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

A student beginning this course should have basic knowledge of computer networks, operating systems, wireless communication systems, programming languages and mathematics. He or she should also have the ability to obtain information from indicated sources and be ready to cooperate within the team.

Course objective

The aim of this course is to provide students with knowledge and skills in data security and cryptography. Presentation of security and data safety issues in wireless communication systems on the market or undergoing standardization.

Course-related learning outcomes

Knowledge:
The student has practical knowledge of security systems or methods to ensure the security of information transmitted in computer networks and radio communications. He or she has basic knowledge of development trends in security in wireless systems.

Skills:

The student is able to design selected elements of security systems or protect network devices against unauthorised access and other threats. He is familiar with the principles of activity in the field of standardization of technical solutions related to the security of telecommunications systems, he knows international and national standardization organizations (ITU, ISO, ETSI, 3GPP, etc.). Can obtain information from literature and databases and other sources in Polish or English; can integrate information obtained, interpret it, draw conclusions and justify opinions.

Social competences:
The student understands the need to learn about emerging new solutions in the field of security of radio communication systems. He or she understands that the deployment of ever newer networks and radiocommunications systems requires the cooperation of various engineering teams. The student understands the challenges of radiocommunications due to the increasing demand for their safety.

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 in the course of the lecture is verified by an oral examination. The examination consists of answers to at least 3 questions. Questions are asked by the teacher. The questions concern issues from a set of several dozen issues known to the students (delivered during the lecture and by e-mail. Each answer to a given question is graded on a scale from 2 to 5. The final grade from the oral examination is the average of the grades for each answer. The examination is passed when the average grade is higher than 2.75.
The skills acquired during the laboratory are verified on the basis of the grades obtained from the reports prepared by the student for the tasks he or she receives to perform during the classes. There are about five or seven of them during a semester. The final grade takes into account both the student"s involvement and attitude during the classes and the grades from these reports. The preparation is verified by an oral response to each class. The prerequisite for passing the laboratory is obtaining positive marks for most of the issues.

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

1. Lecture: the multimedia presentation prepared by the teacher, illustrated with examples given on the board. Lecture conducted mostly in the traditional way, but also partly in the form of a conversation and/or problematic lecture.
2. Laboratory: the performance of tasks given by the instructor and described in the form of problem tasks, practical exercises using the equipment available in the laboratory. The laboratory can be supplemented by multimedia presentations or examples given on the board.

Bibliography

Basic
1. Cryptography and network security: principles and practice / William Stallings ; International edition contributions by Mohit P. Tahiliani.,Boston [etc.] : Pearson, cop. 2014.
2. Cryptography engineering : design principles and practical applicationns / Niels Ferguson, Bruce Schneier, Tadayoshi Kohno.,Indianapolis: Wiley, cop. 2010.
3. A classical introduction to cryptography exercise book / by Thomas Baignères [et al.].,New York : Springer, cop. 2006.
Additional
1. Selected fragments of wireless standards available in the IEEE digital library.
2. Applied cryptography : protocols, algorithms, and source code in C / Bruce Schneier.,New York [etc.] : John Wiley & Sons, 1994.
3. Cryptography in C and C++, M. Welschenbach, APress, 2001.

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,00
Classes requiring direct contact with the teacher	55	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	45	2,00