah, let's just pick Wi-Fi port, for example, which is the third
3 component down on the list on the left-hand side, and if you select that
4 component then over on the right-hand side you'll get various pieces of
5 information about that component, one of which is on the very far right-hand
6 side are the threats associated with that component.

7 So those threats are part of that component even when it's over in the
8 toolbox as a predefined group of interrelated threat model components just
9 as a Windows 7 block, not as the laptop. So it isn't like those threats
10 somehow are generated once it's put into the larger laptop in Figure 10.
11 They're already there in the -- just over in the toolbox space. It's been
12 predefined as having its own threat model.

13 JUDGE HAMANN: Counsel, this is Judge Hamann. So even though
14 something is in the toolbox and may have threats associated with it, that
15 doesn't make it part of the first threat model as you claim does it just because
16 it's in the toolbox?

17 MR. JACKSON: That's right. In the context of the claims, Your
18 Honor, I'm sorry for reaching behind myself here, but in the context of the
19 claims to try to analogize the embodiment I'm describing to the claims, the
20 Windows 7 subgroup in the toolbox would correspond to the predefined
21 component group, which is in the very last paragraph of the claim.

22 And it's that predefined component group and its threat model that get
23 added to the first threat model so you're right. Windows 7, that little
24 subgrouping, if you will, is going to be a second threat model. It's going to
25 have a second threat model that gets added to the first threat model. And
26 when it's added to the first threat model that's how in the language of the

1 patent here, that's how it redefines the first threat model because it's bringing
2 in these threats, this threat model associated with the component group,
3 which wasn't part of the threat model to begin with.

4 JUDGE HAMANN: Thank you.

5 MR. JACKSON: So let me try to move on to some of the other parts
6 here of our discussion. So let me go to my slide 8. This is an excerpt from
7 Jones and this is at column 5, lines 10 to 19. And in this passage Jones
8 explains that, "The information system may be describable in terms of a
9 hierarchical breakdown, what it refers to as the hierarchy of its components,
10 at different levels. In this regard, one or more of the information system's
11 components this may include multiple nested components."

12 So what this is saying is that the components of the information
13 system include their nested components. They're already there. It may not
14 be visible but they're already there. These nested components are already
15 part of that same component, that higher level component. And I think that's
16 consistent with the background. I don't have a slide on this.

17 But the background of Jones, this is Jones column 1, lines 19 through
18 24 it looks like, where this is just setting the environment for the description
19 of Jones. And it talks about how "Aviation platforms and infrastructures, for
20 example, are complex system platforms that involve hierarchically
21 networked, embedded systems with varying operational criticality,
22 reliability, and availability requirements and include systems both onboard
23 and offboard aircraft."

24 The point that I draw from this as it relates to our discussion here is
25 that these are complex systems that involve hierarchically networked,
26 embedded systems. Those lower level components of this system are

1 already in this system that's going to be modeled. This isn't something that
2 gets added to the system later.

3 And so what this is -- this goes back now to my slide 8 --

4 JUDGE BELISE: Well, and, Counsel, this is Judge Belisle. So this
5 now we're getting back to my, sort of, I think, a key issue here. You say it's
6 not being added and the distinction here being adding components to your
7 system or adding the threat components to the threat model because in Jones
8 it may be fair to say that the components, as a system the components are
9 there. But the threat model is only showing certain threat model
10 components, and as you dive deeper in, it decomposes a given, say, black
11 box and then provides the threat model for those that includes those
12 additional threat model components.

13 The system itself hasn't grown or shrunk in how it's made-up as a, as a
14 computer system, but the threat model is changing as you go from tier to
15 tier. And so what I'd like to hear is how does the claim not allow what is
16 going on in Jones? The claim is about adding threat model components to a
17 threat model. Unless you want to show me how it's adding components to a
18 system as opposed to threat model components to the threat model?

19 MR. JACKSON: Sure let me --

20 JUDGE BELISLE: (Unintelligible).

21 MR. JACKSON: I'm sorry, go ahead.

22 JUDGE BELISLE: No, go ahead. Go ahead.

23 MR. JACKSON: All right, thank you. Let me try to tackle that and if
24 I don't answer all the parts of that question please, please let me know and I
25 will try to hit them.

1 With respect to the claim language, so -- which I think, obviously, is,
2 sort of, what we need to keep our eye on, the claim says add a component
3 group to the first threat model and thereby redefine the first threat model by
4 including in it a second threat model associated with the component group.
5 So we are talking about the threat model and adding things to the threat
6 model not previously there.

7 And what I'm saying is that in Jones, and there's a -- I'll get to a
8 passage there in Jones which I think helps illustrate this a little bit better, is -
9 - you use the example, Judge Belisle, with the black box. A black box in the
10 system has embedded in it the threats that are visible to the rest of the system
11 at the border, at the boundary of the black box.

12 So you may not know what gave rise to that particular threat, you
13 know, what component within the black box gave rise to that that threat, but
14 those threats are reflected at the boundary of the black box. Otherwise, what
15 is the black box doing in the threat model? I mean, if it doesn't show its -- if
16 it doesn't exhibit its threats at the boundary of the black box how do we
17 know how to define the black box? How do we know how to interface the
18 black box? How do we know how to mitigate threats associated with the
19 black box?

20 So those, you know, whether it's a Bluetooth port or a USB port or
21 some other port, for example, that might give rise to a particular threat, those
22 threats have to be reflected in the boundary of that black box, which would
23 be the level n of Jones.

24 And what Jones says, and let me see if I can find the passage, I know I
25 don't have a slide on this, but Jones says, oh, I'll have to find the cite. I think
26 actually it's -- well, it's not here on my screen. But what Jones says is when

1 you -- okay, it's over here in column 6. Let me for see here if I have the
2 relevant portion of column 6. I'm afraid I don't have it. Okay. Let me just
3 point you to it.

4 It's column 6, lines -- it's the paragraph we're talking about in column
5 6, line 12 it looks like, beginning of line 12. And it says, and this is the
6 beginning of that paragraph. It says, "In some examples it may be able to
7 look deeper into one or more components of the information system, such as
8 to provide a more thorough analysis of those components for their
9 cybersecurity threat." So it's analyzing going to another level, the n+1 level.
10 The n+1 level allows a more thorough analysis of the components or their
11 threats.

12 It doesn't say I'm adding something, I'm changing the system or I'm
13 changing the threat model. It says I'm going to analyze the threats or the
14 components at a more detailed level. So there's no discussion here of adding
15 something that wasn't already there, whether it be a component or whether it
16 be a threat or even whether it be a component of the information system.
17 We're going to analyze it. It allows us to be more granular in that analysis.

18 And that's where it talks about, as the portion that Petitioner is focused
19 on, the decomposer and what the decomposer does. First of all, I would
20 argue that implied in the name decomposer is this idea of breaking things
21 apart to look at them at a more granular level. That's what it -- that's what
22 something that decomposers does. It breaks things apart, not adding
23 anything there.

