COURSE DESCRIPTION CARD - SYLLABUS

Course name
Operating systems security [S1Cybez1>BSO]

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
elective

Number of hours

Lecture
16

Laboratory classes
30

Other
0

Tutorials
0

Projects/seminars
12

Number of credit points

4,00

Coordinators

dr inż. Marek Michalski
marek.michalski@put.poznan.pl

dr hab. inż. Mariusz Żal
mariusz.zal@put.poznan.pl

Lecturers

Prerequisites

A student enrolling in this course should have knowledge of computer architecture, operating systems, computer networks, basic IoT concepts, and the fundamentals of cryptography. They should also possess the ability to program in high-level languages.

Course objective

The aim of the course is to familiarize students with typical threats and attacks on an operating system. During the classes, students will learn various techniques for securing operating systems, covering both hardware and software aspects. They will also explore methods of attacking an operating system as well as defense techniques.

Course-related learning outcomes

Knowledge:
The student has knowledge of network functions performed by the operating system, including their

security. [K1_W07]
The student knows the types of attacks on operating systems. [K1_W10]
The student understands the threats faced by modern society, which extensively relies on digital services where operating systems play a crucial role. [K1_W20]

Skills:
• The student is able to use literature sources, integrate acquired information, evaluate and interpret it, and draw conclusions to solve complex and unconventional problems in the field of cybersecurity. [K1_U01]
• The student can select appropriate security methods based on the type of operating system and its functions. [K1_U02]
• The student is able to compare different security measures and authentication techniques to choose the most suitable solution ensuring the security of operating systems. [K1_U08]

Social competences:
• The student understands the importance of enhancing professional, personal, and social competencies and is aware that knowledge and skills in the field of cybersecurity evolve rapidly. [K1_K01]
• The student is aware of the responsibility for implemented security solutions and is capable of working effectively in a team. [K1_K05]

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Lecture:
Knowledge acquired during the lecture is verified through a written or oral exam.
Written Exam:
Students must answer 7-10 questions (a combination of multiple-choice and open-ended), each assigned different point values. There are three or four scoring categories/groups.
Oral Exam:
Students draw one question from each scoring category. For each drawn question, the student may also receive an additional follow-up question related to the main question. The evaluation of each question (covering both the main and follow-up) takes into account the completeness of the answer and the depth of understanding of the topic.
For each exam session, 50-60 questions are prepared. A minimum of 50% of the total possible points is required to pass.
Project Assessment:
Skills gained through project work are assessed based on the presented projects. The evaluation focuses on the level of engagement in preparing the project, the tools utilized, and the extent of additional knowledge students had to acquire. Projects can be done individually or in pairs. The grading scale ranges from 2 to 5.
Laboratory Assessment:
Skills acquired in the laboratory are verified through a task assigned during the final lab session. This task is divided into 5-6 subtasks, each with different point values. The subtasks form a complete whole, but each can be done independently. Failure to complete one subtask does not affect the evaluation of the remaining subtasks. The passing threshold is 50% of the total points.
Additionally, 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 program covers aspects of operating system security related to both hardware and software. The presented content also takes into account the user’s impact on operating system security.

Course topics

Lectures:
1. Introduction to operating system security
2. Security of operating system architecture

3. Access control and permissions
4. User authentication and authorization
5. Cryptographic methods used in operating systems
6. Protection against malicious software
7. Operating system configuration
8. Security of network services in operating systems
9. Event logging, intrusion analysis, and incident response
10. Security standards, norms, and policies
Laboratories:
Topics consistent with the lecture content.
Projects:
Projects carried out in one- or two-person teams. Project topics aligned with the lecture themes.

Teaching methods

Lecture - multimedia presentations illustrated with examples provided on the board.
Laboratory exercises - performing tasks assigned by the instructor, supplemented by multimedia presentations.
Project classes - multimedia presentations, discussions with students.

Bibliography

Basic:
1. Abraham Silberschatz, Greg Gagne, Peter B. Galvin, Podstawy systemów operacyjnych tom 1, 2 i 3. Wydawnictwo Naukowe PWN, 2021.
2. Donald A. Tevault, Bezpieczeństwo systemu Linux. Hardening i najnowsze techniki zabezpieczania przed cyberatakami, Wydawnictwo Helion, 2024.

Additional:
1. Forshaw James, Windows Security Internals: A Deep Dive Into Windows Authentication, Authorization, and Auditing, No Starch Pr, 2024

Breakdown of average student's workload

	Hours	ECTS
Total workload	103	4,00
Classes requiring direct contact with the teacher	58	2,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	45	1,50