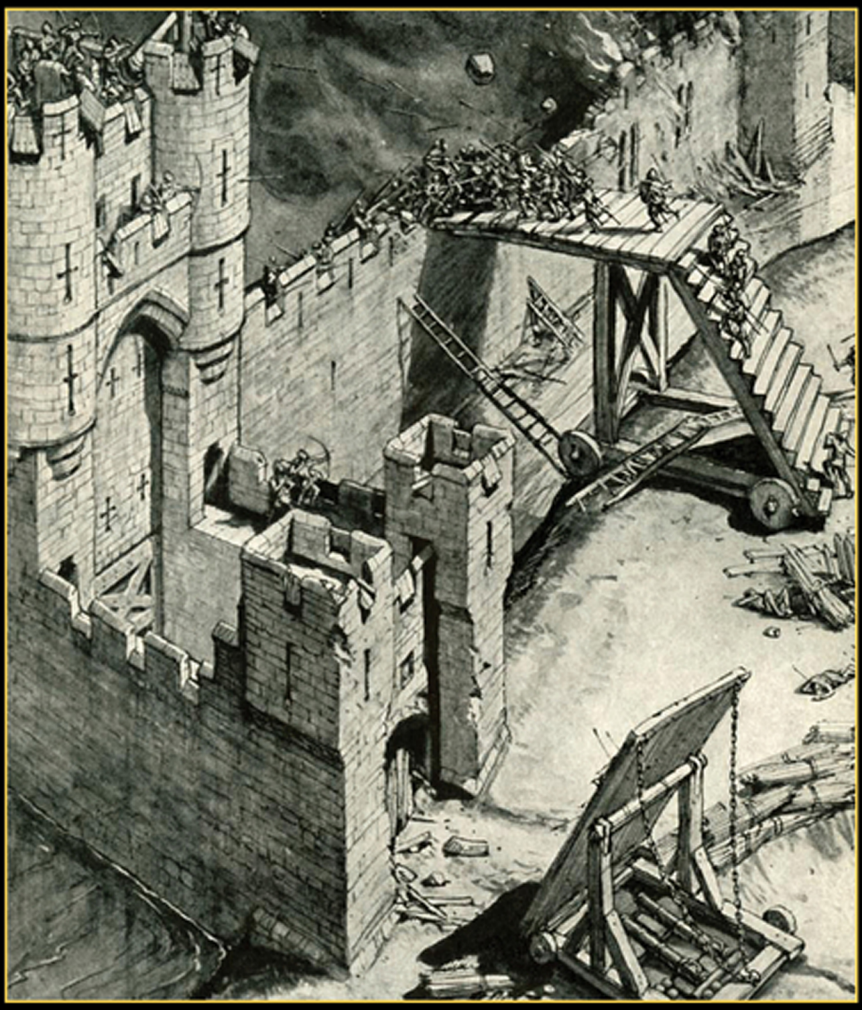

Risk Centric Threat Modeling

Process for Attack Simulation and Threat Analysis

Tony UcedaVélez • Marco M. Morana

WILEY

RISK CENTRIC THREAT MODELING

RISK CENTRIC THREAT MODELING

Process for Attack Simulation and Threat Analysis

TONY UCEDAVÉLEZ AND MARCO M. MORANA

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

Library of Congress Cataloging-in-Publication Data:

Tony UcedaVélez
Risk Centric Threat Modeling : process for attack simulation and threat analysis / Tony UcedaVélez, Marco M. Morana
pages cm
Summary: “This book describes how to apply application threat modeling as an advanced preventive form of security”– Provided by publisher.
Includes bibliographical references and index.
ISBN 978-0-470-50096-5 (hardback)
1. Data protection. 2. Computer security. 3. Management information systems–Security measures. 4. Computer networks–Security measures. 5. Risk assessment. I. UcedaVélez, Tony, 1976- II. Title.
HF5548.37.M67 2015
658.4′7011–dc23

2015000692

Cover Image: Courtesy of Fromold Books, http://www.fromoldbooks.org/
Typeset in 10pt/12pt TimesLTStd by SPi Global, Chennai, India

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

1 2015

To Suzanne, my patient and loving wife, who supported me throughout the five years of writing and research; thank you for your patience and endless support. –Marco

To Heidi, Simon, Serina, Sofia, Samson. For all the soccer balls I missed to kick in the backyard, the tea times I failed to sit in, and the date nights I couldn't make due to fulfilling this project, this is for you. Deo gratias. Deus lux Mea. –Tony

Special thanks to Sarah Varnell and Caitlyn Patterson (VerSprite) for all of their review, edits, and writing guidance.

