COURSE DESCRIPTION CARD - SYLLABUS

Course name
Security of mobile applications [S1Cybez1>BAM]

Course

Field of study
Cybersecurity

Year/Semester
3/6

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
Polish

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
24

Laboratory classes
24

Other
0

Tutorials
0

Projects/seminars
0

Number of credit points

3,00

Coordinators

dr inż. Marcin Rodziewicz
marcin.rodziewicz@put.poznan.pl

Lecturers

Prerequisites

Students starting this course should have: 1. Basic knowledge of programming - knowledge of programming languages such as Java, Kotlin (Android) or Swift (iOS), and the ability to work with appropriate development tools 2. Basic knowledge of mobile operating systems 3. Basic knowledge of IT security - knowledge of application security threats, cryptography and authentication 4. Basic knowledge of computer networks - understanding how computer networks and communication protocols work

Course objective

The goal of the course is to familiarize students with key issues related to mobile application security, including threats specific to Android and iOS platforms and methods to minimize them. Participants will learn how to design and implement secure applications, protect user data, ensure secure communications, and detect and eliminate mobile application vulnerabilities.

Course-related learning outcomes

Knowledge:
1. Has a structured knowledge of mobile application security [K1_W09]

Skills:
1. Is able to use the rich resources available on the Internet to ensure the security of mobile applications [K1_U01]
2. Is able to implement security mechanisms in mobile applications [K1_U02]

Social competences:
1. Knows the limitations of his own knowledge and skills, understands the need for further training [K1_K01]
2. Is aware of the need for a professional approach to solving technical problems and taking responsibility for the technical solutions he proposes [K1_K02]
3. Has a sense of responsibility for the designed systems and realizes the risks to people and society in the event of their inadequate design or execution [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Knowledge acquired in the lecture is verified by a colloquium or oral assessment carried out at the last lecture.
Skills acquired in laboratory classes are verified on the basis of fulfilling tasks assigned in class or project. In both didactic forms, a passing threshold of 50% of the possible points is adopted. The following grading scale is used: < 50% 2.0; 50%-59% 3.0; 60%-69% 3.5; 70%-79% 4.0; 80%-89% 4.5; 90%-100% 5.0.
The course completion rules and the exact passing thresholds will be communicated to students at the beginning of the semester through the university's electronic systems and during the first class meeting (in each form of classes).

Programme content

The course programme covers the following topics:
- Introduction to mobile application security
- Authentication and authorization management
- Secure data storage
- Communication security
- Application code security
- User interface security
- Platform-specific security

Course topics

The lecture program includes:
1. Introduction to mobile application security
2. The architecture of mobile systems security
3. Security of data storage
4. Secure communication in mobile applications
5. Authentication and authorization in mobile applications
6. Code security of mobile applications
7 Permissions and resource management in applications
8. User interface security
9. Typical vulnerabilities of mobile applications
10. Testing the security of mobile applications
11. Security specific to Android and iOS platforms
12. The future of mobile application security
The lab program includes:
1. Application permissions analysis and management
2. Encryption of local data
3. Implementation of secure communication
4. Authentication and authorization

Teaching methods

1.Lecture online: tutorial with multimedia presentation

2. Laboratory exercises: Execution of tasks from instructions provided by the instructor and/or project

Bibliography

Basic:
Dominic Chell, Tyrone Erasmus, Shaun Colley, Ollie Whitehouse, "Bezpieczeństwo aplikacji mobilnych. Podręcznik hakera"
Documentation of mobile platforms:
https://developer.android.com/topic/security
https://developer.apple.com/documentation/security

Additional:
-

Breakdown of average student's workload

	Hours	ECTS
Total workload	90	3,00
Classes requiring direct contact with the teacher	48	1,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	42	1,50