24 In addition, I know I have a Figure 1 here somewhere but let me see if
25 I can find Figure 1. Here's Figure 1. This is Figure 1 from Jones.

1 JUDGE BELISLE: Counsel, this is Judge Belisle. Now, you say it's
2 not adding anything and I would tend to agree that we're not, sort of, in this
3 discussion here of Jones' disclosure, we're not adding a component like a
4 hard drive or a Wi-Fi driver or something. We're not adding that to the
5 system.

6 But what I hear Petitioner saying is that the claim isn't talking about
7 adding a component to the system. It's talking about adding threat model
8 components to a threat model and that by decomposing the component in
9 Jones you went from having one, I'll call it a black box since that's what
10 Jones says, that you have one black box but I open it up and suddenly I have
11 a bunch of threat model components that I'm then going to add into the
12 overall threat model.

13 And so what I'd like you to continue talking about, the language that
14 Jones says it "modifies the threat model, data flow diagram for those
15 decomposed components to include them and their data flows and the
16 metadata to produce basically a different level of threat model diagram."

17 So how is the words modifying and adding these threat model
18 components, how is that not relevant to your findings?

19 MR. JACKSON: Thank you, Your Honor. Again, this is Mr.
20 Jackson. So what that -- that is a very souped up -- that's the highest level of
21 superficial visualization. That isn't modifying the threat model itself.

22 And to take again your example of the black box and the
23 subcomponents that are in the black box, those components were already
24 there when we just were showing, when we were just depicting the black
25 box, whether that be a, you know, server or a computer or what have you.
26 When you're looking at that black box those components and their threats

1 that are associated with those components are already part of the black box
2 in the system, in the overall larger system.

3 When you say, and this is what Jones is saying, when you decompose
4 it you basically take the lid off the black box and say now I want to see
5 what's giving rise to those particular threats. Maybe I want to do some
6 additional analysis or mitigation perhaps on some of these subcomponents of
7 the black box. And that decomposition allows one to do that.

8 So it's not that Jones is -- so then contrast that with what the '008
9 patent is talking about. The '008 patent is talking about bringing something
10 into the threat model that wasn't there previously. So in the case of the
11 figure we looked at earlier, the Windows 7 component was not a part of that
12 laptop. That laptop appears to be basic hardware in terms of the input and
13 output of that. That's all that was present in the threat model at that time.

14 When you import the Windows 7 subcomponent into the laptop it
15 changes the overall characteristics of the Windows -- I'm sorry, of the laptop
16 because now it's a Windows 7 laptop. It has an operating system and all of
17 the threat model components and threats that come with that. That's
18 different than what's being shown here and described here in Jones.

19 Jones is let's take the lid off the black box and see what's causing
20 these threats to occur so we can do some additional analysis on those
21 components or their cybersecurity threats. And again, that's column 6, lines
22 roughly 12 to 15. So that's what it means.

23 So I understand. And this, honestly, is what Petitioner has picked up
24 on and has touted down lower in this paragraph in column 6 where it talks
25 about, "thereby producing a level $n+1$ threat model, DFD, and there was
26 another word that they like to focus on as well that makes it sound closer to

1 what is described in the '008 patent. But we don't look at prior art
2 references, you know, for verbatim but that works both ways, right? You
3 have to look at what actually is being disclosed in the prior art, what concept
4 is really being taught, and what content -- and how does that relate to the
5 claim's concepts and the claimed language?

6 And so you can't just say, oh, well, it uses the same word. It uses the
7 word change or add or what have you and that means the same thing. It may
8 mean the same thing but my point is we have to look deeper than that. What
9 I'm saying is that when you look deeper at Jones it's clear this is more of the
10 situation where you're pulling the top off the black box to see what's inside
11 and perhaps do -- at that point taking mitigations on some of those
12 subcomponents.

13 But that's not what the '008 patent teaches. It's not what's claimed in
14 the '008 patent either.

15 And to that point, Your Honor, I would also direct you back in here to
16 this Figure 1 of Jones, and if you look at the decomposer, which is element
17 110 its only input comes from the DFD creator through the threat indicator.
18 So the threat indicator adds threats to the DFD that's output by the DFD
19 creator.

20 And the decomposer, based on this figure and there's no other
21 discussion anywhere in Jones, at least that I've found and I've been through
22 Jones multiple times, the decomposer 110 doesn't have any other sources of
23 information. The decomposer 110 has whatever is given to it most directly
24 by the threat indicator which is, you know, additional information that's put
25 on the output of the DFD creator.

1 So those threats have to be there. What other source of information
2 does it have about the system or its components? It doesn't. There's no
3 description in Jones anywhere of having some other reservoir of data that it
4 draws from and can add to the threat model something that is not already
5 present in the threat model.

6 So again, I think this Jones is disclosing the black box scenario. It's
7 something that's already there if you look at the boundary of the of the black
8 box. Whatever threats are being caused by the subcomponents internally to
9 the black box they're being reflected at the boundary of that black box and
10 all you're doing with Jones is you peel these layers or the lid off the black
11 box and look inside.

12 That doesn't, by the way, change what happens at the boundary of the
13 black box. The black box boundary is still the same. The same threats are at
14 the boundary as they were before the top was taken off the box. And that's
15 why Jones doesn't disclose a change of the first threat model by peeling the
16 lid off the black box because those threat --

17 JUDGE BELISLE: Counsel, this is Judge Belisle. Even if it were not
18 to ultimately change the threats around that black box, the claim is about
19 configuring the diagram interface, configuring that relational diagram to add
20 these threat models to -- the threat model components to the threat model.

21 And by taking a lid off the box it would seem that Jones is configuring
22 the relational diagram because before it didn't have those components to
23 now have those components and to show how they're interacting in the
24 system. Is it -- so I agree that the claim or that, you know -- let me take that
25 back.

1 The patent itself when talking about that Windows component,
2 Windows 7, added in as a component to the system, as an actual, like, it
3 wasn't -- Windows 7 wasn't there when I was trying to prepare the system of
4 the challenged patent and then I dragged it in and suddenly now it's part of
5 the present.

6 Claim 1 at least does not appear to be directed at growing the system
7 itself. It's about the threat model. And so I come back to Claim 1 recites
8 configuring the diagram interface or the relational diagram interface to add
9 these components, these threat model components to a threat model.

10 So and you may have already done it, but tell me again how Jones
11 when it decomposes a black box to reveal additional threat model
12 components is not configuring its diagram interface, redefining it, to reveal
13 those additional threat model components as part of a redefined threat
14 model?

15 MR. JACKSON: So let me give it another shot, Your Honor. I think
16 it's in this -- that particular question is answered by the claim language that
17 reads, "By including in it," that's referring to the first threat model, "by
18 including in it a second threat model associated with the component group."

19 So in the black box example, what we would refer to as the second
20 threat model, if you will, and I'm not willing to even concede there is a
21 threat model at that point, but the second threat model is already present in
22 the threat model. It's inside the black box. We're not adding a new threat
23 model.