CONTENTS

FOREWORD

The cover page of this book includes a drawing from George Kruger Gray's "The Siege of the Castle." The picture depicts castles under siege and illustrates the challenges to protect against the different attacks used in the Middle Ages such as siege equipment; mobile armored shelters, ladders, and wheeled ramps, by attackers trying to scale the walls built to protect the castles. This picture is a stark reminder of the challenges that cyber-security faces to defend from cyber-attacks of the modern era. In the Middle Ages, attackers stormed the castle from different positions, bypassing the defensive walls, and breaking into the main entry castle doors. In the modern era, attackers strike from the different data interfaces that are available, breaking into the applications user and data interfaces, attacking the firewalls, and application access controls. This picture is also a reminder that defenses such as castle walls, fortified gateways, towers, turrets, arrow loops, drawbridges, and moats become obsolete with the emergence of new threats. In the case of castle defenses, this was the increased presence of gunpowder weapons, such as cannons, in the fourteenth century. In the case of cyber-defenses, the emergence of sophisticated cyber-crime tools that can successfully bypass security defenses, such as anti-viruses, firewalls, and user authentication; require that we be vigilant, monitoring, and improving our defenses before they are rendered obsolete.

Today, businesses that conduct operations online (which is almost a requirement in order to remain consumer friendly) are targeted by motivated threat actors seeking to steal customer's personal and private data, and to obtain business's intellectual property for a competitive advantage. Small-medium businesses (SMB) have gone out of business as their bank accounts have been drained. Businesses that accept credit cards online or at Point of Sale (POS) machines, are the target of fraudsters and organized cyber-criminals. Bank customers who are accustomed to checking their

account balance and making payments and money transfers using online banking are the target of fraudsters armed with banking Trojans/malware. Once customers, personal and identifiable information is compromised, customers are notified by the bank of the breach, customer accounts are suspended, and the security incident has to be reported to the data privacy officer(s) and released to public in accordance to the data breach notification law enforced in the specific country. For most consumer customers, banks will take liability for the fraud being committed and repay their customers for losses, while commercial customers might face lawsuits from their clients when they refuse to pay for their losses. When business are found negligent of not applying the standard security controls and found noncompliant with information security standards, they are also impacted with additional fines and audits. Often businesses suffer large data breaches despite being compliant with technology security standards and conducting regular audits by qualified security auditors. This fact also challenges the assumption that adopting traditional security measures, processes, and technology, and compliance checks are enough to protect businesses from cyber-attacks. The assumption that security measures are "good enough" is often backed by evidence of successfully testing networks, systems, and application software for vulnerabilities, which is a factor in reducing the opportunity for an attacker to exploit them in targeted attacks.

Today, the risk mitigation effectiveness of the traditional approach of compliance driven security is challenged by the emergence of new cyber-threats and the fact that these threats have increased in sophistication and damage potential, which have rendered several security measures used today as obsolete. The adoption of sophisticated attack tools also referred to as cyber-crime toolkits for cyber-criminals and fraudsters as well as increased sophistication in the type of attack techniques, procedures, and tactics used are among the causes of an increased number of security breaches and the resulting increased economic losses felt by businesses. These cyber-crime tools are often freely available for attackers to download over the Internet and ready to be used for specific attacks against targets, such as Distributed Denial of Service (DDoS). Attacks tools can be purchased in the black market or rented for a fee such as in the case of malware and botnets. This increased availability of high-tech cyber-crime tools at very low cost severely increases the risks that businesses face when protecting customers data and company intellectual property from these attacks.

