Advanced Whiteboard hacking – aka hands-on Threat Modelling

Training Course

30th & 31st of October

Table of Contents

All training courses are two full days of intensive, hands-on learning and include complimentary morning tea, lunch and afternoon tea. Tickets can be secured buy going to the website https://appsecday.io/.

Course Abstract

As skilled and experienced professionals we know that there is a gap between academic knowledge of threat modelling and the real world.

To close that gap, we developed practical use cases, based on real-world projects. Each use case includes a description of the environment, together with questions and templates to build a threat model. Using this methodology, we provide our students with the best training possible and the templates to incorporate threat modelling best practices in their daily work. Students will be challenged in groups of 3 to 4 people to perform the different stages of threat modelling on:

- B2B web and mobile applications, sharing the same REST backend
- An IoT deployment with a 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, attacking a nuclear facility

What attendees will learn?

Threat modelling is a crucial technique to assure more secure software and systems. This training will provide our students with the know-how, templates and exercises to start threat modelling themselves. Key takeaways are:

- becoming a better (security) professional
- understanding the process and technique of threat modelling
- knowing when and how to introduce and improve threat modelling

What attendees should bring?

Students should bring their own laptop or tablet to read and use the training handouts and exercise descriptions.

Pre-requisites

Students should be familiar with basic knowledge of web and mobile applications, databases & Single sign on (SSO) principles.

Detailed Outline

Day 1

Threat modelling introduction

- Threat modelling in a secure development lifecycle
- What is threat modelling?
- Why perform threat modelling?
- Threat modelling stages
- Different threat modelling 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
-

Day 2

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 modelling

- GDPR
- Privacy by design
- Privacy impact assessment (PIA)
- Privacy threats
- LINDUNN
- Mitigating privacy threats

- Hands-on: privacy threat modelling of a face recognition system in an airport

Penetration testing based on offensive threat models

- Create pentest cases for threat mitigation features
- Pentest planning to exploit security design flaws
- Vulnerabilities as input to plan and scope security testing
- Prioritization of pentesting based on risk rating
- Hands-on: get into the defenders' head – modelling points of attack of a nuclear facility.

Advanced threat modelling

- Typical steps and variations
- Validation threat models
- Effective threat model workshops
- Communicating threat models
- Updating threat models
- Threat models examples: automotive, industrial control systems, IoT and Cloud

Threat modelling resources

- Open-Source tools
- Commercial tools
- General tools
- Threat modelling tools compared

Examination

- Hands-on examination
- Grading and certification

Trainer Biography

https://www.linkedin.com/in/steven-wierckx

Steven Wierckx is a consultant at Toreon. A software and security tester with 15 years of experience in programming, security testing, source code review, test automation, functional and technical analysis, development, and database design, Steven shares his passion for web application security through writing and training on testing software for security problems, secure coding, security awareness, security testing, and threat modeling. He is the project leader for the OWASP Threat Modeling Project and organizes the BruCON student CTF. This year, he spoke at Hack in the Box Amsterdam, hosted a workshop at BruCON and delivered threat modeling trainings at OWASP AppSec USA and O'Reilly Security New York.