24 Visually you can't see it. I will concede that. You don't visually see it
25 but it's there. All of its attributes are there just like if we were to look at a,
26 let's say, a Wi-Fi port. There are multiple threats that can be associated with

1 a Wi-Fi port. We don't know which one necessarily is attributable to which
2 part of the Wi-Fi port. I'm making -- picking up an example here, Your
3 Honor.

4 But my point is that the Wi-Fi port itself is a bit of a black box.
5 We've got a label. We know certain things about it, obviously, but it has
6 certain threats. And there may be certain parts of that port that are subject to
7 one threat that may not be subject to a different type of threat for an Ethernet
8 port, for example.

9 So for a for a hard drive, for what, HTTP access, those things can be
10 subject to different things -- well, HTTP is not a good example, Your Honor,
11 but I'm straying from the record so let me rein myself in a little bit.

12 But my point is that in the example of Jones we're not adding new
13 threats or a new threat model but. We're not adding a second threat model.
14 It's there even though visually you may not be able to see it. You can see --
15 but you do see its manifestation at the border of the black box and how it
16 interrelates with the rest of the system.

17 And all Jones is saying is that we can dig into that and do some
18 further analysis of that but we're not adding it. So I think that's in the claim
19 language. It's really in multiple pieces of this last paragraph of Claim 1 that
20 I think they've attempted to specifically claim that system, that arrangement
21 that's described in the '008 patent in the figure we looked at earlier.

22 So you have to add a threat model component group to the first threat
23 model, number one, and that thereby redefines the first threat model. I
24 mean, it's got to change. That first threat model that you had before had to
25 change and it's changed by including in it a second threat model. So it's

1 changed by adding a threat model that wasn't there previously, and that
2 second threat model is associated with the component group.

3 And then the claim goes on to say, "Wherein the component group
4 comprises the predefined interrelated group of two or more threat model
5 components."

6 So if I could also pick up on that and respond to something that
7 Petitioner's counsel said about that, there's a little bit of trying to have your
8 cake and eat it too in the sense that when it comes to the predefined
9 interrelated group, Petitioners pointed to the fact that there would be
10 components of the information system that were predefined and interrelated.

11 So you can't say, well, I'm going to rely on the fact that the
12 information system itself has predefined and interrelated components to
13 satisfy this requirement of the component group that gets added to the threat
14 model, but then say but we're not going to look at the information system
15 itself when analyzing the rest of this paragraph because we want to focus on
16 the threat model and not the information system.

17 It can't be -- both can't be true. You can't say the component group is
18 predefined in Jones because the information has predefined components but
19 when it comes to the earlier part of this paragraph about redefining the threat
20 models and identifying the first and the second threat models we're not going
21 to look at the at the component group. I'm sorry. We're not going to look at
22 the information system and instead we're going to look at this language in
23 Jones about decomposing components.

24 Did you have further questions on that, Judge Belisle? I know it's --

25 JUDGE BELISLE: I do have some questions. Maybe we should
26 back up in the claim. So the claim says, "Providing, "Claim 1, "Providing

1 one or more interfaces, including the diagram interface, configured to be
2 displayed." So the interface is -- am I correct that the interfaces are what's
3 being displayed?

4 MR. JACKSON: I'm sorry. I was catching up to Your Honor. Could
5 you give me a line, roughly line number?

6 JUDGE BELISLE: Oh, 44 --

7 MR. JACKSON: Forty-four, 45? Yeah, there it is. Okay.

8 JUDGE BELISLE: It says, "Providing one or more interfaces,
9 including the diagram interface, configured to be displayed on one or more
10 end user computing devices." So is it correct that the diagram interface is
11 what's being displayed? Is the purpose for having this diagram interface is
12 to be able to show it to the user? Is that correct?

13 MR. JACKSON: That's right.

14 JUDGE BELISLE: And then later in the claim, then we configure
15 that interface to display a relational diagram. So that diagram interface that
16 has been configured to display and is being displayed, you can configure it
17 to display a relational diagram so that the user can see the relational
18 diagram. Is that correct?

19 MR. JACKSON: That's right. At least that's one of the reasons, yes.

20 JUDGE BELISLE: Okay. So then we get to the last part of the claim
21 where it says, "Configuring the diagram interface." This is the part about
22 where we're adding components.

23 So I understand this section here to be focused on changing that
24 diagram interface, what's being displayed as part of the -- well, what's being
25 shown on the display, to configure that interface or to change that interface
26 so that it adds in the component group to what was previously shown as the

1 first threat model. I'm going to redefine that threat model to show it
2 including this second threat model because I've added in an additional set of
3 threat model components.

4 So is it correct that this method claim here is the last part of the claim
5 is about configuring the diagram interface. Is it correct that that is about
6 redefining, changing the threat model being shown on the screen so that it
7 shows the model including a second threat model that's associated with a
8 component group?

9 So it's about what's being revealed to the user. You're showing them
10 basically a changed threat model because they brought in additional
11 components. Is that correct?

12 MR. JACKSON: Yes and no. Yes it certainly changes what's visually
13 displayed but it's more than that. Recall that in figure, I believe it was
14 Figure 6 of the '008 patent which is not the Figure 10 view we were looking
15 at earlier, but in Figure 6 this lists the components and then their associated
16 threats. And then you can drill down into the threats on the different figures
17 here in the '008 patent.

18 So it isn't just what's shown in a figure like Figure 10 that's being
19 changed. It's also that you're adding in these components. You're also
20 adding their threats so it would be, I mean, it's still visually depicted but in
21 Figure 6 this is not the same type of a diagram as shown in Figure 10.

22 So but I guess what I'm getting at is this idea that when you add these
23 components in the claim, when you add the components into the first threat
24 model you're more than just changing the visual view on something like
25 Figure 10.

1 You're also changing the components that would be listed, for
2 example, in Figure 6. You're changing therefore the list of threats before
3 that group of components because now you have new components that have
4 perhaps their own associated threats. And you can drill down by looking at
5 the particular threats associated with each of those new components.

6 So it's not just a two-dimensional, if you will, change in what's
7 displayed on the screen but you can also go into other screens, if you will,
8 menu items or menus and you look at other components that therefore get
9 added. And if you were to -- and therefore there are associated threats and
10 then how those, of course, threats, you know, manifest themselves in the
11 threat model as a whole.

12 And in Jones they're already there, so whether we display them or can
13 see them in the display it's they're already present. They aren't being added
14 and they aren't there by redefining the first threat model. They're already
15 embedded in the first threat model. Because you're not adding that
16 component group visually you may not see it in Jones. I'll grant you that.

17 But what's described, you know, as part of the threat model in Claim 1
18 is more than just the visual representation of a, sort of, a two-dimensional
19 landscape, if you will, of the system.

20 JUDGE BELISLE: All right. So, counsel, Judge Belisle again. So
21 let me, if I understand what you're saying is Claim 1 is not about just first I
22 reveal to you on an interface five boxes and then I reveal to you on that
23 screen 10 boxes. It's not just that I'm changing what you're seeing because
24 those boxes have attached to them threats as such. I could click on one of
25 those and I would see more information.

