

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

IRIUSRISK, INC.,
Petitioner,

v.

THREATMODELER SOFTWARE, INC.,
Patent Owner.

Case IPR2023-00656
Patent 10,713,366

SUPPLEMENTAL DECLARATION OF SETH JAMES NIELSON, PH.D.

Case IPR2023-00656

Patent 10,713,366

Supplemental Declaration of Seth James Nielson, Ph.D.

EXHIBITS

Exhibit No.	Description
EX-2001	Patent Owner’s December 4, 2023 Power of Attorney
EX-2002	Transcript of Robert Hurlbut Deposition taken December 18, 2023
EX-2003	CIO Article dated August 23, 2016
EX-2004	Draft NIST Special Publication 800-154 entitled “Guide to Data-Centric System Threat Modeling,” March 2016
EX-2005	Excerpts from <i>Measuring and Managing Information Risk, A FAIR Approach</i> , by Jack Freund and Jack Jones, 2015
EX-2006	NIST Special Publication 800-30, Rev. 1, entitled “Guide for Conducting Risk Assessments, Sept. 2012
EX-2007	Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, April 6, 2015
EX-2008	Excerpts from <i>Threat Modeling</i> by Frank Swiderski and Window Snyder, 2004
EX-2009	Declaration of Seth James Nielson
EX-2010	Supplemental Declaration of Seth James Nielson
EX-2011	Excerpts from the PDF version of <i>Measuring and Managing Information Risk, A FAIR Approach</i> , 2015 copyright date
EX-2012	U.S. Copyright Office record for <i>Threat Modeling</i> by Frank Swiderski and Window Snyder, 2004

1. I am Seth James Nielson, Ph.D. I am over 18 years of age. I hereby declare as follows:

2. I have personal knowledge of all of the matters about which I testify in this declaration. I am the same Seth James Nielson, Ph.D. who provided a declaration in support of Patent Owner's Response in this same IPR on January 12, 2024.

3. My background, qualifications, compensation, and engagement terms for this IPR are the same as provided in my January 12, 2024 declaration. My qualifications also include education and professional experience with threat modeling and cybersecurity risk management. The importance of threat models and basic examples of threat modeling are typical topics for courses in cybersecurity. For example, my first graduate class in computer security in 2004 used as the textbook "Security Engineering" by Ross Anderson (1st edition). This edition of the book is freely available online from Ross Anderson's website (<https://www.cl.cam.ac.uk/~rja14/book.html>). Anderson explains that threat models are fundamental to cybersecurity: "Where a top-down approach to security engineering is possible, it will typically take the form of threat model—security policy—security mechanisms." (Security Engineering, 1st Edition, p. 138). He goes on to say, "In a top-down approach to security engineering, one should first

determine the threat model, then write the policy, and finally test the policy by observing whether it works in real life.” (*Id.* p. 171). Throughout the text, the importance of the threat model to cybersecurity is repeated and analyzed.

4. Chapter 22 of the first edition also includes an example of concrete threat modeling techniques. For example, one such technique known as “threat trees” at pages 500-501. I have reproduced an illustration from this chapter hereinbelow:

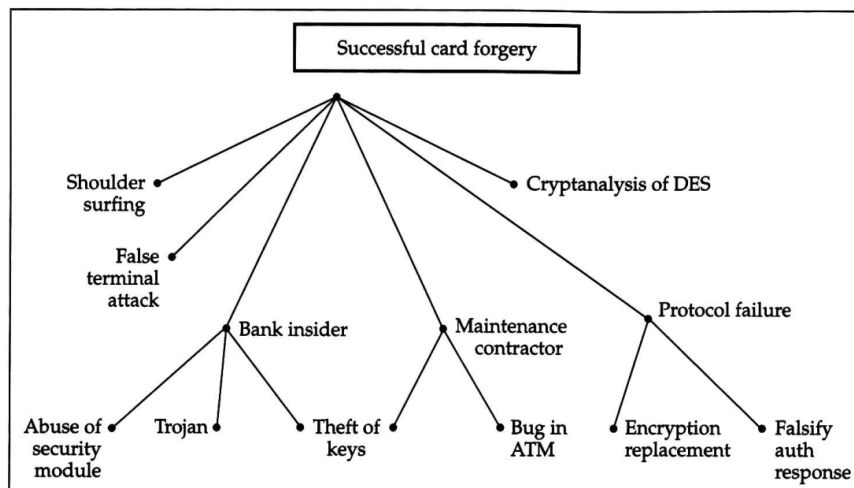


Figure 22.4 A threat tree.

5. I subsequently taught courses in Network Security at the undergraduate and graduate levels at the Johns Hopkins University from 2014-2019. I used later editions of Ross Anderson’s book as my text and specifically instructed my students on threat models and techniques such as threat trees.

6. Moreover, in my work as a professional cybersecurity engineer, I worked with my clients to develop threat models. I also used the threat tree analysis as one of the approaches in creating the model. This included threat models for a medical device manufacturer. I have also used frameworks such as NIST SP800-154 (“Guide to Data-Centric System Threat Modeling”, <https://csrc.nist.gov/pubs/sp/800/154/ipd>) in my work with clients.

7. Similarly, I have also taught and also consulted on the topic of cybersecurity risk management. On these topics, I also use various guidelines and recommendations including those from NIST. A list of relevant NIST publications related to risk management can be found here: <https://csrc.nist.gov/projects/risk-management/publications>. These are publications I have used in consulting with clients about cybersecurity risk.

8. Exhibit 2003 is a true and correct copy of an article published by CIO magazine on its website entitled “Risk = Likelihood x Impact” having a publication date of August 23, 2016. (<https://www.cio.com/article/238969/risk-likelihood-x-impact.html>, last accessed on January 31, 2024). I was personally familiar with CIO magazine for years prior to the date of this article. CIO magazine continues to publish today at the www.cio.com URL.

