CENTER FOR CYBER SECURITY TRAINING

Hands-On Threat Modeling

Abstract

Threat modeling is the primary security analysis task performed during the software design stage. Threat modeling is a structured activity for identifying and evaluating application threats and vulnerabilities. The security objectives, threats, and attacks modeling activities during the threat modeling are designed to help you find vulnerabilities in your application and the supporting architecture. You can use the identified vulnerabilities to help shape your design and direct and scope your security testing.

Threat modeling allows you to consider, document, and discuss the security implications of designs in the context of their planned operational environment and in a structured fashion. It also allows consideration of security issues at the component or application level. The threat modeling course will teach you to perform threat modeling through a series of workshops, where our trainer will guide you through the different stages of a practical threat model.

Learning Objectives

Students will be challenged in groups of 3 to 4 people to perform the different stages of threat modeling on the following:

- B2B web and mobile applications, sharing the same REST backend
- An Internet of Things (IoT) deployment with an on-premise gateway and a cloud-based update service
- OAuth scenarios for an HR application
- Privacy of a new face recognition system in an airport
- Get into the defenders' head – modeling points of attack against a nuclear facility

- Agile threat modeling, 3 sprints to migrate a legacy application to AWS while building an attack library for the CI/CD pipeline
- The nuts" poker tournament – create a threat model for an online poker tournament

Target Audience

Software developers, architects, system managers or security professionals

Course Outline

Threat modeling introduction

- Threat modeling in a secure development lifecycle
- What is threat modeling?
- Why perform threat modeling?
- Threat modeling stages
- Different threat modeling methodologies
- Document a threat model

Diagrams – what are you building?

- Understanding context
- Doomsday scenarios
- Data flow diagrams
- Trust boundaries
- Sequence and state diagrams
- Advanced diagrams
- Hands-on: diagram B2B web and mobile applications, sharing the same REST backend

Identifying threats – what can go wrong?

- STRIDE introduction
- Spoofing threats
- Tampering threats
- Repudiation threats
- Information disclosure threats
- Denial of service threats

- Elevation of privilege threats
- Attack trees
- Attack libraries
- Hands-on: STRIDE analysis of an Internet of Things (IoT) deployment with an on premise gateway and secure update service

Addressing each threat

- Mitigation patterns
- Authentication: mitigating spoofing
- Integrity: mitigating tampering
- Non-repudiation: mitigating repudiation
- Confidentiality: mitigating information disclosure
- Availability: mitigating denial of service
- Authorization: mitigating elevation of privilege
- Specialist mitigations
- Hands-on: threat mitigations OAuth scenarios for web and mobile applications

Privacy threat modeling

- GDPR
- Privacy by design
- Privacy impact assessment (PIA)
- Privacy threats
- LINDDUN
- Mitigating privacy threats
- Hands-on: privacy threat modeling of a face recognition system in an airport

Threat modeling for agile and DevOps

- Iterative and incremental threat modeling
- Updating threat models
- Threat modeling as code
- pytm: A Pythonic framework for threat modeling
- OWASP Threat Modeling Playbook (OTMP)
- Hands-on:

- Sprint 1: Threat identification migrating the booking system application to AWS
- Sprint 2: AWS threat mitigations for the booking system build on microservices
- Sprint 3: Building an attack library for CI/CD pipelines

Advanced threat modeling

- Typical steps and variations
- Validation threat models
- Effective threat model workshops
- Soft skills for threat modelers
- Offensive threat modeling, threat modeling for penetration testers
- Communicating threat models
- Hands-on: The nuts" tournament – create a threat model for an online poker tournament

Threat modeling tooling and resources

- Open-Source tools
- Commercial tools
- General tools
- Threat modeling tools compared
- Threat models examples: automotive, industrial control systems, IoT and Cloud
- Hands-on: Microsoft Threat Modeling Tool

Examination

- Hands-on examination
- Grading and certification

Students' Knowledge Pre-Requisites:

Before attending this course, students should be familiar with basic knowledge of web and mobile Applications, databases & Single sign on (SSO) principles