1 So it's not just about what I'm seeing, literally see on the screen. It's
2 about the information that's coming along with what I'm seeing.

3 MR. JACKSON: That's exactly right, Your Honor.

4 JUDGE BELISLE; So with that said, let's go back to Jones in column
5 6 and this is essentially the paragraph that's all over the briefing, so in
6 column 6 of Jones, lines 12 roughly to 34. Okay. Let me know when you
7 have it.

8 MR. JACKSON: I have it here, thank you.

9 JUDGE BELISLE: Okay. About midway in that paragraph it says,
10 "The decomposer then provides feedback that its decomposition to the DFD
11 creator 106, which may modify the threat model DFD to the decomposed
12 components to include their nested components and data flows." Then as a
13 parenthetical, "(and appropriate metadata) thereby producing the level n+1
14 threat model and DFD."

15 My question is what does -- how do you interpret Jones disclosing that
16 they modify the threat model DFD, what is being modified if it's not
17 modifying the threat model? I mean, I've heard from you that Jones doesn't
18 change anything, but Jones expressly says it's modifying the threat model.

19 MR. JACKSON: Right. And so it's not that it doesn't change
20 anything. I think I have indicated earlier it does change this, what I referred
21 to earlier as the two-dimensional visualization, if you will. But what this is
22 saying is it talks about here to include their nested components. They're
23 already there. Those components were already there.

24 When it's refers to the DFD that's the data flow diagram. That's just
25 the data flow diagram or in the case of the threat model it's the threat model
26 data flow diagram, which is just the data flow diagram with the threats, those

1 little boxes. I think there were 904 of the little circles, rather, added on top
2 of the diagram.

3 So it's not saying that it's adding components that weren't there or that
4 it's changing the overall threat model of the system. It's simply allowing you
5 to dig deeper down into the system and view what may be giving rise to
6 individual threats. And that's why it says, "modified their threat model DFD
7 for the decomposed components to include their nested components."

8 Nested components and that's -- that language is, I think, elaborated
9 on a little bit more over in column 5, roughly line, I guess it really begins on
10 line 14 or 15. It says -- in 14 it says, "In this regard one or more of the
11 information system's components may include multiple nested components."

12 So those components already include multiple nested components
13 which may be further analyzed as described over in column 6 by peeling the
14 onion, so to speak, and going through a different layer of detail.

15 So even though I agree with you what you see visually in Jones, based
16 on this, when you go to a level $n+1$ threat model DFD, and let's assume that
17 there is some, you know, component at that level, what you visually see in
18 this two-dimensional depiction is going to look different.

19 But what I'm saying is when you talked about earlier how you
20 correctly characterized at least my description of the '008 patent, which is it's
21 not just you're bringing these two-dimensional components in that weren't
22 there previously but you're also bringing in the threat model -- or I'm sorry,
23 the threats that are associated with those components.

24 And that is new information that's coming into the threat model that
25 wasn't there previously. The threat model is not just the two-dimensional
26 depiction, although I think that, you know, oftentimes we call that a threat

1 model but that's not it. And it is clear from the '008 patent it's much more
2 than that. It's being able to look at individual components and see their
3 threats and mitigations, et cetera, et cetera.

4 JUDGE BELISLE: Okay. Counsel, just for your timing, you're at
5 about 44 minutes so as I said to the Petitioner I'm going to lay off on the
6 adding questions and let you move on.

7 MR. JACKSON: All right, thanks. Forty-four minutes I'll probably --
8 let me, if I may, just reserve the rest of my time. Your Honor. I think I'm
9 going to just reserve the rest of my time, Your Honor, and I'll stand on the
10 briefs with respect to the other topics I haven't been able to touch on.

11 JUDGE BELISLE: Perhaps before you go you could just touch on the
12 Claim 3 argument that you have in response to what was said just earlier
13 today by Petitioner?

14 MR. JACKSON: All right. Okay. Let me go to slide 17 at least as a
15 starting point. All right. Slide 17 is just Claim 3. The one thing I didn't
16 hear Petitioner focus on is the multiple uses of the word additional in this
17 claim, additional threat model components, additional threats, additional
18 compensating controls.

19 So in Claim 3, Claim 3 is dependent on Claim 1. It's reciting the
20 method of Claim 1 where it further stores additional threat model
21 components and additional threats. It associates the additional -- "Each
22 additional threat with at least one of the additional threat model components
23 and stores one or more additional compensating controls and associated
24 features, additional compensating controls with each of the additional
25 threats."

1 So and the faults that we find in the petition with respect to Claim 3 is
2 that Petitioner didn't identify any additional groupings of threat model
3 components, threats, or compensating controls that would line up with Claim
4 3.

5 Instead they relied on the same set of threats, compensating controls,
6 and threat model components that they identified with respect to Claim 1.

7 And then on slide 18 they have an excerpt of the deposition testimony
8 of Petitioner's expert, Mr. Hurlbut, and he agreed -- this was at the
9 beginning. This is from Exhibit 2002, page 82 starting at line 17.

10 So the question was so the additional threat model components of
11 Claim 3 are not satisfied by the threat model components of Claim 1, right?
12 He says correct. And then we asked him the same question with respect to
13 the threats and the compensating controls and he agrees that whatever would
14 line up with Claim 3 is not the same or wouldn't be satisfied by what was
15 identified with respect to Claim 1.

16 And at the end here on this page, he says that's the understanding he
17 used when he analyzed Claim 3 in his declaration. But in the petition they
18 didn't identify anything other than what they had already previously pointed
19 to. And, in fact, in Petitioner's presentation today there was no distinction
20 between the threats and compensating controls and threat model components
21 of Claim 1 versus what would be satisfied by Claim 3. Petitioner, if my
22 memory is correct, simply pointed to the same teaching in Jones for Claim 3.

23 JUDGE BELISLE: Okay. Thank you, counselor. Before you go do
24 you want to touch on that one argument that I raised with respect to Ground
25 2 regarding selecting one component first without the other?

26 MR. JACKSON: Yes.

1 JUDGE BELISLE: And just so you know, I'm going to give each side
2 five extra minutes here because of all my questions. So --

3 MR. JACKSON: Well, thank you, Your Honor. Yeah. So I agree
4 with Your Honor a hundred percent but, you know, Claim 2 recites receiving
5 a user selection of, one, the diagram threat model components, and the
6 Petitioner relies on Zheng for this.

7 Zheng only discloses the display or not displaying of layers as a whole
8 so there isn't a selection of a particular threat model component where you
9 can look at the threats associated with that in the case of Claim 2 paths
10 associated with those threats for a particular component. There may be
11 benefits to doing the system differently, but the claims recite this particular
12 arrangement. You want to be able to in the context of this Claim 2 you want
13 to be able to select the particular threat model component and see all of the
14 attack paths or to see all the attack paths for all these threats that are
15 associated with that component.

16 And that's not what Zheng discloses. Zheng is the layered teaching
17 where it has, this is in slide 20. Zheng has these different layers, 202 being
18 the base layer of the actual system itself and I think 204 is the layer
19 representing threat modeling.