9. Exhibit 2004 is a true and correct copy of the Draft NIST Special Publication 800-154 entitled “Guide to Data-Centric System Threat Modeling” dated March 2016.

(https://csrc.nist.gov/files/pubs/sp/800/154/ipd/docs/sp800_154_draft.pdf, last accessed January 31, 2024). NIST stands for National Institute of Standards and Technology which is an agency within the U.S. Department of Commerce. According to the NIST website for Exhibit 2004, NIST SP800-154 was intended to provide information on the basics of data-centric system threat modeling (<https://csrc.nist.gov/pubs/sp/800/154/ipd>, last accessed January 31, 2024). I have been personally familiar with the NIST SP800-154 publication for many years.

10. Exhibit 2005 is a true and correct copy of excerpts from the book entitled *Measuring and Managing Information Risk, A FAIR Approach* by Jack Freund and Jack Jones and dated 2015. The excerpts that make up Exhibit 2005 are from the electronic book version of the book. But the book is also available in hard copy and online in PDF format. I have a copy of *Measuring and Managing Information Risk, A FAIR Approach*.

11. Exhibit 2011 is a true and correct copy of excerpts from the PDF version of *Measuring and Managing Information Risk, A FAIR Approach* having a

copyright date of 2015. Exhibit 2011 reproduces the same pages/information as shown in Exhibit 2005.

12. Exhibit 2006 is a true and correct copy of the NIST Special Publication 800-30, Rev. 1, entitled “Guide for Conducting Risk Assessments” dated September 2012.
(<https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>, last accessed January 31, 2024). NIST stands for National Institute of Standards and Technology which is an agency within the U.S. Department of Commerce. According to the NIST website for Exhibit 2006, NIST SP800-30 was intended to provide guidance for conducting risk assessments of federal information systems and organizations (<https://csrc.nist.gov/pubs/sp/800/30/r1/final>, last accessed January 31, 2024). I have been personally familiar with the NIST SP800-30 publication for many years.

13. Exhibit 2007 is a true and correct copy of the Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009, dated April 6, 2015.
(<https://nsarchive.gwu.edu/sites/default/files/documents/3238368/Document-08-Committee-on-National-Security.pdf>, last accessed February 1, 2024). This copy was obtained from the National Security Archive maintained by The George Washington University in Washington, D.C. The current version of this

publication is dated March 2, 2022 (included in CNSS's current publications here:

<https://www.cnss.gov/CNSS/issuances/Instructions.cfm> last accessed February 2,

2024). According to the CNSS About webpage, the CNSS "is responsible for

setting national-level cybersecurity policies, directives, instructions, operational

procedures, guidance and advisories for U.S. Government (USG) departments and

agencies for the security of National Security Systems (NSS) through the CNSS

Issuance System." (<https://www.cnss.gov/CNSS/about/about.cfm>, last accessed

February 1, 2024). That is consistent with my knowledge of CNSS and its role.

NIST documents, with which I am familiar and have used professionally, rely on

CNSS documents and definitions (see, e.g., the NIST glossary for "threat" found

here: <https://csrc.nist.gov/glossary/term/threat>, specifically referencing CNSS

definitions for "threat" separately and in various NIST documents). I have

personally used the NIST glossary to find NIST documents related to security

concepts and techniques.

14. Exhibit 2008 is a true and correct copy of excerpts from the book entitled *Threat Modeling* by Frank Swiderski and Window Snyder having a 2004 copyright date. I have a copy of *Threat Modeling*. *Threat Modeling* is available for purchase on Amazon.com. The U.S. Copyright Office's Public Catalog shows that this book has a Registration Date of June 6, 2004

Case IPR2023-00656
Patent 10,713,366
Supplemental Declaration of Seth James Nielson, Ph.D.

(<https://cocatalog.loc.gov/cgi-bin/Pwebrecon.cgi?v1=7&ti=1,7&Search%5FArg=threat%20modeling&Search%5FCode=TALL&CNT=25&PID=qdVtcB3UTyQBO6hWCo5RbEFOYn&SEQ=20240131151251&SID=1>, last accessed February 2, 2024).

15. Exhibit 2012 is a true and correct copy of the U.S. Copyright Office's record for *Threat Modeling* by Frank Swiderski and Window Snyder, 2004. This record shows a Registration Date of June 6, 2004.

16. There are many aspects to threat modeling. Threat modeling has many applications and can be conducted for a variety of purposes. Each of the articles, publications, and books making up Exhibits 2002-2008, and 2011 are documents that those of skill in the art, including a POSITA at the time of the invention of the '366 Patent, would reasonably consult and rely upon as part of their threat modeling analyses, as needed. From my perspective, the relevance of each of those exhibits as they relate to the present IPR is provided in my January 12, 2024 declaration and in this supplemental declaration. Mr. Hurlbut's December 18, 2023 deposition testimony also provides information showing that at least some of these exhibits are relevant to the issues in this IPR.

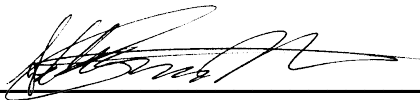
17. In signing this declaration, I recognize that the declaration will be filed as evidence in a case before the Patent Trial and Appeal Board of the United

States Patent and Trademark Office. I also recognize that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

18. I reserve the right to supplement my opinions and declarations in the future to respond to any arguments that the Petitioner may raise and to take into account new information as it becomes available to me.

19. I declare that all statements made herein of my knowledge are true, and that all statements made on information and belief are believed to be true, and that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Dated: February 5, 2024



Seth James Nielson, Ph.D.