COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security in wireless networks [S2EiT1E-TIT>BwSB]

Course

Field of study
Electronics and Telecommunications

Year/Semester
2/3

Area of study (specialization)
Information and Communication Technologies

Profile of study
general academic

Level of study
second-cycle

Course offered in
English

Form of study
full-time

Requirements
elective

Number of hours

Lecture
15

Laboratory classes
30

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

4,00

Coordinators

dr hab. inż. Piotr Remlein
piotr.remlein@put.poznan.pl

Lecturers

Prerequisites

none

Course objective

none

Course-related learning outcomes

Knowledge:
-

Skills:
-

Social competences:
-

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

none

Programme content

Practical application of security policy principles. The use of classical cryptography principles in practical applications to achieve authentication, confidentiality, and data integrity in wireless telecommunication systems.
The utilization of intrusion detection systems, as well as statistical, linear, and differential analysis techniques.
Data protection methods employed in wireless communication systems, including WLAN-802.11 networks, cellular systems (GSM, UMTS, LTE, 5G), TETRA systems, WiMAX, Bluetooth, ZigBee, and IoT solutions.
In the laboratory, students perform tasks using educational software like Cryptool, the Kali Linux system and its tools, and may also use Tamarin software.
Students write programs in C/C++ implementing algorithms that ensure data confidentiality, integrity, or authentication mechanisms.

Course topics

Intrusion Detection Mechanisms and Security Analysis.
Security in WLAN Networks (802.11).
WEP, WPA, WPA2, WPA3 – security mechanisms and their evolution.
Attacks on WLAN networks: eavesdropping, Evil Twin, brute force attacks.
Data protection in corporate and home networks.
Security in Cellular Systems (GSM, UMTS, LTE, 5G).
Encryption and authentication mechanisms: A5/1, KASUMI, 5G-AKA.
User data and transmission protection.
Threats and attacks: IMSI catchers, attacks on SS7 signaling.
TETRA: TEA algorithms and user authentication.
WiMAX: encryption and authorization mechanisms (PKMv2).
Bluetooth: security features in Bluetooth LE and Classic.
ZigBee: application-layer encryption (AES-128).
Security in IoT Solutions.
Practical Implementation of Data Confidentiality and Integrity.
Implementation of VPNs in wireless networks.
Two-factor authentication and digital certificates.
Configuration and securing WLAN networks (WPA3).
Security protocol analysis for WEP, WPA, WPA2, and traffic monitoring.
Attack detection and traffic analysis using IDS tools.

Teaching methods

none

Bibliography

Basic:
-

Additional:
-

Breakdown of average student's workload

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