20 So here on slide 21 it's describing these different layers but there's no
21 teaching anywhere in Zheng of being able to select a particular individual
22 threat model component. It's focused on layers.

23 There are later -- let me get back to the slide. This comes from the
24 reply brief. This is slide 23. The reply cites to Zheng at column 11, lines 41
25 to 55 and in Zheng 41 to 55 at column 11 it talks about how the -- it says, "In
26 some embodiments at least one of the base layer 202, the threat modeling

1 layer 204, the security controls layer 206, or the threat update layer 208, has
2 subcategories in the layer that can be toggled, for example, enabled or
3 disabled by the user.

4 So that's a category or subcategory, but it's still -- it's not selecting an
5 individual threat model component certainly. And then it goes on and says,
6 "For example, a particular type of threats in the threat model modeling layer
7 204 can be toggled on or off to provide more focused visualization." So
8 again, we're talking about a type or a category or a subcategory but not a
9 selection of an individual sub -- threat model component.

10 In fact, in this case it's particularly talking about threats not threat
11 model components.

12 JUDGE BELISLE: Counsel, it's Judge Belisle. This is my last
13 question before we move over to Petitioner. I understand that it may not, as
14 I said to the Petitioner, explicitly recite selection of one component as the art
15 that's being applied. But we're not in an anticipation environment. We're in
16 an obviousness environment with skilled artisans that could -- I don't think I
17 know exactly what the skilled artisan is here, but I'm sure it's a four-year
18 degree in some type of engineering or science field.

19 So why would it have not, faced with disclosures of toggling on and
20 off various threats, selecting threats, how does not these teachings of being
21 able to manipulate what's being revealed to the skilled artisans or on the
22 screen to a user, how does that not at least suggest to the skilled artisan
23 selecting a particular component, isolating it down to a component? If they
24 can do all those other things how can they not simply just select the
25 component or at least suggest to them to do that?

26 MR. JACKSON: I'm not saying it's not possible or wouldn't have been

1 possible. I'm saying that Zheng doesn't disclose that or suggest that. In fact,
2 Zheng's focus is on the layered approach or the subcategories at most
3 approach. The only way you get to selecting an individual component,
4 threat model component is through hindsight. That's the only way you get.

5 There isn't anything in the references themselves that suggest that.
6 Are there -- there are probably a multitude of things that a person of skill in
7 the art could do based on the teachings.

8 This is a particular aspect to the claims but there isn't any evidence-
9 based reason for getting there from Zheng, even in Zheng in combination
10 with Jones, which we argue in the briefing can't properly be combined. But
11 you don't get there with Zheng's teachings.

12 Zheng talks about being able to look at either layers or at best
13 enabling or disabling categories or subcategories of threats or components of
14 the individual layers, but there's no teaching of the individual. Why?
15 Because in Zheng, Zheng thought it was beneficial, for example, in the case
16 of toggling threats on and off, to be able to see those categories of threats
17 across the entire system. Zheng's focus is not on a particular component of
18 the system. There's no indication that there's any desire to look at an
19 individual component in the system.

20 Jones, on the other hand, takes the exact opposite approach to the
21 whole thing. In Jones you can -- this was the popup box 814, I think. In
22 Jones you can select a particular component and look at additional data or
23 metadata of this system. But there's no description. There's no teaching or
24 desire in Jones, anything that's evidence-based that would suggest that you'd
25 want to go to a layered approach and look at layers of information, which is
26 what Zheng is teaching.

1 So this goes to our point about there's really no proper reason for
2 combining Zheng with Jones. Those two really teach diametrically opposed
3 approaches and therefore there's not really a reason for combining this.

4 Your Honor, I mean, if you were an engineer or a person of skill in
5 the art at the time maybe, you know, that's one thing you would have come
6 up with. But I think that it's fair to say from the teachings here that the only
7 way you'd come to that conclusion is because you knew that was your
8 objective. And that's what they've done here.

9 Essentially what I heard, this is my characterization of what I heard in
10 the presentation earlier from Petitioner, was we can see a lot of the
11 components in the prior art and it would have been desirable because, of
12 course, it's self-serving for a person of skill in the art to pick and choose the
13 pieces and come up with the claims.

14 That's obviously not the right approach. You have to have an
15 evidence-based approach to not just combining the references but also what
16 would that combination yield? And that's just not present on the record here
17 at all.

18 JUDGE BELISLE: Okay. Thank you, counsel. That's going to -- so
19 like I said, even though that was 55 minutes, we're going to add some time
20 here.

21 So we're going to turn to Petitioner for rebuttal. Petitioner, you will
22 have the additional five minutes which gives you 18 minutes in total.

23 And Patent Owner, for your planning purposes you will have 10
24 minutes of rebuttal with the additional five minutes added.

25 MR. JACKSON: Thank you, Your Honor.

26 JUDGE BELISLE: Petitioner, when you're ready?

1 MR. YAMASHITA: Thank you, Your Honor. Brent Yamashita for
2 Petitioner again. You know, I think I'll address some of the issues raised by
3 Mr. Jackson in reverse order. So I'll start with Zheng, the thing that we just
4 finished talking about.

5 First, I would just like to point out that, with all due respect, counsel
6 contradicted himself when he was talking about Zheng. At first he said
7 Zheng only discloses the ability to turn an entire layer off or on. So turn the
8 layer on or turn the layer off. But then later he did start talking about the
9 subcomponent, which is the portion of Zheng that I touched on earlier.

10 So Patent Owner argued two different positions there that are
11 inconsistent. But in any event, I have put back on the screen Zheng. So
12 we're looking at column 11, lines 42 through 55 which is what counsel was
13 just talking about.

14 And here Zheng is not too restrictive at all. The very first sentence
15 says, "In (unintelligible) results in visualization to achieve the desired
16 display effects." So it's not saying, oh, you can turn off a category of Zheng
17 but you can't go any finer than that. The teaching to a POSITA is that, you
18 know, if it's known that a user might want to interact with the visualization
19 to turn things on or off, Zheng is encouraging that and teaching that.

20 But even if we were to view Zheng the way Patent Owner does, he
21 just conceded that this portion of Zheng talks about turning on or off a
22 particular type of threat. And I think the point he was making was it's
23 talking about categories and not individual things.

24 So even if we were to view Zheng exactly the way he does, you could
25 certainly have a threat model where you have a category and only one
26 instance of the thing in that category. And in that instance the clear reading

1 of Zheng is, well, if you turn on and off the category, since there's only one
2 item that is in that category, so one laptop or one port or whatever, if you're
3 turning on or off into a category, by definition you're turning on and off the
4 one thing that's in that category because there are no other members of that
5 category.

6 And that's certainly a possibility and a person of ordinary skill would
7 understand that.

8 So I guess to wrap up the point on Zheng, Zheng is teaching what you
9 should come to expect from graphic user interfaces. It's just that, you know,
10 users like the ability to manipulate the user interface to make things easier or
11 harder for them as needed. And Zheng is certainly trying to teach them that
12 threat within the threat model realm what happens on the screen you can
13 enable or disable things to achieve the desired display effect.

