COURSE DESCRIPTION CARD - SYLLABUS

Course name
IoT Security [S2Inf1E-CYB>IOT]

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 30	Laboratory classes 30	Other 0
Tutorials 0	Projects/seminars 15	

Number of credit points

6,00

Coordinators

dr hab. inż. Paweł Śniatała prof. PP
pawel.sniatala@put.poznan.pl

prof. dr hab. inż. Mariusz Głąbowski
mariusz.glabowski@put.poznan.pl

Lecturers

Prerequisites

A student starting this course should have a basic knowledge of digital electronics, microcontrollers, and microprocessors. He should have knowledge to be able to design and implement computer programs in chosen programming languages (e.g., C, Python) He should also have the ability to obtain information from the indicated sources and be ready to cooperate as part of a team. In the area of social competence, he must present attitudes such as honesty, responsibility, perseverance, cognitive curiosity, creativity, personal culture, and respect for other people.

Course objective

To provide students with knowledge in the field of broadly understood IoT security as well as methods and tools used to estimate and control the risk of compromising confidentiality, integrity and data availability. Key security concepts: confidentiality, authentication, integrity, access control, non-repudiation, and availability) and the state-of-the art security solutions will be reinforced and explored. To acquaint students with advanced methods, techniques and tools used in solving complex engineering tasks in the area of designing and maintaining IoT systems and device focusing on systems and data security.

Course-related learning outcomes

Knowledge:
students will be able to understand or master iot security related to hardware, system and networking.
a student has structured and theoretically founded general knowledge related to key issues in the field of iot security. both device and system level will be discussed.
a student has advanced detailed knowledge of integrating selected sensors with hardware platforms (raspberry pi, arduino) and has knowledge of security vulnerabilities related to analyzed systems.
a student has knowledge of development trends and the most important new achievements of it and telecommunications in the field of iot security.

Skills:
a student can obtain information on the selection of sensors for the implementation of the assumed functions of iot systems and iot devices from the security perspective. the obtained information, student is able to integrate and subsequently subject it to critical evaluation.
a student is able to plan and conduct tests in the field of measuring and testing iot devices and systems security, interpret the obtained results and draw conclusions.
a student will be able to implement light-weight crypthography algorithms on iot platfroms.
a student is able to use experimental methods to formulate and solve engineering tasks and simple research problems in the area of iot security.
a student is able to integrate knowledge from various areas of computer science and telecommunications when formulating and solving engineering tasks related to the design and implementation of iot systems with respect to security requirements.
a student is able to assess usefulness of using new hardware and software solutions for solving engineering tasks, consisting in building efficient, secure iot systems.

Social competences:
a student understands that iot systems integrate several technologies and knowledge and skills in the field of iot security become obsolete very quickly.
a student understands the importance of using the latest knowledge in the field of iot in solving research and practical problems.
a student is aware of the need for a professional approach to solving iot problems and taking responsibility for the projects she/he proposes.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
The knowledge acquired during the lecture is verified by an oral and / or written test.
Test issues, on the basis of which questions are developed, are sent to students via e-mail using the university"s e-mail system.
An oral and / or written test consists of 3 to 5 questions for which a descriptive answer is expected. Each answer to the question is rated on a scale of 0 to 5 points. Each question is scored equally. Passing threshold: 50% of points.
In the case of the oral test, students draw questions from a set of 30 questions. In the case of a written test, questions are asked by a lecturer.
The skills acquired during the laboratory classes are verified on an ongoing basis. At each laboratory class, the correctness of the exercises is assessed on a scale from 2 to 5. The final grade is the average of the grades obtained from individual laboratory classes. The final grade is the average of the grades obtained from each laboratory session.

Programme content

- Internet of Things (IoT).
- Principles of IoT security.
- Case studies of cyber-attacks on IoT systems.
- Overview of selected IoT hardware platforms and software environment.
- Connectivity / communication of IoT devices.
- Lightweight crypthography algorithms.
- Digital forensics in IoT.

Course topics

Lecture topics:
- Internet of Things (IoT) - applications, systems, devices, sensors.
- Principles of IoT security.
- Case studies of cyber-attacks on IoT systems.
- Overview of selected IoT hardware platforms and software environment (Raspberry Pi, Tizen) .
- Connectivity / communication of IoT devices (lightweight IoT communication protocols)
- Lightweight crypthography algorithms.
- IoT systems security and TustZone, Intrusion detection and prevention in IoT, Malicious software in IoT
- Digital forensics in IoT.

Laboratory topics:
- Using Arduino to retrieve information about environmental parameters (temperature sensors, fororesistors, etc.)
- Emergency stop of the production process in response to environmental alarms (Raspberry PI, JSON, MongoDB).
- Using Packet Tracer to test solutions in the field of smart cities and networks (smart grids).
- Prototyping and testing of smart home installations using Packet Tracer (Python, Single Board Computer, smartphone / tablet, router, door opening sensor, etc.)
- Smile-sensitive smart camera (Raspberry PI, Raspberry PI camera, Python, machine learning)
- Intrusion Prevention System (IPS) configuration.
- Testing the vulnerability of simple IoT solutions (Sensor-Actuator System, IFTTT) in the field of ICT security
- Implementation of a choosen lightweight cryptography algorithms (C, python)

Project:
Preparing a research paper in a choosen topics.

Teaching methods

Lectures: multimedia presentations, illustrated with examples given on the blackboard.
Laboratory exercises: practical exercises in groups with the use of hardware platforms.

Bibliography

Basic
1. Paweł Śniatała, Sitharama S Iyengar, Sanjeev Kaushik Ramani: Evolution of Smart Sensing Ecosystems and the need for Tamper Evident Security: Theory to Practice. Springer 2021
2. William Stallings, Lawrie Brown: Compujter Security, Principles and Practice, Pearson 2015. ISBN: 0-13-377392-2.
3. Gaston C. Hillar, Internet of Things with Python Paperback, Packt Publishing, 2016.

Additional
1. Marcin Sikorski, Adam Roman: Internet Rzeczy, Wydawnictwo Naukowe PWN 2020. ISBN: 9788301208400

Breakdown of average student's workload

	Hours	ECTS
Total workload	150	6,00
Classes requiring direct contact with the teacher	75	3,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	75	3,00