Security engineering - course description

General information

Course name	Security engineering
Course ID	11.9-WE-INFD-SecEng-Er
Faculty	Faculty of Computer Science, Electrical Engineering and Automatics
Field of study	Computer Science
Education profile	academic
Level of studies	Second-cycle Erasmus programme
Beginning semester	winter term 2022/2023

Course information

Semester	1
ECTS credits to win	5
Course type	obligatory
Teaching language	english
Author of syllabus	• dr hab. inż. Bartłomiej Sulikowski, prof. UZ

Classes forms

The class form	Hours per semester (full-time)	Hours per week (full-time)	Hours per semester (part-time)	Hours per week (part-time)	Form of assignment
Lecture	30	2	-	-	Exam
Laboratory	30	2	-	-	Credit with grade

Aim of the course

- familiarizing the student with cryptographic algorithms and protocols
- development of skills in the use of information security procedures
- familiarizing the student and shaping the skills of defining and applying security policy in company

Prerequisites

Computer networks

Scope

Information Safety. Definitions. Infrastructure. Security models.
Access to the system. System access control. User access management. Range of the user responsibility. Risk estimation and management.
Security of teleinformatic systems and networks. Types of attacks. Firewalls (IDS and IPS). Physical security. Alarm systems. Protection against electro-magnetic eavesdropping - TEMPEST standard.
Security policies. The role and tasks of the security administrator.
Industrial safety.
Cryptography. Symmetric algorithms (DES, 3DES, AES, Twofish, RCx family, Serpent, Mars) and asymmetric (RSA, DH, ElGamal, EC). Cryptographic protocols. Public key cryptography. Hashing functions. Electronic signature and its verification. Certification of devices and users. PKI architecture. Other services using cryptography.
Basics of digital forensics.

Teaching methods

lecture: conventional lecture, discussion

laboratory: laboratory exercises

Learning outcomes and methods of theirs verification

Outcome description	Outcome symbols	Methods of verification	The class form
knows the rules for protection of classified information, in particular physical protection and electromagnetic		• a quiz	• Lecture
understands the problems related to industrial security		• a quiz	• Lecture • Laboratory
knows the characteristics of cryptographic algorithms and protocols and hashing functions		• a quiz • an observation and evaluation of activities during the classes	• Lecture • Laboratory

Outcome description	Outcome symbols	Methods of verification	The class form
is capable of choosing cryptosystem parameters in order to mantain prescribed functions in data protection		• a discussion • a quiz • an observation and evaluation of activities during the classes	• Lecture • Laboratory
has knowledge of applications and threats of electronic signature		• a quiz • an observation and evaluation of activities during the classes	• Laboratory
Student knows the structure of the protection division in the organizational unit (enterprise), understands the tasks of employees of the protection division		• a quiz	• Lecture

Assignment conditions

Lecture - the condition for passing is to obtain positive grades from the knowledge tests in the written form, carried out at least once per semester
Laboratory - the condition to pass is the realization of at least 80% of the planned exercises
Components of the final grade = lecture: 50% + laboratory: 50%

Recommended reading

1. W. Stallings, Cryptography and Network Security Principles and Practices, Prentice Hall, 2018
2. S. McClure et al., Hacking Exposed: Network Security Secrets and Solutions, 2012
3. B. Halton et al., Kali Linux 2: Windows Penetration Testing, Packt, 2016
4. R. Boddington, Practical Digital Forensics, Packt, 2016

Further reading

1. Kutyłowski M., Strothmann W.B.: Kryptografia. Teoria i praktyka zabezpieczania systemów komputerowych, Oficyna Wydawnicza Read ME, Warszawa, 1998.

2. Russell R. i in. : Hakerzy atakują. Jak przejąć kontrolę nad siecią, Helion, 2004.

3. Potter B., Fleck B.: 802.11. Bezpieczeństwo, Wyd. O'Reilly, 2005.

4. Balinsky A. i in.: Bezpieczeństwo sieci bezprzewodowych, PWN, CISCO Press, 2007.

5. Mochnacki W.: Kody korekcyjne i kryptografia. Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 1997.

Notes

Modified by dr hab. inż. Bartłomiej Sulikowski, prof. UZ (last modification: 21-04-2022 12:15)