14 So those are my thoughts on Zheng. I then would, kind of, go in
15 reverse order. I would like to go back to Claim 3, which Your Honor was
16 asking about. So I'm going to go back to my slides and specifically to slide
17 22 of Exhibit 1017, that slide. And I'm just putting this up simply just to
18 have Claim 3 on the screen.

19 So I think we're all agreed that, you know, Claim 3 depends on Claim
20 1, and it does say that you have to deal with additional components,
21 additional threats, additional compensating controls. But with all due
22 respect, I think Mr. Jackson ignored the portions of the spec that I, kind of,
23 marched through earlier today when I showed you portions of Jones that
24 expressly say that for all of those things, components, threat, controls, that
25 those can come from the user, the operator, and then that information is
26 stored in a database or other system such as a file system.

1 Jones does that for all three types of things and, you know, it's clear
2 that Jones was not limited to Figure 9. You know, I've relied on Figure 9
3 heavily for Claim 1 that it seems, okay, Claim 3 requires something other
4 than whatever it is you can see I relied on in Claim 1.

5 You know, this is a dynamic system. It's a threat modeling system.
6 So a user, a person of ordinary skill in the art would understand that you
7 could add to Figure 9. You could create a new threat model altogether.

8 And Jones teaches us that as you do this for components, threats, and
9 compensating controls you can get that information to populate your
10 databases from the operator and then store them in a database. So, you
11 know, Claim 3 in our view is met by Jones then.

12 Next, I'd like to --

13 JUDGE BELISLE: Counsel, before you move on from that slide, it's
14 Judge Belisle. I think I just need to spend a little more time, sort of,
15 appreciating what you're arguing here and that is that you have citations that
16 were used from Jones used to support the anticipation of Claim 1.

17 Now, this method adds in this further step of configuring the interface
18 in response to user input to store more, well, one or more additional threat
19 model components." Where are those -- where are those additional threat
20 models components coming from in Jones?

21 Jones already had a system. The system had, sort of, levels to it. You
22 could decompose a given component to view -- or, sort of, decompose a
23 black box to reveal additional -- the components that are within that box.
24 Where does Jones talk to me about storing additional threat model
25 components beyond the system it's looking at?

26 MR. YAMASHITA: Sure. Let me address that, Your Honor. So Claim 1 is

1 talking about a specific threat model. So in our view a threat model is the
2 threat model is a data structure that represents a real-world, physical system.
3 So to make it more tangible, in my law firm we have a computer network.
4 That's a physical system. Jones teaches us that you can create a threat model
5 to represent that system and let's just say that Figure 9 results from that.

6 What Claim 3 is talking about is not adding to the threat model. It's
7 talking about adding basic information to the databases that are used to
8 create the threat model. So it's talking about, what we'll call Claim 1, talks
9 about having one or more databases that stores threats and threat
10 components. This is simply saying you can add to those databases. You're
11 not adding to the threat model. You're just adding -- so let's just go back to
12 my example.

13 Suppose there's a new router that comes out onto the market and some
14 IT guy is like, oh, there's a new router on the market. Let me add that to my
15 threat model system so that we can use that component in future threat
16 models. That's the level at which this comes into play. Like, there's a new
17 component of some sort of interest, a new threat, a new compensational
18 control and a person is using the system to add those things to the databases
19 so that you can later use those things to build your treat model.

20 So again, we're not adding it to the threat model. We're adding it to
21 the databases from which the threat models are built. And the portion of --

22 JUDGE BELISLE: So --

23 MR. YAMASHITA: Okay.

24 JUDGE BELISLE: -- now, let's take that, just take me back to Jones
25 and show me where Jones at an anticipation level discloses doing that.

1 MR. YAMASHITA: Sure, Your Honor. I'm going to flip back to
2 Jones. (unintelligible). Okay. So again, so Claim 3 is talking about adding
3 components, threats, and controls to your databases. It's not requiring that
4 we add them to the threat model with Figure 9. It's simply that a user
5 teaching (phonetic sp.) to add those components, threats, and controls to the
6 database. And so I'll take them in order.

7 Component, if you look at Jones column 7, lines 49 to 53, I've
8 highlighted it here, Jones is talking about components. And it says, "The
9 components may be identified through the collection of information from an
10 operator, security architect." So in my example that would be assumed to be
11 an IT guy and, hey, there's a new router on the market. Let's add that to our
12 database so we can use it later in the threat model. This is saying a person,
13 the operator, can add that information.

14 And then a couple of paragraphs later in column 8, lines 10 through
15 20, Jones is still talking about this DFD decomposer to (unintelligible) its
16 work. It's saying that the information that I was just talking about can be
17 stored in any number of different types, file storage, database storage, cloud
18 storage. (unintelligible) is, of course, the same. I can receive information
19 about components from the operator, and then it's saying, "And then I stored
20 it, of course, just to use it and one of the places you can store it is in the
21 database."

22 So this is part of Claim 3 where Claim 3 talks about receiving input
23 from a user and storing it in a database. This is component.

24 Then we have similar language to threat and compensating control.
25 Threat is here at column 12, lines 22 through 25. It says that "An operator, a
26 person, can provide information regarding threats." And then later, lines 48

1 to 54, Jones says, "You can store the data I was just talking about, threats in
2 a threat model DFD storage (unintelligible)," which, again, in the
3 parenthetical says it could be a database.

4 And then finally we have the same type of language for compensating
5 controls, column 15, lines 10 through 12 and 18 through 22. It says exactly
6 the same thing, that the suggested mitigation which are compensating
7 controls, can come from the collection of information from the operator.

8 And then it says, "And these things can be stored in storage such is a
9 database."

10 And for controls it has, sort of, an extra portion that I've highlighted at
11 lines 27 through 31 where it goes into even more detail in (unintelligible)
12 and says, "It can source information from the operator through questions and
13 answers regarding possible mitigations of threats to the information system,
14 its performance and data flow."

15 So these are the portions of Jones, as well as other portions that satisfy
16 Claim 3. These are outside of this scope of Figure 9 and outside of whatever
17 I relied on for Claim 1. This is just simply saying that we build our database
18 by allowing the operator to input information regarding components, threats,
19 and controls and we store those things in a database or cloud storage or file
20 storage.

21 JUDGE BELISLE: Thank you, Counsel. You can continue.

22 MR. YAMASHITA: Thank you. And I'm going to go back to my
23 slides and, again, kind of going in reverse order. I want to go back to Claim
24 1 and Jones. Your Honor asked several question of Mr. Jackson and I just
25 wanted to respond to a few things that he said.

1 So I think in our view of things there's a few things that, sort of, you
2 need to mentally keep track of. So one is, you know, there might be a
3 physical system that you're building the threat models of, so my example the
4 physical network in my building is, like, a real thing that I can process
5 (unintelligible). That's what Jones calls the information system.

6 Then you have your threat model environment, a threat model
7 software that allows a person like Mr. Hurlbut to build a threat model. This
8 is the thing that has access to databases that are populated by information
9 from the operator. And from that you can build a threat model.

