



## COURSE DESCRIPTION CARD - SYLLABUS

Course name

Side-channel attacks

### .Course

Field of study

Computing

Area of study (specialization)

Cybersecurity

Level of study

Second-cycle studies

Form of study

full-time

Year/semester

1/2

Profile of study

general academic

Course offered in

English

Requirements

elective

### Number of hours

Lecture

15

Tutorials

Laboratory classes

15

Projects/seminars

Other (e.g. online)

### Number of credit points

2

### .Lecturers

Responsible for the course/lecturer:

dr inż. Marek Michalski

marek.michalski@put.poznan.pl

tel: 61 665 39 06

Faculty of Computing and Telecommunications

Responsible for the course/lecturer:

### . Prerequisites

Student has basic knowledge about electronics, computer networks, programming and operational systems

Student can find proper source of information

Student can find and verify information from given sources

### Course objective

The goal is to provide to students knowledge about nature of system for information processing, mechanisms used for construction of this systems in terms of cybersecurity

Description of known attacks, their results, scopes and ways to prevent them on practical examples



### Course-related learning outcomes

#### Knowledge

Student knows mechanisms which are basis of functionality for described systems/devices

#### Skills

Student can analyze described mechanisms, understand their rules, can find and correct vulnerabilities

#### Social competences

Student knows that knowledge in cybersecurity has to be actual and extended continuously

### Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Written test, 51% to pass

### Programme content

Categorization of attacks and security breaches

Attack mechanisms (limited to Side Channel attacks)

Analysis of selected examples of devices

Who made a mistake, could it have been avoided, how to do it better

Physicality and programmability of devices

Scopes of SCA - common devices

SCA vulnerability areas - consumer devices

Ways of implementing the functionality of devices and security vulnerabilities

Vulnerabilities of networks (telecommunications, energy, banking, traction, various media)

Methods of analyzing devices and discovering their vulnerabilities

Automation of vulnerability analysis at the design, prototype and product stages

Consequences of backwards compatibility

Historical, legal and social conditions

Ways and tools to prevent SCA

Methods and tools of SCA susceptibility monitoring and detection

The lecture will include a meeting with professional device builders and a conversation on the analysis and safety of their products



## Lab

Become familiar with the laboratory pathform for the investigation and analysis of side channel attacks.

Operation on Linux, debugger of real sample systems,

Hardware analysis at the electrical level, use of software and hardware device analyzers

Radio band analysis

Measurements of real test devices

Designing safe devices, analysis of their security level

### Teaching methods

Lecture with students activities, discussions, presentations

Laboratory with demonstrations and live experiments

### Bibliography

Basic

Omar Santos, CCNP and CCIE Security Core SCOR 350-701 Official Cert Guide, Cisco Press, Hoboken, NJ, 2021

Additional

### Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,0
Classes requiring direct contact with the teacher	30	1,5
Student's own work (literature studies, preparation for laboratory classes/tutorials, preparation for tests/exam, project preparation) <sup>1</sup>	20	0,5

<sup>1</sup> delete or add other activities as appropriate