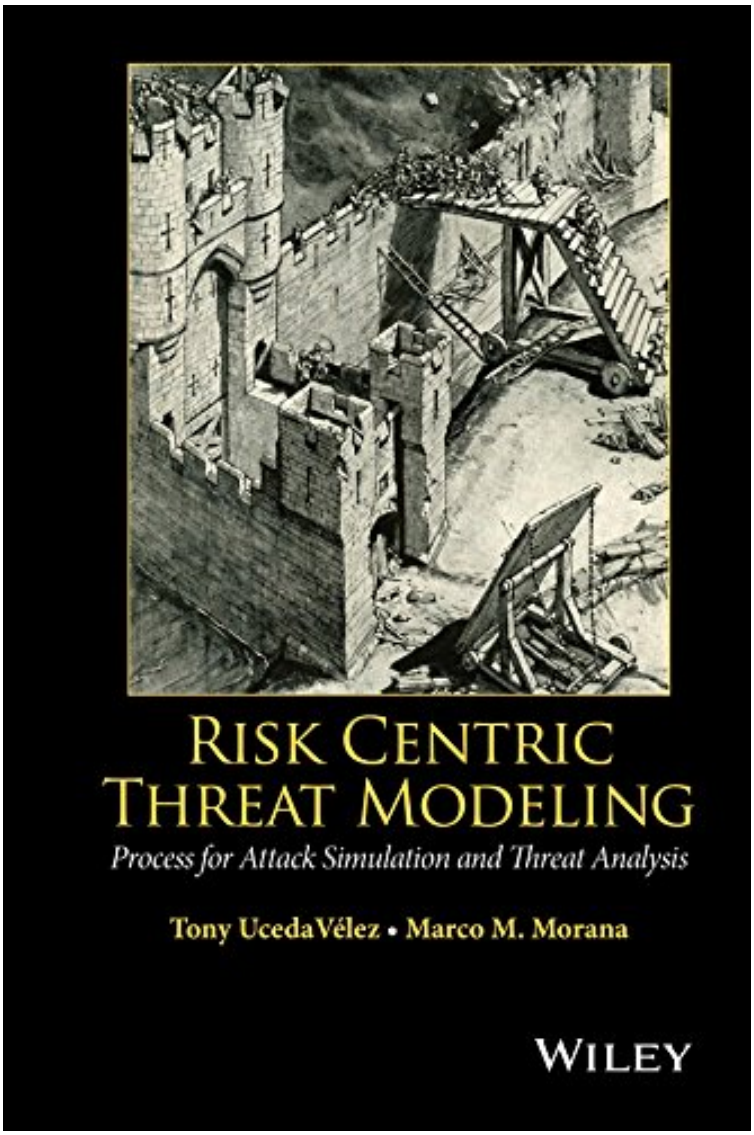
Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis

Tony UcedaVelez, Marco M. Morana
*ePub | *DOC | audiobook | ebooks | Download PDF*



#1025271 in eBooks 2015-05-12 2015-05-12File Name: B00XN46KTU | File size: 18.Mb

Tony UcedaVelez, Marco M. Morana : Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis before purchasing it in order to gage whether or not it would be worth my time, and all praised Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis:

1 of 1 people found the following review helpful. Lots of good info and a few areas for improvementBy Mark R LindseyThis book has lots of good info and I'd recommend it for someone working on protecting real systems against bad things happening. (As for somebody trying to check off a list to demonstrate compliance with security standards --

you probably want a different book.)But I offer four areas for improvement in the next edition:1. They're focused on threats with known, documented vulnerabilities. There's so much space spent on CVE and related documentation of software bugs, when hacks like the OPM happen in the absence of known software bugs. They need to expand the book to cover exploitless threats.2. From Chapter 3: "Many management officials do not see the business relevance on how exploitable software or permeable networks translate to an imminent business risk outside of simply not meeting a regulatory requirement." They're right, but they don't do much to help the situation. This approach focuses on *Use Cases* rather than *Abuse Cases*, and the methods tend to bury the easily-understood abuse risks like "Millions of bank account numbers could be stolen from Target Corp" behind "X% chance of exploitation of Y vulnerability could cause ID (Info Disclosure)".Besides these main points, this edition is dragged down by:3. Wordy, awkward prose; e.g., "Information correlated and/or aggregated from security operations will have to have some degree of topicality to the assessed application environment within the threat model." I think I know what they're trying to say...maybe "Security operations will influence the understanding of the application environment."4. Poor proofing; "Enurate" instead of "Enumerate". Diagram/artwork formats are all over the place: E.g., Figure 3.7 and Figure 8.1 show the same thing, using somewhat different color coding and slightly different terminology. Why? This is the job of the editors to polish this up.2 of 2 people found the following review helpful. Welcome addition for Threat Modeling guidanceBy Robert HurlbutThis is an excellent book for learning about Threat Modeling. In particular, it introduces the reader to the basic concepts of Threat Modeling in the first more-than-half part of the book and to the authors' 7-Step Threat Modeling process called PASTA (Process for Attack Simulation and Threat Analysis) in the latter part of the book.There are several things I liked about this book. One is its in-depth history, treatment and application of Threat Modeling to many scenarios, systems, and types of applications. The authors emphasize the importance of understanding the system, identifying the threats (the authors mostly use STRIDE), and then apply Risk Management to qualify the likelihood and consequences of the threats as well as suggest mitigations of those threats. One other benefit from the book is it points to one key aspects of PASTA in which you include attack simulation in your threat model. This provides a more comprehensive understanding (and "proof" if you will) of your model.A couple of negatives for me regarding the book, but by no means minimizing my recommendation, is the use of DREAD for determining risk and the density and length of the book. DREAD is no longer being used by Microsoft in their Threat Modeling process since 2009 (as also noted by the authors in this book). Instead, most threat modelers now use a simpler approach (High/Medium/Low based on probability of attack + business impact) or the more involved FAIR approach. But, regardless of choice of method, the authors' treatment of risk analysis AND threat modeling is excellent and welcome. This is a dense book with nearly 700 pages of small type (I bought and read a hardcover copy and took many notes) . At times I thought some ideas and concepts could have been expressed more succinctly. But I also thought it was worth the time and attention to read it through, and I wasn't disappointed. The book ends with a good example of applying PASTA to an eCommerce web application.I enjoyed reading this book when it came out last summer (2015) and I plan to reread it again this year in 2016. The book is one of a few Threat Modeling books I now recommend to my own clients in my Threat Modeling practice2 of 3 people found the following review helpful. The book is very well written and very easy to readBy Matthew HennesseyVery insightful. The book is very well written and very easy to read. I'm about a third way through and will update this review once I have completed the book.