10 In my view, a threat model is a data structure. It's the data that
11 represents whatever it is you're trying to model in the real world. And I
12 think that often that data structure doesn't really mean much in the real world
13 because I think only patent people care enough about the structures in
14 computer sciences, and so this point manifests itself through a visualization.

15 And, you know, the visualization is a graphical depiction of your
16 threat model that you see, you know, components, threats, and attack paths.
17 And that's really the portion that's most useful to people and so Claim 1 does
18 talk about those threat models as well as the diagrams representing the threat
19 models. And I think in the real world these are often conflated together
20 because people really only care about the visualizations and not the data
21 that's underlying it.

22 But to pick up on the question that you had asked Mr. Jackson about,
23 this portion of Claim 1, let's start off at the (unintelligible). It's in the
24 graphical environment. I then want to add a component group to my threat
25 model, which again, I view as a data structure.

1 And that's exactly what Jones is saying when it's talked about here in
2 column 6, lines 12 through 34, Jones talks about the decomposer being
3 called into action to look at the component and figure out what its threat
4 components are.

5 And, you know, the line in Jones, this highlighted portion that I have
6 here, says that "You may modify the threat model DFD for the proposed
7 components if you include their nested components and data flows." So
8 you're modifying the existing threat model. First of all, that's not very
9 obvious language of the claims. You're modifying the threat model.

10 But this is also telling us that that information wasn't there in the
11 existing threat model. If it was, why would you need to modify it? It is
12 surely the decomposer that figures out what those method components are
13 and tells the DFD creator what those are so that the threat model can then be
14 modified to include the nested components.

15 And the same with threats. Those threats were not part of the original
16 threat model. They are added to the work of the threat indicator 108 that's
17 described in this paragraph.

18 So, counsel used this analogy quite often about a black box, and he
19 seems to suggest that if you open the lid and walk through what's inside that
20 black box that it was there all along. I think a more accurate way to use that
21 analogy with the teaching of Jones is, yes, there's a black box but when you
22 open it it's empty because we don't know what goes in there.

23 We don't know what goes in there until the decomposer and the threat
24 indicator and the DFD creator perform the work that's described in this
25 portion of Jones. Once it does that and we look back into the black box and
26 we see and nested components and threats, and then Jones tells us in that

1 thing has modified the original threat model and for in the alternative you
2 could store it as a use threat model.

3 So clearly, you know, the original threat model has been modified and
4 this information was not present all along because if it was you wouldn't
5 need to have to the decomposer there and the threat indicator to see anything
6 at all. It would already be there and it wasn't.

7 JUDGE BELISLE: Counsel, you have one minute left.

8 MR. YAMASHITA: Okay. I'll just end on a less dramatic issue,
9 which is Mr. Jackson talked about this constant redefining in the first threat
10 model. First, I would just note that Patent Owner's claim construction really
11 adds a lot of language to an otherwise simple phrase that we're defining.
12 And this just, you know, screams immediately of adding limitations for the
13 amount (unintelligible) previously.

14 But on top of that, he focused his -- he emphasized this aspect of you
15 have to add something that was not there before. And conceptually I think I
16 understand what he's getting at but the problem I have with this is if we go
17 back to the example of the '008 patent with the laptop and Windows, we
18 suppose we had a threat model with multiple laptops. My original threat
19 model already has the laptop and it already has Windows in it. And then I
20 want to add another laptop.

21 This leads to -- if we read -- if we apply this literally, (unintelligible)
22 is saying, like, oh, well, when you add that Windows 7 threat model to your
23 second laptop that doesn't count because it's already present in the first
24 laptop over here. And that's one logical problem I have with his
25 construction, which is that he's trying to carve out something but he's trying
26 in vain so he's definitely, I think, not staying true to the original language but

1 also leading us to a place that I think just doesn't make sense in terms of the
2 issues of the patent and just what the words say.

3 So I think my time is up. And unless Your Honors have any other
4 question?

5 JUDGE BELISLE: Well, thank you, counsel.

6 Patent Owner? Patent Owner, I'm going to bump you to 11 minutes.
7 You have an extra minute.

8 MR. JACKSON: Thank you, Your Honor. I'll try not to use all that
9 time. So again, Mr. Jackson for Patent Owner.

10 Let me just start where counsel just left off on the claim construction
11 of the phrase "redefine the first threat model." So this particular issue that
12 they raised, they raised this issue in their reply and we addressed this in our
13 surreply at pages 1 to 2, so I don't want to spend a lot of time. This is the
14 issue of, well, if the Windows 7 laptop is already there and you add another
15 one then you aren't satisfying the claim language.

16 We've addressed that in our briefing and in our surreply on pages 1 to
17 2, and I don't have anything more to say about that. It doesn't satisfy the
18 claim language to add a second version of the laptop and say that it doesn't
19 satisfy the claim language because when you add the second laptop you are
20 redefining -- you are further redefining the first threat model. So let me just
21 hit that one real quick.

22 Going backwards, Jones' decomposer and this is Figure 1, let me see if
23 I can share my screen real quickly. So again, Petitioner made the point or
24 made the argument that the decomposer would add these components to the
25 system as part of this feedback here in Figure 1. But I made this point
26 earlier, there is no input to the decomposer 110 other than what the

1 decomposer receives from threat indicator 108, which is just adding threats
2 to DFD creator 106.

3 So if it's not already present there's no way for the decomposer to
4 know that those components are there, so it's not an empty black box. It's a
5 black box that has components in it. We're just not visually looking at those.

6 And there's no description anywhere in Jones, as I said earlier, that I
7 found of any other source of information for the decomposer 110. So based
8 on the teachings of Jones themselves, you've got to say whatever it's
9 exposing through its decomposition process has to be something that was
10 already there. It received it from the DFD creator via the threat indicator.
11 There's no other source. You won't find any other teaching in Jones about
12 that.

13 Also with respect to the -- I'm, sort of, going backwards here again,
14 but claim construction of the redefined phrase, and I apologize for going
15 back to it. I meant to make one additional point before I moved on.

16 But just the phrase redefined the first threat model by including in it a
17 component group having a second threat model, and I'm paraphrasing. We
18 need to step back. You know, claim construction, just to reorient ourselves,
19 everybody knows this but claim construction starts with looking at the
20 intrinsic evidence, that they try to understand what the claims mean. We
21 obviously start with the claims but we don't end with the claims.

22 We look to the specification. What is it teaching? We look to the
23 prosecution history if it's relevant. And when you look at the specification it
24 appears that based on the discussion earlier it seems clear that Claim 1 is
25 addressing the situation where, and just to use an example, you're importing

1 the Windows 7 component or subgrouping into the laptop subgrouping.
2 That's the situation that the claim is directed to.

3 And I asked myself as we were talking here today how would the
4 applicant have changed Claim 1 to more clearly recite that arrangement if
5 not for the language that they used here? And I come empty on how else
6 they could have been more clear, but they were not addressing or intending
7 to include or including within the scope of the claims what's disclosed in
8 Jones, which is this exposing of additional components that are already part
9 of the system and they're already in the threat model based on Figure 1 or in
10 the DFD at least based on Figure 1.

