TOREON

Training – Whiteboard Hacking aka Hands-on Threat Modeling

Toreon CVBA
Grotehondstraat 44 1/1, B-2018 Antwerpen, Belgium | T +32 33 69 33 96
VAT BE0542.795.568 info@toreon.com | www.toreon.com

Table of contents

Revision control

Version	Date	Author	Comments
1.0	10-Feb-17	Sebastien Deleersnyder	Syllabus

Whiteboard hacking – aka hands-on Threat Modeling

As highly skilled professionals with years of experience under our belts we know that there is a gap between academic knowledge of threat modeling and the real world.

In order to minimize that gap we have developed practical Use Cases, based on real life projects. Each use case includes a description of the environment, together with questions and templates to build a threat model. Using this methodology for the hands on workshops we provide our students with a robust training experience and the templates to incorporate threat modeling best practices in their daily work.

The students will be challenged to perform practical threat modeling in groups of 3 to 4 people covering the different stages of threat modeling on:

- A hotel booking web and mobile application, sharing the same REST backend
- An Internet of Things (IoT) deployment with an on premise gateway and secure update service
- An HR services OAuth scenario for mobile and web applications

This edition also introduces a new section on privacy threats and privacy by design, including a hands-on privacy impact assessment of a face recognition system in an airport. Each student will receive a hard copy of the book: Threat Modeling, designing for security by Adam Shostack (2014, Wiley)

Trainer: Sebastien Deleersnyder will share his practical threat modeling experience. He specializes in Application Security, combining both his software development and information security experience. Sebastien has led and performed engagements in the domain of ICT-security, Web and Mobile Security with customers in the last 15 years. Sebastien has performed several successful secure development lifecycle projects in the financial and utility sector, started up software security groups, supported customers in selecting and implementing Web Application Firewalls (WAF), delivered web application security training and closed a lot of audit findings regarding application security :-).

Sebastien started the Belgian OWASP Chapter Leader, was a member of the OWASP Foundation Board and performed several public presentations on Web Application and Web Services Security. He also co-founded the yearly security & hacker BruCON conference and trainings in Belgium. Sebastien has achieved CISSP, CISM, CISA and Prince2 Practitioners certifications. Specialties: Application Security, Secure Development Lifecycle, ICT security product management, Business Development and Security Project Management

Hands-on Threat Modeling course

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.

This course is aimed at software developers, architects, system managers or security professionals. Before attending this course, students should be familiar with basic knowledge of web and mobile Applications, databases & Single sign on (SSO) principles. The students should bring their own laptop to the course.

Course topics

Threat modeling introduction

- Threat modeling in a secure development lifecycle
- What is threat modeling?
- Why perform threat modeling?
- Threat modeling stages
- Diagrams
- Identify threats
- Addressing threats
- Document a threat model

Diagrams – what are you building?

- Understanding context
- Doomsday scenarios
- Data flow diagrams
- Trust Boundaries
- **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
- **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
- **Hands-on: threat mitigations OAuth scenarios for web and mobile applications**

Privacy by design

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

Attack libraries

- Attack libraries
- CAPEC
- OWASP Top 10
- Other lists
- Create your own checklist
- **Hands-on: map OWASP T10 to STRIDE**

Practical threat modeling

- Typical steps
- Validation threat models
- Effective threat model workshops
- Communicating threat models
- Updating threat models

Threat modeling resources

- Open-Source tools
- Commercial tools
- General tools

Examination

- Hands-on examination
- Grading and certification

Student package:

The course students receive the following package as part of the course:

- Each student will receive a hard copy of the book: Threat Modeling, designing for security by Adam Shostack (2014, Wiley)
- Hand-outs of the presentations
- Work sheets of the use cases,
- Detailed solution descriptions of the use cases
- Template to document a threat model
- Template to calculate risk levels of identified threats
- Receive certificate: Following a successful exam (passing grade defined at 70%) the student will receive certification for successful completion of course

Threat Modeling – Real Life Use Cases

As highly skilled professionals with years of experience under our belts we know that there is a gap between academic knowledge of threat modeling and the real world.

In order to minimize that gap we have developed practical Use Cases, based on real life projects. Each use case includes a description of the environment, together with questions and templates to build a threat model. Using this methodology for the hands on workshops we provide our students with a robust training experience and the templates to incorporate threat modeling best practices in their daily work.

The students will be challenged to perform the threat modeling in groups of 3 to 4 people performing the different stages of threat modeling on:

- B2B web and mobile applications, sharing the same REST backend
- An Internet of Things (IoT) deployment with an on premise gateway and secure update service
- OAuth scenarios for mobile and web applications
- Privacy impact assessment of a face recognition system in an airport

After each hands-on workshop, the results are discussed, and the students receive a documented solution.

Training prerequisites

Important pre-requisites for the training room are:

- Internet access for the trainer and the students
- Projector
- White board
- One flip chart per 4 students
- Room setup in groups of 4 students
- Power adapters

The students should bring their own laptop or have a training PC available.

About Toreon

At Toreon, we believe that ***security is vital*** for people to live and work confidently and with trust in our digital society.

We are ICT security consultants. We help you to leverage your information technology and achieve your organisation's goals. While you run your business, we keep track of the information risks that your organisation faces and we help you to only take actions that fit your risk appetite.

Toreon is an ***independent partner*** you can trust. We act as trusted advisors for our clients. We accompany you and help to make informed decisions about ICT. We help to optimize your choices so that you can have peace of mind.

We work differently. For every engagement, we mobilize a ***team of experts***. This always brings solid experience and expertise to the task at hand. It benefits our clients to always get the right person for the job.

Toreon is all ***about people***. We care about our employees and support their ambitions. We give them the opportunities to develop their skills and the freedom to evolve as a person and as a professional. Working in ever changing, multi-skill teams fosters knowledge sharing and personal development. This leads to well-functioning project teams that support our clients better.

We are experts in:

- CISO assistance & coaching
- Governance, risk and compliance
- Security architecture & design
- Cyber defence
- Application security
- Industrial security