Due to this increased level of risk caused by emerging cyber-threats, businesses today cannot base their security on compliance and evidence of assurance followed by traditional information security standards and processes. Chances are that several business today that have audited for information security compliance with ISO 27001, PCI-DSS and have traditional security measures in place can still be targeted by cyber-attacks and experience losses of confidential data and fraud. Public and private organizations whose services and business depend on the web to generate a significant part of their revenues cannot look at compliance alone for security, but also need to consider a risk management approach that is based upon threat analysis, attack modeling, and simulations. This multifaceted risk management approach will reveal the level of resilience to targeted attacks and aid in determining the necessary countermeasures for reducing the risks to a manageable level. In addition,

the analysis of threat actors, the modeling of attacks, and the execution of threat driven tests cannot be restricted to security practitioners but needs the collaboration of the application stakeholders that include information security officers, application architects, software developers, application architects, security testers, and business owners. Engineering systems and software that are resilient enough to withstand the impact of cyber-attacks is necessary, and requires organizations and businesses to adopt new processes such as risk-based threat modeling.

Many of the cyber-attacks occurring against web applications today are facilitated by exploitation of design flaws and security bugs in the applications, such vulnerabilities that are introduced because of coding errors in the software components. For this reason, a focus on identifying design flaws using threat modeling is critical and this is best done during the software engineering life cycles. Threat modeling is an activity that can be executed during the early stages of the Software Development Life Cycle (SDLC) to identify and remediate design flaws prior to coding and prior to security testing. The adoption of threat modeling in the SDLC is risk effective in building attack resilient software as well as cost effective, since it allows for identifying design issues as early as possible and provides time to make changes to the design before the application product is built. Today, there is a need to adopt a risk-based threat modeling process to engineer business critical web applications and software. For example, consider software that is used for credit card processing, software that is used in critical industrial systems, such as SCADA, and runs oil, gas, water, and electric utilities; manufacturing controls; traffic controls; and mission critical systems for the military. In the financial sector, this software is used to handle online banking, make payments, and trade stocks and bonds. A little bit closer to our everyday experience as consumers, consider software used for mobile payments and for online purchases, which processes and stores credit card information and other personal data.

The main question for security practitioners and risk managers today is how businesses can design and implement applications and products that are engineered to withstand cyber-attacks and yet be cost effective to build. This is the call for security practitioners to look at engineering software from the perspective of a risk manager, to understand the threats and types of attacks and be able to identify solutions that are cost effective, yet still able to mitigate the impact of attacks. There is also a call for "cyber-threat application security and software awareness" since businesses and organizations still focus on protecting the network infrastructure and the perimeter, and overlook how web and mobile applications are built and how they securely store and process sensitive customer and corporate data. Today it seems that there is disconnect among the information security practitioners and risk managers between the escalation of emerging cyber-threats and the effectiveness of the countermeasures implemented. This disconnect can be bridged by the adoption of new approaches, such as risk-based threat modeling. For threats that specifically target applications and enterprise software, it is important to build countermeasures into products during the software development life cycle, rather than bolt on security at the end. In order to understand how these attacks can be prevented and detected, the identification of countermeasures to mitigate threats needs to be driven by threat analysis and

modeling of the attacks. For awareness sake, when making the case of software security to executive management, you can make parallels between the software industry and the car industry. "If applications today were built as resilient to cyber security attacks as cars are built resilient to car accidents, we would have software that is built with security controls equivalent to that of the car air bag. The car still needs to be repaired, but the consumer, the data, is protected."

Traditionally, threat modeling as methodology has been advocated by software security consultants to model threats to software and to identify design flaws that could be remediated during the SDLC. Examples of these thereat modeling methodologies include Microsoft Threat Modeling that is based on categorizing threats as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges). Software developers can use MS STRIDE methodology to design software with countermeasures for these threats such as data and channel encryption, digital signatures/hashes, mutual authentication, authentication, and authorization. This is certainly a good start, but it is not enough to design applications that can withstand sophisticated threats, such as one used today against business-critical software and web applications, the designs must be implemented. Consider the example of a threat that exploits the business logic of an application, such as a financial application that uses credit card data to validate the identity of a customer to conduct a specific financial transaction. An attacker can abuse this functionality to enumerate which credit card numbers previously stolen are valid so that they can be used for online purchases or counterfeit credit cards. This type of threat exploits abuse of functionality and logic flaws, and can be analyzed for specific threat actors and specific attacks using methods such as "use and abuse cases." This type of threat can also create a set of attack vectors and attack-driven test cases that are based upon this dynamic type of analysis, not a static assumption of threats. Another important reason for a risk-based threat modeling is the modeling of attacks to derive a set of tests that can be used to emulate the attack, and identify the presence of vulnerabilities and design flaws that need to be remediated. This modeling of attack starts by considering the product surface that is the available point of attacks for a threat actor such as the data interfaces and data channels. An attacker will seek to compromise the application by identifying the path of least resistance, exploring different channels that lead to the data assets, such as online, mobile, B2B channels, and in the cloud where data is either stored or processed.

