COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security in wireless networks

Course

Field of study
Electronics and Telecommunications

Year/Semester
II/III

Area of study (specialization)

Profile of study
general academic

Level of study
Second-cycle studies

Course offered in
Polish

Form of study
full-time

Requirements
elective

Number of hours

Lecture
30

Laboratory classes
0

Other (e.g. online)

Tutorials
0

Projects/seminars
15

Number of credit points

4

Lecturers

Responsible for the course/lecturer:
dr hab. inż. Piotr Remlein
piotr.remlein@put.poznan.pl

Responsible for the course/lecturer:

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:

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

Security policy principles. Basic concepts of cryptography, examples of classical cryptographic systems. Cipher breaking methods, statistical, linear, differential cryptogram analysis. Examples of other cryptographic systems DES, AES. Ciphers with a public key. Backpack cipher. RSA cipher. RSA cipher security. Diffy-Hellman's, El Gamal's and Massey's ciphers - Omura. Shortcut functions MD5, SHA. Intrusion detection systems. Data protection methods used in wireless communication systems: DECT, GSM, UMTS, LTE, 5G, IoT, TETRA, WLAN-802.11, WiMAX, Bluetooth, ZigBee.

Laboratory: the students carry out tasks based on Cryptool didactic software, they write programs in C/C++ they implement basic encryption/decryption algorithms, solve security problems of 802.11 wireless networks using devices from the wireless networks laboratory.

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. Ocena bezpieczeństwa sieciowego / Kevin Lam, David LeBlanc, Ben Smith ; [przekł. Marek Włodarz] ; Microsoft.,Warszawa : APN PROMISE, 2005.

2. Kryptografia i bezpieczeństwo sieci komputerowych : matematyka szyfrów i techniki kryptologii / William Stallings ; [tł. Andrzej Grażyński].,Gliwice : Helion, cop. 2012.

3. Systemy radiokomunikacji ruchomej, Krzysztof Wesołowski, WKiŁ, Warszawa, 2003.

4. Ochrona danych w sieci i intersieci – w teorii i praktyce, W. Stallings, WNT, Warszawa, 1997.

Kali Linux : audyt bezpieczeństwa sieci Wi-Fi dla każdego / Vivek Ramachandran, Cameron Buchanan ; [tłumaczenie: Grzegorz Kowalczyk]. Gliwice : Helion, cop. 2016.

Additional

1. Wybrane fragmenty standardów systemów bezprzewodowych dostępnych w bibliotece cyfrowej IEEE.

2. Dowolny podręcznik dotyczący sieci Wi Fi (802.11) dostępny w j. polskim lub angielskim.

3. Dowolny podręcznik dotyczący standardów Bluetooth, Z-Wave, ZigBee, LoRA, TETRA.

4. Cryptography in C and C++, M. Welschenbach, APress, 2001.

5. UMTS system telefonii komórkowej trzeciej generacji, J. Kołakowski, J. Cichocki, WKiŁ, Warszawa, 2003.

Breakdown of average student's workload

	Hours	ECTS
Total workload	100	4,0
Classes requiring direct contact with the teacher	55	2,0
Student's own work (literature studies, preparation for laboratory classes/tutorials, preparation for tests/exam, project preparation) [1]	45	2,0

[1] delete or add other activities as appropriate