11 So how else would they have captured what they intended to claim but
12 exclude something like what's being shown in Jones? I don't know. That's a
13 rhetorical question, but I think it's something that we ought to think about
14 because that's, sort of, the point. What do the claims mean in the light of the
15 specification, in light of the teaching of the specification of which the --
16 where the inventor or the applicant attempted to describe and then claim the
17 invention?

18 Another point, just moving on, another point that Petitioner's counsel
19 made was regarding Claim 3 and the additional components language in
20 Claim 3. One part, let me see if I can find it, I think I have it here pulled up
21 on my screen. This is -- you can see slide 22 from Petitioner's presentation.
22 Is that visible?

23 JUDGE BELISLE: Yes, I can see it. Yes.

24 MR. JACKSON: Okay, great. So on the left-hand side they have
25 Claim 3 repeated here but you'll notice in the whited out portion, the parts
26 that aren't highlighted, it says that here in the middle of Claim 3, it says that

1 you have to associate each additional threat with at least one of the
2 additional threat model components.

3 So it's not just adding additional threats or additional threat model
4 components to the database. It's now that within this second group, within
5 this group of additional components I'll call them, within this group of
6 additional components the prior art has to show that one of the -- each
7 additional threat is associated with one of the additional threat model
8 components, not one of the components or threat model components that
9 were there originally. It's got to be within this set of components or threat
10 level components that are added.

11 And then later at the very end of the claim it also has similar
12 language. It says, "and associate each additional compensating control with
13 at least one of the additional threats through one or more databases." So
14 again, this is subdividing in the claim. It's subdividing the totality of the
15 threats, the totality of the threat model components and the totality of the
16 compensating controls into two groups,. One is recited in Claim 3 -- I'm
17 sorry. One is recited in Claim 1 and then the additional ones that are added
18 in Claim 3, and in Claim 3 there has to be this association, our point was
19 they didn't identify this additional category of components, threats, or
20 compensating controls and because they didn't identify this additional
21 category they certainly didn't satisfy this additional associating language
22 that's in Claim 3.

23 Last point is that with respect to Claim 2, and this has to do with
24 Zheng so let me find my --

25 JUDGE BELISLE: Counsel, this is Judge Belisle. Before we move
26 on on this, I just want to honor (phonetic sp.) your point. So Claim 1 says --

1 of the challenged patent, "Providing one or more databases to one or more
2 databases comprising threat model," and I'm paraphrasing here, "threat
3 model component, threats that are associated with those components." Well,
4 I should emphasize a plurality of threat model components, a plurality of
5 threats that are associated with that model component and a plurality of
6 compensating controls that are associated.

7 So it has this plurality of components, threats, threat models, threats,
8 and compensating controls, so what is it Claim 3 is adding? You already
9 have a comprising claim with a plurality of all three of those things
10 (unintelligible). What is Claim 3 adding to that comprising claim?

11 MR. JACKSON: So Claim 3 is adding additional method steps. This
12 is a method -- Claim 1 is a method claim. So Claim 3 is adding additional
13 method steps that have to be satisfied. So once you have satisfied Claim 1,
14 that is you have this grouping of threat model components and threats and
15 compensating controls and you, you know, done -- well, done the analysis, if
16 you will, on the system based on those, Claim 3 requires that we, as an
17 additional method step, store these additional threats or their threat model
18 components and compensating controls and then make those associations
19 within that additionally stored set of elements, threat level components.

20 So within this additionally stored set of elements there has to be this
21 interrelationship association among those. So that's what Claim 3 adds.

22 JUDGE BELISLE: Well, Claim 3 strikes me that it's simply further
23 populating the database with additional threat models that have associated
24 threats and associated compensating controls. Is it doing anything more than
25 just further populating the database with these items?

1 MR. JACKSON: It is. It's not just adding these additional or further
2 populating to use your language, Your Honor, but it also says that within the
3 group that is added you have to make these associations among threats and
4 threat model components and among compensating controls and threats. So
5 it has to be within that group.

6 Again, I think the applicant was trying to claim -- probably trying to
7 claim a different scope of the invention. That's a common practice, as Your
8 Honors know, for purposes of at least protecting you against potential prior
9 art and so this is one of the ways that they decided to do that. And they've
10 recited this particular additional set of method steps and at least one method
11 step that has to be performed. It requires this additional storage and
12 association and it has to be the association within the group of components --
13 or elements that are added via -- per Claim 3.

14 JUDGE BELISLE: Counsel, it's Judge Belisle again. Would you
15 agree that the method step being added in Claim 3 that there's no ordering
16 requirement to that as in when that occurs relative to Claim 1?

17 MR. JACKSON: I don't see an ordering requirement, Your Honor.

18 JUDGE BELISLE: Thank you, counsel. You have about one minute
19 left if you want to --

20 MR. JACKSON: Okay.

21 JUDGE BELISLE: -- take it home.

22 MR. JACKSON: I think I just had one point as it relates to Zheng and
23 Claim 2 and counsel focused on, again, the portion of Zheng at column 11,
24 beginning at lines 4. It's the paragraph that goes 41 to line 55. And again, I
25 think that counsel was essentially trying to make the argument that, well,

1 you know, we're close enough and so that would render it obvious. But
2 that's not what the petition relied on.

3 The Petitioner or the petition, rather, relied on Zheng in its disclosure
4 as teaching the elements of Claim 2 and but counsel said here with respect to
5 this subcategory language here at line 45, counsel pointed to the fact that
6 Zheng says that the different layers can have subcategories in the layer that
7 can be toggled, either be enabled or disabled by the user.

8 And then it goes on to say, for example, a particular type of threats,
9 and counsel, I think, focused on that particular language. But threats is not
10 what recited in the claim. The claim says selecting one threat model
11 component, not a threat, but a threat model component and then being able
12 to visualize all the attack paths associated with the threats that compromise
13 that particular threat model component.

14 So I'm just pointing out that I think that even with counsel's, you
15 know, further elaboration on what Zheng allegedly means it still doesn't
16 satisfy Claim 2.

17 And that's all I had, Your Honor, thank you.

18 JUDGE BELISLE: Thank you, counsel. Okay. It does not appear
19 our panel has any additional questions for either of the parties at this time.
20 Counsel, your case is submitted, and taken under advisement. We are off
21 the record.

22 (Whereupon, the proceedings at 3:51 p.m. were concluded.)

IPR2023-00821
Patent 10,699,008 B2

PETITIONER:

Brent Yamashita
Blake Jackson
Matthew Middleton
DLA Piper LLP (US)
brent.yamashita@dlapiper.com
blake.jackson@dlapiper.com
matthew.middleton@us.dlapiper.com

PATENT OWNER:

Donald Jackson
Marc Kaufman
RIMON P.C.
donald.jackson@rimonlaw.com
marc.kaufman@rimonlaw.com