MASTER OF SCIENCE IN ENGINEERING

Module Description, available in: EN

IT-Security

General Information

Number of ECTS Credits

3

Module code

TSM_ITSec

Valid for academic year

2023-24

Last modification

2019-10-09

Coordinator of the module

Stephan Neuhaus (ZHAW, stephan.neuhaus@zhaw.ch)

Explanations regarding the language definitions for each location:

- Instruction is given in the language defined below for each location/each time the module is held.
- Documentation is available in the languages defined below. Where documents are in several languages, the percentage distribution is shown (100% = all the documentation).
- The examination is available 100% in the languages shown for each location/each time it is held.

	Lausanne			Lugano	Zurich		
Instruction					**X** E 100%		
Documentation					**X** E 100%		
Examination					**X** E 100%		

Module Category

TSM Technical scientific module

Lessons

2 lecture periods and 1 tutorial period per week

Entry level competences

Prerequisites, previous knowledge

This module assumes that students have a working knowledge of basic security technologies such as cryptology, secure communication protocols, and access control mechanisms (which amounts to approx. a 4 ECTS bachelor module). See e.g.: William Stallings, Network Security Essentials: Applications and Standards. We also assume that students have a working knowledge in a general purpose programming language such as Java, C, or similar and are familiar with modern software development processes.

Brief course description of module objectives and content

This module teaches two aspects of IT security. The first part deals with secure software, focusing on developing secure software and exploiting defects in software. The second part deals with several advanced security technologies, which includes authentication, access control, network security devices, and operating system security.

Aims, content, methods

Learning objectives and acquired competencies

- The students know and understand the secure development lifecycle and are capable of developing secure software.
- The students can analyze software with respect to security and can exploit vulnerabilities.
- The students can employ threat modeling to identify threats and use this to define security requirements.
- The students know and understand advanced authentication and access control methods including identity federations.
- The students understand the underlying principles of application layer firewalls and intrusion detection/prevention systems.
- The students are able to apply the current network access control standards to establish trust in client platforms.

Contents of module with emphasis on teaching content

The module consists of 2 main topics, Software Security and Security Technologies. Each covers 6-8 weeks.

- Main topic 1: Software Security. The skills taught here are applicable to any software project and therefore include web applications, web services, and mobile applications.
    - Introduction to software security (motivation, secure development lifecycle)
    - Finding and exploiting vulnerabilities in software (e.g. web applications) by combining manual methods and tools
    - Developing secure software (e.g. web applications and web services)
    - Security requirements engineering and threat modeling
- Main topic 2: Security Technologies. The skills taught here are applicable to a wide range of scenarios, and include Internet and operating system security.
    - Advanced access control and authentication methods and federated identities
    - Application level firewalls and intrusion detection/prevention systems
    - Internet security, e.g., network access control
    - Operating system security and trusted platforms

Teaching and learning methods

- Lecture: Ex cathedra teaching
- Exercises/self-study: reading texts about security topics, some self-study, mainly about web application development frameworks; practical exercises (computer-based); theoretical exercises

Literature

Lecture slides, references to Internet sources and textbooks

Assessment

Certification requirements

Module does not use certification requirements

Basic principle for exams

As a rule, all the standard final exams for modules and also all resit exams are to be in written form

Standard final exam for a module and written resit exam

Kind of exam

written

Duration of exam

120 minutes

Permissible aids

No aids permitted

Special case: Resit exam as oral exam

Kind of exam

oral

Duration of exam

30 minutes

Permissible aids

No aids permitted