IT-Security

General Information

Number of ECTS Credits

3

Abbreviation

TSM_ITSec

Version

03.02.2016

Responsible of module

Marc Rennhard, ZHAW

Language

	Lausanne	Bern	Zürich
Instruction	☐ E ☐ F	☐ D ☐ E ☐ F	☐ D ☑ E
Documentation	☐ E ☐ F	☐ D ☐ E ☐ F	☐ D ☑ E
Examination	☐ E ☐ F	☐ D ☐ E ☐ F	☑ D ☑ E

Module category

☐ Fundamental theoretical principles

☑ Technical/scientific specialization module

☐ Context module

Lessons

☑ 2 lecture periods and 1 tutorial period per week

☐ 2 lecture periods per week

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
  - Introduction to software security (motivation, secure development lifecycle, secure design principles)
  - Finding and exploiting vulnerabilities in software (e.g. web applications) by combining manual methods and tools
  - Developing secure software (e.g. web applications)
  - Security requirements engineering and threat modeling
- Main topic 2: Security Technologies
  - Advanced access control and authentication methods and federated identities
  - Application level firewalls and intrusion detection/prevention systems
  - Network access control
  - Operating system security and trusted platforms

Teaching and Learning methods

- Lecture: Ex cathedra teaching
- Exercises/self-study: practical exercises (computer-based), theoretical exercises

Prerequisites, previous knowledge, entrance competencies

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, International Fifth Edition, 2013, Pearson Education Limited. 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.

Literature

Lecture slides, references to Internet sources and textbooks

Assessment

Certification requirements for final examinations (conditions for attestation)

Written module examination

Duration of exam:	120 minutes
Permissible aids:	Closed book, no written summary, no electronic devices