COURSE DESCRIPTION CARD - SYLLABUS

Course name
Physical security of IT systems and devices [S1Cybez1>BFSiUIT]

Course

Field of study
Cybersecurity

Year/Semester
4/7

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
24

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
24

Number of credit points

5,00

Coordinators

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

Lecturers

Prerequisites

Student has basic knowledge about electronics, 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:
K1_W02 Has advanced knowledge of physics necessary to understand the fundamental physical phenomena occurring in electronic components and circuits, as well as in communication systems.
K1_W05 Has advanced knowledge of complex data structures; is familiar with the theoretical foundations, principles of data administration, and relevant standards; understands cybersecurity and privacy principles used to manage risks associated with using, processing, storing, and transmitting information or data.

K1_W08 Has detailed knowledge of the structure and principles of operation of basic logic gates, flip-flops, and registers; knows methods for minimizing logic functions; understands the physical construction of a computer and its architecture, including the roles of individual components (CPU, GPU, memory, input/output devices); is knowledgeable about programmable devices and hardware description languages (Verilog, VHDL, P4, NPL); knows and understands the phenomena and mechanisms on which these systems operate.
K1_W020 Knows and understands the threats facing modern civilization, which extensively relies on digital services; is aware of the latest developmental trends related to the field of study.

Skills:
K1_U01 Is able to use literary sources, integrate acquired information, assess and interpret it, and draw conclusions to solve complex and unusual problems in the field of cybersecurity.
K1_U02 Can apply appropriately selected methods and tools, including advanced information and communication technologies, as well as develop simple applications or configure basic systems to conduct simulations, analysis, and design of systems or applications relevant to the field of study.
K1_U12 Is capable of preparing and delivering a presentation on a task related to the field of study, communicates using specialized terminology, and presents and justifies various opinions and viewpoints.

Social competences:
K1_K01 Understands the importance of enhancing professional, personal, and social competencies; is aware that knowledge and skills in the field of cybersecurity evolve rapidly.
K1_K02 Recognizes the significance of knowledge in solving cybersecurity problems; is aware of the necessity of utilizing expert knowledge when addressing engineering tasks that exceed one's own competencies.
K1_K03 Understands the need to formulate and communicate information and opinions to society regarding the positive and negative aspects of cybersecurity and is willing to act in the public interest.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture: Oral or written exam.
Laboratories: Pass based on ongoing work.
Project: Evaluation of a project completed in two-person groups.
In each form of the course assessment, the grade depends on the number of points the student earns relative to the maximum number of required points. Earning at least 50% of the possible points is a prerequisite for passing. The relationship between the grade and the number of points is defined by the Study Regulations. Additionally, the course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university’s electronic systems and during the first class meeting (in each form of classes).

Programme content

Subjects are related with modern electronic devices, mainly programmable, rules, mechanisms and weaknes of their implementation. There are presented mechanisms of attacks on security, cryptography and data privacy. Some ideas for mitigation and preventing are also discussed.

Course topics

Categorization of attacks and security breaches (MITRE table)
Side Channel Attack mechanisms
Analysis of selected examples of devices
Who made a mistake, could it have been avoided, how to do it better
Power analysis (simple, differential, corelational - SPA/DPA/CPA)
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
Methods of analyzing devices and discovering their vulnerabilities
Automation of vulnerability analysis at the design, prototype and product stages

Consequences of backwards compatibility
Ways and tools to prevent SCA
Elements of Desing for Testing - DFT
Methods and tools of SCA susceptibility monitoring and detection
Lab
Become familiar with the laboratory platform for the investigation and analysis of side channel attacks.
Hardware analysis at the electrical level, use of software and hardware device analyzers.
Radio band analysis
Measurements of real test devices
Glitching and Fault Injection
Power analysis and demonstration of attacks on cryptptohraphy
Project:
Student will have to prepare some part of software or whole software tool for demostrating attack, measure some parameters, gather and anlazyze gathered data.

Teaching methods

Lecture with students activities, discussions, presentations
Laboratory with demonstrations and live experiments
Project - practical task supervised by lecturer

Bibliography

Basic:
The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks; Jasper van Woudenberg, Colin O'Flynn; No Starch Press 2021

Additional:
Power Analysis Attacks: Revealing the Secrets of Smart Cards, Stefan Mangard, Elisabeth Oswald, Thomas Popp, Springer 2007

Breakdown of average student's workload

	Hours	ECTS
Total workload	147	5,00
Classes requiring direct contact with the teacher	72	2,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	75	2,50