A threat model can be used to emulate a real attack and test critical application functionality and software. To be realistic, the threat model needs to imitate the threat actors, tools, and attack techniques used, in order to derive a set of test cases that can be used by security testers to test the application resilience. This book advocates the use of risk based threat modeling, which is the analysis of threats and modeling of attacks in the context of information security and management of application and software as business assets. The main drive for the adoption of risk centered threat modeling is that using threat analysis and attack modeling allows risk managers to focus on the emerging threats to determine which countermeasures are most effective in mitigating these threats. Such a risk-based threat modeling process "bakes in"

all the essential ingredients of compliance; threat analysis, business impact analysis, software security, and risk management; and can be proven in the field by application security practitioners and risk managers.

Though there is not a silver bullet or a single solution for the complexities of software development, the authors offer a new application threat-modeling methodology, the "Process for Attack Simulation and Threat Analysis" (PASTA), which is documented in this book. PASTA is a risk-centered threat-modeling process that focuses on understanding first and foremost the business context and inherent risk profile of the application that needs to be secured. Secondly, PASTA factors threats and attacks and risk managers in designing web and mobile applications that are resilient to the emerging cyber-threats. As application security is a journey and not a destination, I also hope that the risk-based threat modeling methodology documented in this book will be useful as one of the ways to mitigate risks of the numerous emerging threats targeting your web applications and software.

HON. HOWARD A. SCHMIDT

PREFACE

> "The Senate determined to bring eight legions into the field, which had never been done at Rome before, each legion consisting of five thousand men besides allies. … Most of their wars are decided by one consul and two legions, with their quota of allies; and they rarely employ all four at one time and on one service. But on this occasion, so great was the alarm and terror of what would happen, they resolved to bring not only four but eight legions into the field."
>
> *Polybius, The Histories of Polybius*

Battle of Cannae in 216 BC [1] when Hannibal employed defense in depth in order to encircle and destroy 10 Roman Legions all at once, resulting in the largest single slaughter of Roman troops in the history of the republic. Edward Luttwak used the term to describe his theory of the defensive strategy employed by the Late Roman army in the third and fourth centuries AD.

This book introduces the Process for Attack Simulation and Threat Analysis (PASTA) threat modeling methodology, an asset, or risk-centric approach. Its purpose is to provide a framework for risk mitigation based upon viable threat patterns against various types of threats. This book was written to usher in a new approach on threat analysis and risk mitigation. Both the methodology and the book have been inspired by more than 50 years of collective IT and Information Security experience where lackluster risk management measures and predictable security testing has yielded bloated and ineffective responses to instill organic security controls. The PASTA methodology is for both IT and Security professionals alike who recognize that there is no such thing as a "risk-free" utopia. The methodology appeals to IT, Security, Compliance, and Risk leaders who want to mitigate the residual risks that

matter and understand the causal threat factors that make them relevant in the first place.

This book intends to illustrate how the impact, attributed to threat scenarios, has never been properly addressed. It shares the status quo problem of risk today and how risk management today is simply the shuffling of best guesses and control gaps that do not speak to the heart of the risk equation. While there are many threat modeling methodologies, PASTA presents a step-by-step, risk-centric threat modeling approach that is centered around understanding business impact, focused on threat research, and concerned about countermeasures that truly demonstrate risk reduction. PASTA is an iterative, maturing process that can be measured and aligned to several different frameworks and existing best practices. Its design centers on the understanding that threat motives and targeted attacks are truly unpredictable and require a more sophisticated method for identifying their possible target assets. PASTA is supported by a logical consideration around attack patterns, and considers the multiple ways in which threat successes can be achieved across a myriad of targeted exploits. With this broad understanding, PASTA aims to provide a linear approach to attack simulation while considering impact levels attributed to compromised data, infrastructure, and even reputation.