This book introduces the Process for Attack Simulation Threat Analysis (PASTA) threat modeling methodology. It provides an introduction to various types of application threat modeling and introduces a risk-centric methodology aimed at applying security countermeasures that are commensurate to the possible impact that could be sustained from defined threat models, vulnerabilities, weaknesses, and attack patterns.nbsp;nbsp; This book describes how to apply application threat modeling as an advanced preventive form of security. The authors discuss the methodologies, tools, and case studies of successful application threat modeling techniques. Chapter 1 provides an overview of threat modeling, while Chapter 2 describes the objectives and benefits of threat modeling. Chapter 3 focuses on existing threat modeling approaches, and Chapter 4 discusses integrating threat modeling within the different types of Software Development Lifecycles (SDLCs). Threat modeling and risk management is the focus of Chapter 5.nbsp; Chapter 6 and Chapter 7 examine Process for Attack Simulation and Threat Analysis (PASTA). Finally, Chapter 8 shows how to use the PASTA risk-centric threat modeling process to analyze the risks of specific threat agents targeting web applications. This chapter focuses specifically on the web application assets that include customerrsquo;s confidential data and business critical functionality that the web application provides. bull; Provides a detailed walkthrough of the PASTA methodologynbsp;alongside software development activities, normally conducted via a standard SDLC process bull; Offers precise steps to take when combating threats to businesses bull; Examines real-life data breach incidents and lessons for risk management Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis is a resource for software developers, architects, technical risk managers, and seasoned security professionals.nbsp;

From the Back CoverThis book introduces the Process for Attack Simulation Threat Analysis (PASTA) threat

modeling methodology. It provides an introduction to various types of application threat modeling and introduces a risk-centric methodology aimed at applying security countermeasures that are commensurate to the possible impact that could be sustained from defined threat models, vulnerabilities, weaknesses, and attack patterns. nbsp; This book describes how to apply application threat modeling as an advanced preventive form of security. The authors discuss the methodologies, tools, and case studies of successful application threat modeling techniques. Chapter 1 provides an overview of threat modeling, while Chapter 2 describes the objectives and benefits of threat modeling. Chapter 3 focuses on existing threat modeling approaches, and Chapter 4 discusses integrating threat modeling within the different types of Software Development Lifecycles (SDLCs). Threat modeling and risk management is the focus of Chapter 5.nbsp; Chapter 6 and Chapter 7 examine Process for Attack Simulation and Threat Analysis (PASTA). Finally, Chapter 8 shows how to use the PASTA risk-centric threat modeling process to analyze the risks of specific threat agents targeting web applications. This chapter focuses specifically on the web application assets that include customerrsquo;s confidential data and business critical functionality that the web application provides. Provides a detailed walkthrough of the PASTA methodologynbsp;alongside software development activities, normally conducted via a standard SDLC process Offers precise steps to take when combating threats to businesses Examines real-life data breach incidents and lessons for risk management Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysisis a resource for software developers, architects, technical risk managers, and seasoned security professionals.nbsp; Tony UcedaVeacute;lez is CEO at VerSprite, an Atlanta based security services firm assisting global MNCs on various areas of cyber security, secure software development, threat modeling and security risk management. Tony has worked and led teams innbsp;the areas of application security, penetration testing, security architecture, and technical risk management for various organizations in Utility, Banking, Government, Retail, Healthcare, and Information Services. Marco M Morana serves as Senior Vice President-Application Security Architect for CitiGroup, where henbsp;is responsible for managing the architecture risk analysis and threat modeling program globally and leads global initiatives to mitigate risks of emerging cyber-threats targeting web applications of institutional clients. Marco hasnbsp;designed and developed business critical security software products for several Fortune 500 companies,nbsp;and also fornbsp;NASA. nbsp;nbsp;About the AuthorTony UcedaVeacute;lez is CEO at VerSprite, an Atlanta based security services firm assisting global MNCs on various areas of cyber security, secure software development, threat modeling and security risk management. Tony has worked and led teams innbsp;the areas of application security, penetration testing, security architecture, and technical risk management for various organizations in Utility, Banking, Government, Retail, Healthcare, and Information Services. Marco M Morana serves as Senior Vice President-Application Security Architect for CitiGroup, where henbsp;is responsible for managing the architecture risk analysis and threat modeling program globally and leads global initiatives to mitigate risks of emerging cyber-threats targeting web applications of institutional clients. Marco hasnbsp;designed and developed business critical security software products for several Fortune 500 companies,nbsp;and also fornbsp;NASA.nbsp;nbsp; nbsp;