POZNAN UNIVERSITY OF TECHNOLOGY

EUROPEAN CREDIT TRANSFER AND ACCUMULATION SYSTEM (ECTS)

COURSE DESCRIPTION CARD - SYLLABUS

Course name
Advanced System Security [S2Inf1E-CYB>ZBSK]

Course

Field of study
Computing

Area of study (specialization)
Cybersecurity

Level of study
second-cycle

Form of study
full-time

Year/Semester
1/1

Profile of study
general academic

Course offered in
English

Requirements
compulsory

Number of hours

Lecture	Laboratory classes	Other
15	45	0
Tutorials	Projects/seminars	
0	0	

Number of credit points

5,00

Coordinators

dr inż. Michał Szychowiak prof. PP
michal.szychowiak@put.poznan.pl

Lecturers

Prerequisites

Student starting this module should have basic knowledge regarding operating systems, network technologies, and fundamental concepts of cryptology. Should also efficiently use the Unix family and MS Windows operating systems, have basic programming skills, and be able to acquire additional information from supplementary sources. Student should also understand the need to extend his/her competences. In addition, in respect to the social skills the student should show such attitudes as honesty, responsibility, perseverance, curiosity, creativity, manners, and respect for other people.

Course objective

1. Provide students with a detailed knowledge of the security of computing systems in the field of computer networks and distributed processing. 2. Develop students" ability to solve particular security problems of distributed processing and data protection in a distributed environment.

Course-related learning outcomes

Knowledge:
upon completion of the course the student:
1. has well-established theoretical knowledge regarding algorithms and computational complexity,

computer systems architecture, operating systems, and networking technologies
2. has detailed theoretical knowledge related to selected areas of computer science
3. has knowledge regarding trends and the most important new developments in computer science and related disciplines, concerning in particular security threats and methods of protection
4. has basic knowledge regarding life-cycle of software or hardware systems
5. knows the basic methods, techniques and tools used to solve problems in the field of information security

Skills:
upon completion of the course the student is able to:
1. acquire, combine, interpret and evaluate information from literature, databases and other information sources (in mother tongue and english); draw conclusions and formulate opinions based on it
2. to plan and arrange self-education process
3. to employ analytical, simulation, and experiment methods to formulate and solve engineering tasks and basic research problems
4. to combine knowledge from different areas of computer science (and if necessary from other scientific disciplines) to formulate and solve engineering tasks; and use system approach that also incorporates nontechnical aspects
5. to formulate and test hypotheses regarding engineering problems and basic research problems
6. to assess usefulness and possibility of employing new developments (methods and tools) and new it products
7. to propose enhancements (improvements) to existing technical solutions
8. to evaluate usefulness of methods and tools (also to identify their limitations) used to solve engineering tasks, i.e., building it systems or their components
9. to design (according to a provided specification which includes also non-technical aspects) a complex device, an it system, or a process; and is able implement it (at least partially) using appropriate methods, techniques, and tools (including adjustment of available tools or developing new ones)

Social competences:
upon completion of the course the student:
1. understands that knowledge and skills related to computer science and data mining quickly becomes non relevant
2. knows examples of data mining and analysis and understands their limitations
3. is aware of the social role of technical university graduates, and especially understands the need of informing the society (especially through mass-media) about new developments in engineering and others areas

Methods for verifying learning outcomes and assessment criteria

Learning outcomes presented above are verified as follows:

Learning outcomes presented above are verified as follows:
Formative assessment:
a) lectures:
• based on answers to question in a written exam,
b) laboratory classes:
• evaluation of doing correctly assigned tasks (following provided lab. instructions).
Total assessment:
a) verification of assumed learning objectives related to lectures:
• evaluation of acquired knowledge on the basis of the written exam,
b) verification of assumed learning objectives related to laboratory classes:
• evaluation of student’s knowledge necessary to prepare, and carry out the lab tasks,
• monitoring students’ activities during classes,
• evaluation of the written final test concluding the laboratory classes.
Additional elements cover:
• discussing more general and related aspects of the class topic,
• showing how to improve the instructions and teaching materials.

Programme content

The programme covers the following subjects:
Distributed and Web systems threats. System hardening. Distributed authentication and access control policies. Intrusion detection and prevention. Security of the Web Services and Service Oriented Architecture environment.

Course topics

The detailed course topics include:
Formal access control models and their practical implementations, with special attention to DAC, CAP, MAC, RBAC and ABAC models. System hardening for increased security: sandboxing (chroot), compartmentalization (Docker containers, Windows AppContainers), restricted execution environment (AppArmor, SELinux). Secure global network infrastructure (configuration and use of the DNSsec service). Distributed authentication and access control (Kerberos, Active Directory, Radius). Cross-platform (Linux, Windows, Cisco IOS) VPN technologies: IPsec and OpenVPN. Advanced firewalls (NextGeneration Firewalls), IDS/IPS systems (Snort/Suricata), and Application Layer Gateways (ModSecurity). Protection against DDoS attacks. Security of the Web Services and Service Oriented Architecture environment. Operating system and application vulnerability assessment (Kali Linux, BurpSuite). Security monitoring and event management.

Teaching methods

Lectures: multimedia presentation illustrated with examples and showcases.
Labs: practical exercises, discussion, teamwork, competitions or case studies.
Additionally: selected techniques of the Flipped Blended Learning methodology.

Bibliography

Basic
1. William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", IV ed., Pearson Education, 2018
2. Andrew Hoffman, "Web Application Security", O'Reilly, 2020
3. Mullder et al. (ed.), "Trends in Data Protection and Encryption Technologies", Springer, 2023

Additional
1. Hakima Chaouchi, Maryline Laurent-Maknavicius, "Wireless and Mobile Networks Security", Wiley, 2009
2. Song Y.Yan, "Cybercryptography: Applicable Cryptography for Cyberspace Security", Springer, 2019
3. Chris Fry, Martin Nystrom, "Security Monitoring", O"Reilly, 2009
4. Bartosz Brodecki, Piotr Sasak, Michał Szychowiak: "Security policy conflicts in service-oriented systems", In New Generation Computing, vol. 30, no. 2-3, pp. 215-240; Ohmsha Ltd. & Springer-Verlag, 2012
5. Michał Jabczyński, Michał Szychowiak: "Orwell. From Bitcoin to secure Domain Name System", Proceedings of the 3rd Workshop on Social and Algorithmic Issues In Business Support (SAIBS 2015), 2015

Breakdown of average student's workload

	Hours	ECTS
Total workload	125	5,00
Classes requiring direct contact with the teacher	60	2,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	65	2,50