COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of IoT and IIoT Systems [S1Cybez1>BSIoT]

Course

Field of study
Cybersecurity

Year/Semester
3/5

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
16

Other
0

Tutorials
0

Projects/seminars
16

Number of credit points

4,00

Coordinators

dr hab. inż. Maciej Sobieraj
maciej.sobieraj@put.poznan.pl

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

Lecturers

Prerequisites

Fundamentals of Local and Wide Area Networks (LAN & WAN) and IoT Systems.

Course objective

• Introduce students to key security issues in IoT and IIoT. • Develop skills in designing and securing IoT and IIoT systems. • Understand the specifics of security in industrial environments, including critical infrastructure. • Prepare students for working in teams focused on IoT and IIoT system security.

Course-related learning outcomes

Knowledge:
• A student understands the fundamental security issues related to IoT and IIoT. [K1_W10]
• A student understands security models used in industrial environments (e.g., Purdue Model). [K1_W10]
• A student ss familiar with the principles of lifecycle management for IoT and IIoT systems.[K1_W09]

Skills:
• Can design and implement security measures for IoT and IIoT systems. [K1_U02]
• Is able to analyze threats and deploy protection mechanisms in industrial systems. [K1_U09]
• Utilizes monitoring and automation tools in IoT and IIoT environments. [K1_U04]

Social competences:
• Understands the importance of protecting critical infrastructure in industrial environments. [K1_K01]
• Recognizes the need for continuous learning in the rapidly evolving field of IoT and IIoT. [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

1. Knowledge: A written exam covering IoT and IIoT security topics.
2. Skills: Ongoing assessment of laboratory tasks and final evaluation of the group project.
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

The course "Security of IoT and IIoT Systems" introduces students to key issues related to protecting Internet of Things (IoT) and Industrial Internet of Things (IIoT) systems. The course combines theoretical and practical aspects, allowing students to understand the specifics of physical, network, and organizational infrastructure in industrial environments. It covers threats specific to IoT and IIoT, such as attacks on critical infrastructure, unsecured Ethernet standards, and issues arising from a lack of network segmentation. Practical sessions include designing and securing IoT systems, as well as analyzing real-world industrial threat scenarios.

Course topics

I. Introduction to IoT and IIoT Security (6x45 minutes)
1. Basic Concepts and Definitions
• Differences between IoT and IIoT.
• Security requirements and challenges in industrial environments.
• Standards and regulations (e.g., NIS2, IEC 62443).
2. Purdue Model
• Layered architecture of industrial systems.
• Network segmentation and isolation as a foundation for security.
3. Legal and Organizational Aspects
• Legal requirements for critical infrastructure protection.
• Organizational structure and security teams.
II. Hardware and Platform Security (6x45 minutes)
1. Security of IoT Platforms
• Security analysis of devices such as Raspberry Pi and Arduino.
• Hardware-level security measures.
2. Security of IoT Network Connections
• Communication protocols (MQTT, CoAP) and their security.
• Protection of wireless connections (Wi-Fi, Bluetooth).
• Firewalls and IPS systems in IoT and IIoT environments.
3. Security of Cloud IoT Platforms
• Microsoft Azure, AWS, Google Cloud - threat analysis and security measures.
• Secure cloud data management.
III. Security Specifics in Industrial (IIoT) Environments (6x45 minutes)
1. Industrial Network Security
• Threats resulting from unsecured Ethernet standards.
• Security in industrial networks (MPLS, Carrier Ethernet).

• Traffic management and protection against DDoS attacks.
2. Attacks on Critical Infrastructure
• Case studies of attacks on SCADA and other industrial systems.
• Mechanisms for protecting critical infrastructure.
3. Functional and Operational Security
• Overview of functional safety in industry.
• Safety principles in industrial environments.
IV. IoT and IIoT System Lifecycle Management (6x45 minutes)
1. Monitoring and Updating IoT/IIoT Systems
• Secure management of device updates.
• Remote management and monitoring of IoT systems.
2. Automation of Network Device Configuration
• Introduction to scripts automating configuration processes.
• Examples of automation tools in IoT and IIoT environments.
V. Laboratories and Project
1. Laboratories
• Configuration of secure IoT and IIoT connections (e.g., securing MQTT, CoAP).
• Implementation of firewall and IPS mechanisms in IoT environments.
• Security analysis of Raspberry Pi and Arduino devices.
2. Group Project
• Development of a secure IoT system: threat analysis, architecture design, and security implementation.
• Presentation of results and discussion on the effectiveness of applied solutions.
Assessment Criteria
1. Knowledge: A written exam covering IoT and IIoT security topics.
2. Skills: Ongoing assessment of laboratory tasks and final evaluation of the group project.
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).

Teaching methods

• Lectures incorporating case studies and multimedia presentations, online
• Practical laboratory sessions on configuring and securing IoT devices.
• Teamwork within a group project.

Bibliography

Basic:
1. "IoT Security: Advances in Authentication" - Chintan Patel, Sudhir Rawat. Wiley, 2021. ISBN: 978-1119676687.
2. "Industrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems" - Pascal Ackerman. Elsevier, 2019. ISBN: 978-0128146870. Amazon.
3. NIS2 Directive - Directive (EU) 2022/2555 of the European Parliament and of the Council. Official Journal of the European Union, December 2022. EUR-Lex.
IEC 62443 - Industrial communication networks - Network and system security. International Electrotechnical Commission (IEC), 2020. IEC Standards.

Additional:
Educational materials prepared by the instructors.

Breakdown of average student's workload

	Hours	ECTS
Total workload	116	4,00
Classes requiring direct contact with the teacher	56	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	60	2,00