COURSE DESCRIPTION CARD - SYLLABUS

Course name
Network security [S2TIIZM1E>BS]

Course

Field of study
Information Technology for Smart and Sustainable Mobility

Year/Semester
1/1

Area of study (specialization)
–

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
32

Laboratory classes
16

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

4,00

Coordinators

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

Lecturers

Prerequisites

Knowledge: Basic knowledge of computer networks, including familiarity with the OSI model, communication protocols (e.g., TCP/IP), IP addressing, and the fundamentals of network devices such as routers and switches. Understanding of operating system fundamentals, particularly in the context of network management and security (e.g., users, permissions, network configuration in Linux/Windows systems). Basic cryptography - general understanding of concepts such as encryption, keys, digital signatures, and hash functions. Skills: Problem-solving - especially in algorithmic and mathematical contexts. Basic programming - ability to analyze and create simple scripts in languages such as Python, C++, or Java. Analytical thinking - ability to approach complex problems methodically.

Course objective

The aim of the course is to introduce students to key concepts, protocols, and techniques for securing computer networks across various layers of the communication model.

Course-related learning outcomes

Knowledge:

The student has knowledge of development trends and the most significant recent achievements in the field of IT network security
The student has advanced and detailed knowledge of the processes occurring in the life cycle of IT systems
The student demonstrates knowledge of advanced methods, techniques, and tools related to network security, in particular methods for protecting wireless networks, ways to secure applications and services using protocols, methods for securing private networks, transport layer and network layer security protocols, and security mechanisms between network layers
The student has knowledge about the risks and dangers associated with network security

Skills:
The student is able to use information and communication technologies applied in the implementation of projects related to IT system security.
The student is able to plan and conduct experiments, interpret the obtained results, draw conclusions, and formulate and verify hypotheses related to complex engineering problems and simple research problems
The student is able to assess the suitability of methods and tools used to secure IT systems, including recognizing the limitations of these methods and tools

Social competences:
The student is prepared to critically assess their knowledge and understands that in computer science, knowledge and skills quickly become outdated
The student understands the importance of using the latest knowledge in network security in the design and operation of IT systems

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Written exam
Practical work - solving problems

Programme content

Network Security, Firewall, VPN (Virtual Private Network), Encryption, IPSec, Wireless Security

Course topics

General concepts: basic network security components such as communication channels, firewalls, VPNs, and proxy servers.
Cross-layer security: cross-layer security mechanisms including EAP and RADIUS, which support secure authentication across network layers.
Network level security: network-layer protocols like IPSec used to secure IP communications through authentication and encryption.
Transport level security: transport-layer security protocols such as SSL/TLS and QUIC, which ensure secure data transmission over networks.
Application/Service level security: securing applications and services with protocols like HTTPS for encrypted web communication.
Wireless security: methods for protecting wireless networks, including WEP and WPA standards.
Private networks (VLAN, VPN): design and security of private networks, focusing on VLANs and VPNs.

Teaching methods

The course is conducted remotely (online) in a synchronous format. Classes may also be held in person. Multimodal presentation. Practical examples, case study.

Bibliography

Basic:
Stallings, W. (2020), Cryptography and Network Security: Principles and Practices, 8th Edition, Pearson.

Additional:

-

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,00
Classes requiring direct contact with the teacher	48	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	52	2,00