COURSE DESCRIPTION CARD - SYLLABUS

Course name
Wireless communication security

Course

Field of study	Year/semester
Computing	1/1
Area of study (specialization)	Profile of study
Cybersecurity	general academic
Level of study	Course offered in
Second-cycle studies	English
Form of study	Requirements
full-time	elective

Number of hours

Lecture	Laboratory classes	Other (e.g. online)
30	15	
Tutorials	Projects/seminars	

Number of credit points

3

Lecturers

Responsible for the course/lecturer:

dr inż. Tomasz Bilski

tomasz.bilski@put.poznan.pl

tel: 61 665 35 54

Faculty of Computing and Telecommunications

Responsible for the course/lecturer:

dr inż. Michał Apolinarski

michal.apolinarski@put.poznan.pl

tel: 61 665 39 92

Faculty of Computing and Telecommunications

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

POZNAN UNIVERSITY OF TECHNOLOGY

EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM (ECTS)

pl. M. Skłodowskiej-Curie 5, 60-965 Poznań

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:

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

Lecture

1. Introduction – classification and description of wireless communication systems (bandwidth, technology, protocols)

2. Standards for wireless transmission (including: Bluetooth, ZigBee, 6LoWPAN, LoRaWAN, 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

POZNAN UNIVERSITY OF TECHNOLOGY

EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM (ECTS)

pl. M. Skłodowskiej-Curie 5, 60-965 Poznań

7. Out of band authentication

8. Current problems and trends.

Laboratory

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/

POZNAN UNIVERSITY OF TECHNOLOGY

EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM (ECTS)

pl. M. Skłodowskiej-Curie 5, 60-965 Poznań

Breakdown of average student's workload

	Hours	ECTS
Total workload	75	3,0
Classes requiring direct contact with the teacher	45	2,0
Student's own work (literature studies, elearning, preparation for test, project and documentation preparation) [1]	30	1,0

---

[1] delete or add other activities as appropriate