Code Mash 2020 – Pre-Compiler
Hands On Threat Modeling Workshop
January 7, 2020 – 8:00 am to 12:00 pm EST

Introduction

Threat Modeling is a way of thinking about what could go wrong and how to prevent it or manage the risk. Instinctively, we all think this way in regards to our own personal security and safety. When it comes to building software, some software shops either skip the important step of threat modeling in secure software design or, they have tried threat modeling before but haven't quite figured out how to connect the threat models to real world software development and its priorities. Threat Modeling should be part of your secure software design process. Using threat modeling and some principles of risk management, you can design software in a way that makes security one of the top goals, along with performance, scalability, reliability, and maintenance.

Threat Modeling (also known sometimes as Architecture Risk Analysis) is the primary security analysis task performed during the software design stage. It is a structured activity for identifying and evaluating application threats and related design flaws. You use the identified flaws to adapt your design, or scope your security testing.

Threat Modeling allows you to consider, identify, and discuss the security implications of user stories in a structured fashion, and in the context of their planned operational environment. This "crash course" workshop will teach you to perform Threat Modeling through a series of exercises, where the instructor will guide you through the different stages of a practical threat model based on a migration from a "classical" web application to a combination of cloud-based hosted microservices.

Objective

In this workshop, attendees will be introduced to Threat Modeling, learn how to conduct a Threat Modeling session, learn how to use practical strategies in finding threats, learn how to find realistic Countermeasures, and learn how to apply Risk Management in dealing with the threats. This is a hands-on workshop. We will use whiteboards, Threat Modeling card games, look at some of the available Threat Modeling tools - all in order to get familiar with the latest approaches in Threat Modeling.

Exercises are built upon a fictional company, where we migrate a legacy client-server system towards a cloud based, microservices stack.

What you'll learn and how you can apply it

By the end of this hands-on workshop, you'll understand:

- Where Threat Modeling fits in a secure development lifecycle
- Benefits of Threat Modeling

- Different stages of Threat Modeling
- The STRIDE model for identifying threats (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege)
- Secure design mitigations
- Risk rating

And you'll be able to:

- Create and update your own threat models with an incremental technique
- Identify design flaws in your software
- Use Threat Modeling as an awareness tool for your team and stakeholders
- Get your team on the same page with a shared vision on security

This workshop is for you because ...

- You're an application security champion, software architect, or IT security specialist
- You work with development and DevOps teams to increase software assurance and resilience
- You're a software developer who wants to understand how to apply secure design techniques to your work

Pre-requisites:

- Familiarity with core principles of software engineering, software security, microservices, and cloud architectures.

Recommended preparation:

- Installation of Microsoft Threat Modeling Tool v7.1.x (TMT 2016 would also work) on a Windows OS (7/10) (https://aka.ms/threatmodelingtool or https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-releases)
- Alternatively, you could use OWASP Threat Dragon (https://threatdragon.org/) or draw.io (see https://github.com/michenriksen/drawio-threatmodeling) on Mac/Linux/Windows

Additional Resources

- Read Threat Modeling: Designing for Security (book)
- Read Securing Systems: Applied Security Architecture and Threat Models (book)
- Read Agile Application Security: Enabling Security in a Continuous Delivery Pipeline (book)
- Read Threat Modeling: Risk Identification and Avoidance in Secure Design (book) – *due Spring, 2020*

Instructor

Robert Hurlbut is a Threat Modeling Architect at Bank of America, a Microsoft MVP for Developer Technologies and Security, and holds the (ISC)2 CSSLP security certification. Robert has 30 years of industry experience in software security, software architecture, and software development. He has served as a project manager, director of software development, and chief software architect for several projects. He speaks at user groups, national and international conferences, and has provided training for many companies.

Robert also co-hosts with Chris Romeo the Application Security Podcast at https://www.securityjourney.com/application-security-podcast/.

Schedule

Overview (30 minutes)

- Introductions
- What is Threat Modeling?

Getting Started (1 hr 30 mins)

- Threat Modeling Process
- Hands-On Exercises with Whiteboards (1hr 30 mins)

Break (5 mins)

Using Tools (1 hr 25 mins)

- Threat Modeling Tools and Card Games
- Hands-On Exercises with Tools and Card Games

What's next? (30 mins)