MASTER OF SCIENCE IN ENGINEERING

Module Description, available in: EN

Advanced Network Security

General Information

Number of ECTS Credits

3

Module code

TSM_AdvNetSec

Valid for academic year

2024-25

Last modification

2023-07-03

Coordinator of the module

Gürkan Gür (ZHAW, gueu@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

Profile Recommendations

This module is recommended for the following profiles:

	Zurich
Profile	ICS

Lessons

2 lecture periods and 1 tutorial period per week

Entry level competences

Prerequisites, previous knowledge

- Understanding of the TCP/IP protocol stack including routing protocols and DNS.
- Basic understanding of secure protocols such as WPA, IPSec and TLS.
- Basic understanding of network security appliances such as firewalls and proxies.

Brief course description of module objectives and content

This course aims to provide students with an in-depth understanding of current network security technologies and their application in solving technical security challenges. Upon completion of the course, students will be able to analyze, design and implement secure network infrastructures, using state-of-the-art security technologies and best practices. They will also develop an understanding of emerging network security techniques and solutions.

Aims, content, methods

Learning objectives and competencies to be acquired

The students

- are able to identify threats for a given network and are able to reason about the security properties of their networks.
- know important concepts of network security in the areas of DDoS protection, BGP security, DNS security, IPv6 security and HTTP/3.
- know the relevant key concepts to build secure network architectures and can develop a secure network architecture for different scenarios.
- are able to undertake an investigation into the course topics and report on their findings.

Module content with weighting of different components

This course is split into three parts:

Part 1: Network Threats and Monitoring
In Part 1 we talk about network threats and mitigation techniques as well as network monitoring. We cover topics such as common network attacks (e.g., Distributed Denial of Service(DDoS) attacks) as well as the challenges and solutions for monitoring network traffic (e.g., analysis of encrypted traffic flows).

Part 2: Network Protocols and Security
In Part 2 we focus on network protocols and security. This includes but is not limited to Border Gateway Protocol (BGP) security, Domain Name System (DNS) security, IPv6 security and HTTP/3.

Part 3: Securing Advanced Network Architectures
Part 3 covers several advanced approaches to securing network architectures from a forward-looking perspective. This includes but is not limited to topics such as Software Defined Networking (SDN), Network Function Virtualization (NFV), Zero Trust Architecture (ZTA), Machine Learning (ML) for network security, network security in containerized environments, and cloud network security.

As network security is a very dynamic and constantly evolving field, the course content will be adapted to current trends and emerging topics in network security.

Teaching and learning methods

Lectures with a mix of practical and theoretical exercises.

Literature

The following material is provided:

- Slides (with notes, where appropriate)
- Selected technical publications

Assessment

Certification requirements

Module does not use certification requirements

Basic principle for exams

As a rule, all standard final exams are conducted in written form. For resit exams, lecturers will communicate the exam format (written/oral) together with the exam schedule.

Standard final exam for a module and written resit exam

Kind of exam

Written exam

Duration of exam

120 minutes

Permissible aids

Aids permitted as specified below:

Permissible electronic aids

-

Other permissible aids

cheat sheet

Special case: Resit exam as oral exam

Kind of exam

Oral exam

Duration of exam

30 minutes

Permissible aids

Aids permitted as specified below:

Permissible electronic aids

-

Other permissible aids

cheat sheet