From CISOs to Security Engineers, this book provides a wrapper to enterprise security processes that work together under the framework of PASTA. We hope you may consider a risk-centric approach to threat modeling as your next evolution to targeted threat analysis and response.

REFERENCE

1. Polybius, Friedric Otto Hultsch (1889). The Histories of Polybius, Vol. 1, Macmillan and Company.

LIST OF FIGURES

LIST OF TABLES

1

THREAT MODELING OVERVIEW

DEFINITIONS

> [Application] Threat Modeling – *a **strategic process** aimed at considering possible **attack** scenarios and **vulnerabilities** within a proposed or existing **application environment** for the purpose of clearly identifying **risk** and **impact** levels.*

Definitions for any type of terminology are necessary evils. While seemingly elementary and potentially annoying, they provide a common ground from which to build. Providing a well-constructed definition also level-sets threat modeling's intended design as a process-oriented control for application security, versus interpretations that mutate its intent and true capability.

In this book, the expression "threat modeling" is reserved for software development and application security efforts. Within the topical boundaries of application security, the aforementioned definition provides some fundamental terms that should resonate with anyone who understands the very nature of security risk management and has implemented the threat modeling machine.

A closer examination of the definition provided reveals greater insights into the essential components that are threat modeling. The first emphasized term, *strategic*, describes a quality of threat modeling reflected in its ability to anticipate threats via

Risk Centric Threat Modeling: Process for Attack Simulation and Threat Analysis, First Edition.
Tony UcedaVélez and Marco M. Morana.

calculated and simulated attack patterns. Each major function within the threat modeling process requires a great deal of consideration and anticipation of multiple risk factors influenced by threat, vulnerability, and impact levels.

Process is one of threat modeling's key, distinguishing qualities. A chain-like reaction of tactical events is conducted across multiple domains (business objectives, system/database administration, vulnerability management, etc.) where additional review, input, and contribution is provided by other stakeholders within the process – all in relation to a protected application environment. To date, the lack of process within information security efforts has accounted for several shortcomings in mitigating security risks introduced by deficiencies in application security, and in many cases acted as causal factors to those noted deficiencies. Although there are isolated victories in traditional security efforts, a growing sentiment is that the war against software exploitation is being lost. Threat modeling is intended to greatly revitalize the effort in securing data via a collaborative, strategic process.

The next term, *attack*, reflects a major science to threat modeling – the discipline of researching how attack patterns can potentially exploit software vulnerabilities and/or poorly designed countermeasures. The hierarchy of an attack becomes dissected via threat modeling techniques, exposing faults in application design and/or software development, as well as other practical yet key areas, such as unveiling plausible motives for which an attacker initially sought to launch their assault.

Vulnerabilities is a term used far more prevalently within other information security efforts. In the scope of threat modeling, however, its use extends the manner in which software vulnerabilities are understood. Vulnerabilities at the platform and software levels are aggregated and correlated to possible attack scenarios. As a result, this term is an essential component to its definition, as we will see in later chapters.

The *application environment* expression serves as the object of the threat modeling process. Other traditional security procedures simply address a single aspect of an entire application environment, thereby negating a more holistic approach to application security. This is not to state that these more isolated procedures are not important, but rather that the sum of their individual benefits is encompassed in the process of threat modeling and applied to the entire application environment.

The term *risk* serves as the object of key interest to threat modeling. Threat modeling, as a supportive role in fulfilling business objectives, seeks to identify risks associated with the cumulative effects of an ever-evolving threat environment, compounded by software/network vulnerabilities, and fueled by attack motives or interest in business information – all managed and/or driven by an application environment. Threat modeling provides greater precision in conveying risk through providing a clear path on how a business application environment could be compromised and the probability of the actual risk. In essence, risk becomes the common glue that unifies security and business professionals in a collaborative effort to protect the enterprise.

Within the threat modeling definition, *impact* is the ability to answer the question "How bad is it?" Unless security professionals consider all possible threat scenarios in order to generate a prioritized, risk-based analysis, they cannot provide an effective and credible answer. As answers morph into speculations and continue downhill, security professionals are again unable to convey an adequate and plausible answer