COURSE DESCRIPTION CARD - SYLLABUS

Course name
Cybersecurity [S1SI1E>BSI]

Course

Field of study
Artificial Intelligence

Year/Semester
4/7

Area of study (specialization)
–

Profile of study
general academic

Level of study
first-cycle

Course offered in
english

Form of study
full-time

Requirements
compulsory

Number of hours

Lecture
30

Laboratory classes
30

Other (e.g. online)
0

Tutorials
0

Projects/seminars
0

Number of credit points

5,00

Coordinators

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

dr inż. Arkadiusz Danilecki
arkadiusz.danilecki@put.poznan.pl

Lecturers

Prerequisites

Student starting this module should have basic knowledge regarding operating systems and computing networks. Should also be able to efficiently use the Unix family and MS Windows operating system, along with basic programming skills (including main system calls), and to acquire additional information from supplementary sources. Student should understand the need to extend his/her competences. In addition, in respect to the social skills the student should show attitudes as honesty, responsibility, perseverance, curiosity, creativity, manners, and respect for other people.

Course objective

1. Acquaint the students with the understanding of basic security problems, regarding the use, configuration and administration of security mechanisms at the system and application level, with particular attention on the communication facilities and protocols. 2. Develop students' skills in solving problems related to securing the computing system infrastructure and applications. 3. Getting the students to develop effective use of cryptographic mechanisms, access control and network communication protection, along with application layer security tools. 4. Acquire such skills by solving practical exercises during laboratory classes.

Course-related learning outcomes

Knowledge:
1. the student knows and understands the methods, techniques and tools used to solve problems in the field of information security concernind operating systems, computer networks, network services and software applications, including the use of cryptographic tools, VPN, firewalls and IDS
2. the student has knowledge related to professional ethics and responsibilities; understands the threats related to electronic crime
3. the student 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
5. the student has a fundamental knowledge necessary to identify security threats of operating systems, computer networks and software applications
6. the student has the knowledge necessary for the proper selection of tools for authentication, confidentiality and integrity protection of data and communication

Skills:
1. the student can protect the transmitted data against unauthorized reading
2. the student is able to assess software architecture from the perspective of non-functional requirements concerning the security protection
3. the student is able to 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
4. the student can configure the operating system and network devices aimed at increasing safety of their work
5. the student can use firewalls and cryptographic tools (e.g. SSH, PGP)
6. the student can build a proper communication environment with VPN (using IPsec) and SSO mechanisms

Social competences:
1. the student understands that knowledge and skills related to computer science and data mining quickly becomes non relevant
2. the student knows examples of data mining and analysis and understands their limitations
3. the student 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:

Formative assessment:
a) lectures:
• based on answers to question in the 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,
• discussion of correct answers in the 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 lab reports (partly started during classes, finished after them),
• evaluation of the written final test concluding the laboratory classes.
Additional grading criteria cover:
• active participation in the class,
• discussing related aspects of the class topic,
• showing how to improve the instructions and teaching materials.

Programme content

The course covers the following main areas:
• Security threats in the context of confidentiality, integrity and availability of information, overall threats analysis, main threat models and basic risk assessment metodologies
• Practical application of cryptography, including digital signature systems, cryptographic certificates and public key infrastructure (PKI), data and communication protection (such as EFS, S/MIME, SSH, TLS,).
• Security of operating systems, including especially sensitive components. Methods of system fingerprinting and service enumeration. Basic models of authentication, biometrics, one-time password systems and the single sign-on (SSO) implementations. Access control strategies (POSIX ACL, Windows DACL). File systems security.
• Security of the network infrastructure, including issues of communication protocols, types and functions of firewalls, network perimeter (demilitarized zone), virtual private networks (VPN) and the protocols used to implement them. Network-wide authentication systems (Kerberos).
• Application security, including threats and protection of network applications and services, such as web services, e-mail and instant messaging. Issues of secure programming, particularly in the context of the construction of network applications. Standards for security services API (e.g. GSSAPI). Mechanisms of hardening the application execution environment, system and application sandboxes.
• Security management, including design and implementation of a security policy, security analysis tools and monitoring systems, IDP/IPS, honeypots and honeynets. Incident response procedures.

Teaching methods

1. Lectures: multimedia presentation, presentation illustrated with examples and showcases
2. Labs: practical exercises, discussion, teamwork, competitions or case studies

Bibliography

Basic:
1. William Stallings, Lawrie Brown, "Computer Security: Principles and Practice", Pearson Education, 2018
2. William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education, 2017
3. Matt Bishop, "Computer Security. Art and Science", II ed., Pearson Education, 2019
4. Ross Anderson, "Security Engineering", John Wiley & Sons, 2020
5. Lee Brotherston, Amanda Berlin, "Defensive Security Handbook", O'Reilly, 2017

Additional:
1. Neil Smyth, "Security+ Essentials", Payload Media, 2012 (http://techotopia.com/index.php?title=Security%2B_Essentials)
2. John Savard, "A Cryptographic Compendium" (http://www.quadibloc.com/crypto/jscrypt.htm)

Breakdown of average student's workload

	Hours	ECTS
Total workload	125	5,00
Classes requiring direct contact with the teacher	62	2,50
Student's own work (literature studies, preparation for laboratory classes/ tutorials, preparation for tests/exam, project preparation)	63	2,50