General Information:

Name of Course: **FOUNDATIONS OF INFORMATION SECURITY**

Course Code:	PMRRTNB237HA
Semester:	**6**th
Number of Credits:	3
Allotment of Hours per Week:	2 Lectures, 2 practical classes /Week
Evaluation:	Exam (with grade)
Prerequisites:	**Computer Networks II.**

Instructor: **Gábor GYURÁK, assistant lecturer**
Office: H-7624 Pécs, Boszorkány u. 2. Office N^{o} B-144
Office hours: Thursday 13:00-13:45
E-mail: gyurak@mik.pte.hu

Introduction, General Course Description:

This course is intended to help students gain fundamental and comprehensive understanding of information security. We will focus on an overview of major information security issues, technologies, and approaches. Students who successfully complete this course will have a concept and knowledge of security properties, concerns, policies, models, cryptography, PKI, firewalls, security evaluation, and real life security cases. Students will also have hands on experience in selected information security technologies through lab sessions.

Course aims:

- To provide an understanding of principal concepts, major issues, technologies, and basic approaches in information security.
- To provide concept level hands on experience in specific topic area.
- To provide the ability to examine and analyze real life security cases.

Learning Objectives:

Students who successfully complete this course will have a comprehensive overview of information security as well as more in depth understanding of a number of focus areas that they select throughout the course. Furthermore, students will have hands on experiences in information security. At the end of the semester, the students will be able to

- Harden servers and clients.
- Recognize common attack patterns.
- Evaluate vulnerability of an information system and establish a plan for risk manage-ment.
- Demonstrate how to detect and reduce threats in Web security.
- Evaluate the authentication and encryption needs of an information system.
- Explain the Public Key Infrastructure process.
- Demonstrate how to secure a wireless network.
- Evaluate a company's security policies and procedures.

Methodology:

- **Lectures**: discussion and lectures on IT security theory.
- **Practical class**: will give an introduction securely of planning, building, programming and operating IT systems.

Schedule:

Week	Lecture	Practical class
Week 1	Course introduction, orientation	CMS registration, laboratory guide
Week 2	Computer security concepts	Reconaissance
Week 3	Threats, attacks and assets	Scanning
Week 4	Defense strategies	Sniffing
Week 5	AAA model	Exploitation
Week 6	Symmetric cryptography	Web hacking
Week 7	***1st test***	
Week 8	Asymmetric cryptography	Management plane security
Week 9	*Spring break – no classes*	
Week 10	Digital signature	Firewalls I.
Week 11	Public Key Infrastructure	Firewalls II.
Week 12	Student presentations	
Week 13	Data center security	PKI
Week 14	***2nd test***	
Week 15	***Retake test or Pre-exam****	

* Pre-exam can be done during the Study Period in case the Student has met the requirements of the attendance and successfully performed the homework presentation.

Attendance:
Attending is required all classes, and will impact the grade (max. 10%). Unexcused absences will adversely affect the grade, and in case of absence from more than 30% of the total number of lesson will be grounds for failing the class. To be in class at the beginning time and stay until the scheduled end of the lesson is required, tardiness of more than 20 minutes will be counted as an absence. In the case of an illness or family emergency, the student must present a valid excuse, such as a doctor's note.

Evaluation + Grading:
The course grade is determined as a combination of study-period performance (attendance, tests, homework) and the final-exam (in some cases final-exam is replaceable with pre-exam).
All exams and tests are closed-book and closed-notes. A student with a proper excuse of being absent from the examination must inform and get a permission from the teacher prior to the time of examination. Any students who do not take the examination at the scheduled time will receive a zero score.

Grading will follow the course structure with the following weight:
10% - Class attendance, class activity
20% - 1st test
20% - 2nd test
10% - Homework
40% - Final Exam (or pre-exam)

Grade:	5	4	3	2	1
Evaluation in percent:	89%-100%	76%-88%	63%-75%	51%-62%	0-50%

PTE Grading Policy:
Information on PTE's grading policy can be found at the following location:
www.pte.hu

Students with Special Needs:

Students with a disability and needs to request special accommodations, please, notify the Deans Office. Proper documentation of disability will be required. All attempts to provide an equal learning environment for all will be made.

Readings and Reference Materials:

Required:

1. Presentation slides (Moodle CMS)
2. William Stallings, Lawrie Brown, Computer Security Principles and Practice, 2012, ISBN-13: 978-0-13-277506-9

More:

1. Chuck Easttom, Computer Security Fundamentals, 2006, ISBN: 0-13-171129-6
2. Randy Weaver, Dawn Weaver, Tactical Perimeter Defense: Becoming a Security Network Specialist, 2008, ISBN-13: 978-1-4283-5630-6
3. Mark Merkow, Jim Breithaupt, Information Security Principles and Practices, 2006, ISBN: 0-13-154729-1