COURSE DESCRIPTION CARD - SYLLABUS

Course name
Side-channel Attacks [S2Inf1E-CYB>SCHA]

Course

Field of study
Computing

Year/Semester
1/2

Area of study (specialization)
Cybersecurity

Profile of study
general academic

Level of study
second-cycle

Course offered in
English

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
15

Laboratory classes
15

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

2,00

Coordinators

dr inż. Marek Michalski
marek.michalski@put.poznan.pl

Lecturers

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 sistem 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 stystems/devices

Skills:
student can analyze described mechanisms, understend their rules, can find and correct voulnerabilities

Social competences:

student knows that knowledge in cybersecurity has to be actual and extented continously

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Writen test, 51% to pass

Programme content

Categorization of attacks and security breaches (MITRE)
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
Power Analysis (Simple/Differential/Correlation)
Physicality and programmability of devices (FPGA)
Design for Testing (DFT)
Scopes of SCA - common devices
Hardware Trojans
Logic locking, obfuscations, IP Piracy
SCA vulnerability areas - consumer devices (XBOX, ZYNQ,STARLINK)
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
Power analysis
Glitching + fault injection
Radio band analysis
Measurements of real test devices
Designing safe devices, analysis of their security level

Course topics

Categorization of attacks and security breaches (MITRE)
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
Power Analysis (Simple/Differential/Correlation)
Physicality and programmability of devices (FPGA)
Design for Testing (DFT)
Scopes of SCA - common devices
Hardware Trojans
Logic locking, obfuscations, IP Piracy
SCA vulnerability areas - consumer devices (XBOX, ZYNQ,STARLINK)
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
Power analysis
Glitching + fault injection
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
Side-Channel Analysis of Embedded Systems; Maamar Ouladj. Sylvain Guilley Springer 2021 (open access)

Power Analysis attacks; Mangard, Oswald, Popp, Springer 2007 (open access)

Introduction to Hardware Security and Trust; Mohammad Tehranipoor • Cliff Wang Springer 2012 (Open access)
Additional

Breakdown of average student's workload

	Hours	ECTS
Total workload	50	2,00
Classes requiring direct contact with the teacher	30	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	20	0,50