TORESON

25-26 April – Ghent (Belgium)

Training – 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

Training - Public

Toreon proposes a 2 day, trainer-led, on-site, Threat Modeling course. The training material and hands-on workshops with real live use cases are provided by Toreon. 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:

- 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
- An OAuth scenario for mobile and web applications

Each student will receive a hard copy of the book: Threat Modeling, designing for security by Adam Shostack (2014, Wiley)

Toreon provides the experienced trainer Sebastien Deleersnyder to share his practical threat model experience. Sebastien led engagements in the domain of ICT-security, Web and Mobile Security with several customers including BNP Paribas Fortis, Atos Worldline, KBC, Nationale Nederlanden (ING), Isabel, Fluxys, OLAF, EU Council, TNT Post, Flemish Community, Agfa-Gevaert and ING Insurance International. Sebastien is the Belgian OWASP Chapter Leader, served as vice-chair of the global OWASP Foundation Board and performed several public presentations on Web Application, Mobile and Web Services Security. Furthermore, Sebastien co-founded the yearly BruCON conference.

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
- Privacy 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
- Mitigating privacy threats
- **Hands-on: Threat mitigations OAuth scenarios for web and mobile applications**

Attack libraries

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

Practical threat modeling

- Typical steps
- Validating threat models
- Organize effective threat model workshops
- Communicating threat models
- Updating threat models

Threat modeling resources

- Open-Source tools
- Commercial tools
- General resources

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

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

Training pricing

Early bird (before January 31st 2017):	€ 1,260.00
Normal(February 1st until March 31st):	€ 1,400.00
Late booking (as of April 1st):	€ 1,540.00

There is a minimum of 6 attendees for the training to take place.

All rates are exclusive of 21% VAT - Invoices payable before training participation.