Óbuda University John von Neumann Faculty of Informatics			Institute for Cyber-Physical Systems	
Name and code: *IT Security NIEIB0EBNE*			**Credits*: 4***	
Computer Science and Engineering BSc programme			*2021/22 year II. semester*	
Subject lecturers: Zsolt Bringye, Ernő Rigó				
Prerequisites (with code):				
Weekly hours: 4	Lecture: 2	Seminar.: 0	Lab. hours: 2	Consultation: 0
Way of assessment:	written exam			

Course description:

Goal: During the semester the students get to know the most important aspects of computer and information Security. In the lab practices the students learn the working and usage of the most important security tools on an advanced level.

Course description:

Topics covered in lecture

- Introduction: Security: Feeling vs Reality; Most important concepts
- Cryptography
- Identification, Authentication and Authorization
- Risks, risk management

Topics covered in lab practice

- User awareness
- Cryptography
- Password management
- System hardening
- PGP, SSL

Homework (optional)

To give a deeper understanding of the material the students allowed to form groups of two and create a homework project during the semester which they will present at the end of the semester.

Lecture schedule	
Education week	*Topic*
1.	Lecture: Introduction. Lab: Introduction, getting to know the environment
2.	Lecture: Cryptography Lab: User awareness I. (web, e-mail, social media)
3.	Lecture: Cryptography (contd.) Lab: User awareness II. (public networks, malware, device security)
4.	Lecture: Cryptography (contd.) Lab: Cryptography I. (basic symmetric ciphers)
5.	Lecture: Identification and Authentication Lab: Cryptography II. (RSA, diffie-hellman)
6.	Lecture: Authorization Lab: Password management
7.	Lecture: Anatomy of risks Lab: Lab exam I.

8.	Lecture: Risk management Lab: Windows hardening
9.	Lecture: Break Lab: Linux hardening
10.	Lecture: Risk management (contd.) Lab: Firewalls
11.	Lecture: Misuse cases, security and software development Lab: Endpoint security, tracing
12.	Lecture: Laws and regulations (in a nutshell) Lab: PGP, e-mail security
13.	Lecture: Presentation of homework Lab: SSL, web security
14.	Lecture: Presentation of homework Lab: Lab exam II.

Midterm requirements

Education week	*Topic*
7	Lab materials between 1st and 6th weeks
14	Lab materials between 7th and 13th weeks

Final grade calculation methods

For a successful semester the students need to write both tests, achieve at least 40% of the score

Type of exam

Written exam. The final score consists of:
- the score of the lab exams (up to 20 points)
- the score of the exam (up to 80 points)
- optionally the score of the presentation (up to 20 points)

The requirement of the pass mark is 51 points.

Type of replacement

Once on the 14th week.

References

Mandatory: See in the e-learning system.

Recommended:
- Computer and Information Security Handbook by John R. Vacca; 3rd edition (2017)
- Security Engineering by Ross J. Anderson; 2nd Edition (2008)
- The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice by Jason Andress; 2nd Edition (2014)
- Applied Cryptography by Bruce Schneier; 20th Edition (2015)
- The Codebreakers by David Kahn (1996)