COURSE DESCRIPTION CARD - SYLLABUS

Course name
Wireless Communication Security [S2Inf1E-CYB>BSB]

Course

Field of study
Computing

Year/Semester
1/1

Area of study (specialization)
Cybersecurity

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
30

Laboratory classes
15

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr inż. Tomasz Bilski
tomasz.bilski@put.poznan.pl

Lecturers

Prerequisites

Student should have basic knowledge on IT systems, including operating systems, computer networks with special emphasis on wireless networks. Student should have abilities for information accessing from given sources and should be prepared to work in a team.

Course objective

Providing students with knowledge on data security in wireless communication systems. Providing students with skills related to wireless communication systems modelling, designing and testing with special emphasis on data security.

Course-related learning outcomes

Knowledge:
1. student has detailed knowledge on wireless communication systems
2. student has knowledge on vulnerabilities and threats related to wireless communication systems
3. student has knowledge on methods, tools and rules for data protection in wireless communication systems.

Skills:
student can:
- provide assumptions, concept and design for wireless communication systems including iot applications,
- perform analysis of structure and operation of wireless communication systems ncluding security level analysis,
- fulfill requirements related to high data security level.

Social competences:
student understands that:
- one of the important it system aspects is data protection,
- it is necessary to update knowledge about particular tools and systems.

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Theoretical knowledge is verified during 45-minute test performed last lecture. To achieve positive result student should get more than 50% of points. Test topics are provided to students by email at the beginning of the semester.
Practical skills are verified during classes (related to particular tasks or design phases) and by assessment of final project and its documentation.

Programme content

The module covers the following topics
1. Introduction
2. Standards for wireless transmission
3. Vulnerabilities and threats
4. Examples of attacks
5. Security in WLAN IEEE 802.11
6. Security in IoT
7. Out of band authentication
8. Current problems and trends.

Course topics

The lecture should cover the following topics:
1. Introduction – classification and description of wireless communication systems (bandwidth, technology, protocols)
2. Standards for wireless transmission (including: Bluetooth, ZigBee, 6LoWPAN, IEEE 802 standards family, NFC, VLC)
3. Vulnerabilities and threats related to wireless communication systems including IoT. General description of tools, methods and rules of protection
4. Examples of attacks: RF jamming, scrambling, skyjacking, ASLEAP, association flood, probe request flood, RTS/CTS flood, …
5. Security in WLAN IEEE 802.11. Encryption, authentication, integrity control
6. Security in IoT
7. Out of band authentication
8. Current problems and trends.

The laboratory classes should cover the following topics:
Classes 1-5: WLAN network configuration in 802.11 standards (modes: IBSS, ESS); preshared-key cryptographic mechanisms; certificate-based cryptographic mechanisms (RADIUS / Kerberos servers); access control mechanisms, traffic isolation (user isolation / multi SSID / VLAN), vulnerabilities in 802.11 WLAN networks and penetration testing.
Classes 6-8: Development of a wireless network concept for a selected application with particular emphasis on methods, tools and principles of protection. Preparation of assumptions for the system. Selection of appropriate protocols, network devices, software. Development of documentation for the

designed system, including implementation costs. System security assessment. Taking into account the latest technologies in the field of data protection.

Teaching methods

Interactive lecture (with questions for students) with a use of multimedia presentation. Files with slides provided to students. Elearning.
Project in the form of consultation and verification of each design phases. Tasks performed in teams of 2 students with a use of computer hardware, software and Internet.

Bibliography

Basic
M. Apolinarski, T. Bilski, M. Retinger, Sieci komputerowe. Laboratorium. Wyd. PP, Poznań, 2020 [in Polish]
Additional
standards.ieee.org/getieee802/index.html
morse.colorado.edu/~tlen5510/text/classwebch1.html
www.wi-fiplanet.com
www.wifialliance.com
www.wlana.org
www.wi-fi.org
www.bluetooth.com
www.dmoz.org/Computers/Data_Communications/Wireless/

Breakdown of average student's workload

	Hours	ECTS
Total workload	75	3,00
Classes requiring direct contact with the teacher	45	2,00
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	30	1,00