COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security in wireless networks [S2Teleinf2-ISS>BwSB]

Course

Field of study
Teleinformatics

Year/Semester
1/2

Area of study (specialization)
Intelligent control systems

Profile of study
general academic

Level of study
second-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
14

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

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

Lecturers

Prerequisites

A student starting 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 the indicated sources and have a willingness to cooperate as part of a team.

Course objective

The purpose of the course is to provide students with knowledge and skills in data protection and security of network systems, the use of cryptography issues in real systems. The presentation of issues of security and data protection in wireless communication systems: present on the market or in the process of standardization.

Course-related learning outcomes

Knowledge:
The student has a practical knowledge of security systems or methods to ensure the security of information transmitted in wireless data communication networks and radio communications. Has a basic knowledge of development trends in security in wireless systems [K2_W01, K2_W02,K2_W06,

K2_W07, K2_W08, K2_W11].

Skills:
The student is able to design selected elements of security systems or is able to protect network devices from unauthorized access and other threats. He/she is familiar with the principles of activity in the field of standardization of technical solutions related to security of telecommunication systems; he/she knows international and national standardization organizations (ITU, ISO, ETSI, 3GPP, etc.). He/she is able to acquire information from literature and databases and other sources in Polish or English; he/she is able to integrate obtained information, interpret it, draw conclusions and justify opinions [K2_U01, K2_U08, K2_U16].

Social competences:
The student understands the necessity to learn about emerging new solutions in the field of radio communication systems security. Understands that the deployment of newer and newer radiocommunication networks and systems requires the cooperation of diverse teams of engineers. Understands the challenges facing radiocommunications due to the increasing demand for their security [K2_K01, K2_K02, K2_K04, K2_U17].

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

The knowledge acquired in the lecture is verified by an oral exam. The exam consists of answers to at least 3 questions. The questions are asked by the instructor. The questions relate to issues from a set of dozens of issues known to the students (provided at the lecture and by electronic means - e-mail). Each answer to the question asked is graded on a scale of 2 to 5. The final grade of the oral exam is the average of the grades for each answer. The exam is passed when the average grade is higher than 2.75. The exam can also be conducted in written form or a test. The exam is passed when the number of points obtained is at least 60%.
The skills acquired in laboratory classes are verified on the basis of the grades obtained from the reports prepared by the student for the tasks he is given to carry out in the course. There are about five or seven of these during the semester. The final grade takes into account both the student's involvement and attitude during class and the grades from the aforementioned reports. The preparation is verified by an oral response in each class The prerequisite for passing the course is the achievement of positive grades for most of the topics.

Programme content

Practical use of security policy principles. Use of the principles of classical cryptography in practical applications for authentication, realization of confidentiality and integrity of data in wireless data communication systems. Use of intrusion detection systems, statistical, linear, differential analysis. (K2_W08, K2_U08, K2_U09, K2_U10)
Data protection methods used in wireless communication systems: in GSM, UMTS. Data protection in LTE, 5G. (K2_W08, K2_U08, K2_U09, K2_U10)
Security implementation in IoT systems, TETRA, in WLAN-802.11, WiMAX, Bluetooth, ZigBee. (K2_W08, K2_U08, K2_U09, K2_U10)
As part of the project, students complete tasks based on Cryptool, Tamarin soft teaching software, write programs in C/C++ implementing algorithms to ensure confidentiality, data integrity, or authentication mechanisms. (K2_W08, K2_U08, K2_U09, K2_U10)

Course topics

Practical use of security policy principles. Use of the principles of classical cryptography in practical applications for authentication, realization of confidentiality and integrity of data in wireless data communication systems. Use of intrusion detection systems, statistical, linear, differential analysis. (K2_W08, K2_U08, K2_U09, K2_U10)
Data protection methods used in wireless communication systems: in GSM, UMTS. Data protection in LTE, 5G. (K2_W08, K2_U08, K2_U09, K2_U10)
Security implementation in IoT systems, TETRA, in WLAN-802.11, WiMAX, Bluetooth, ZigBee. (K2_W08, K2_U08, K2_U09, K2_U10)
As part of the project, students complete tasks based on Cryptool, Tamarin soft teaching software, write

programs in C/C++ implementing algorithms to ensure confidentiality, data integrity, or authentication mechanisms. (K2_W08, K2_U08, K2_U09, K2_U10)

Teaching methods

1. Lecture: multimedia presentation prepared by the instructor, illustrated by examples given on the blackboard. Lecture conducted mostly in a traditional manner, but also partially in the form of a conversational and/or problem lecture
2. Laboratory: performance of tasks given by the instructor and described in the form of problem tasks, practical exercises with the use of equipment available in the laboratory. Laboratory classes can be supplemented by multimedia presentations or examples given on the blackboard.

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.
4. Kali Linux : auditing Wi-Fi security for everyone / Vivek Ramachandran, Cameron Buchanan, 2016.

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.,Ne w 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	78	3,00
Classes requiring direct contact with the teacher	38	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	40	1,50