Course Name : Security in Computer Networks

Course Code	Course Type	Regular Semester	Lecture (hours/week)	Seminar (hours/week)	Lab. (hours/week)	Credits	ECTS
CMP 409	B	Fall	3.00	1.00	0.00	3.50	6.00

Lecturer	Artur Koci, PhD
Assistant	Edlir Spaho, MSc
Course language	Albanian
Course level	Master
Description	Techniques for achieving security in multi-user computer systems and distributed computer systems: Basics of cryptography, network security applications and system security, conventional encryption and message confidentiality, public-key cryptography and message authentication, authentication applications. Electronic mail, IP, web, and network management security. Intruders, viruses, and firewalls.
Objectives	To understand the basic principles of computer network security. To analyze and apply cryptographic techniques for data protection. To evaluate threats and design protective mechanisms in a networked system.
Core Concepts	Symmetric and asymmetric cryptography Authentication protocols Firewalls and intrusion detection systems Network and application layer security Key management and PKI infrastructures

Course Outline

Week	Topic
1	Introduction and Computer Security Concepts
2	Cryptography - Symmetric Encryption and Message Confidentiality
3	Public-Key Cryptography and Message Authentication
4	Part II: Network Security Applications - Key Distribution and User Authentication
5	Network Access Control and Cloud Security
6	Transport-Level Security
7	Wireless Network Security
8	Midterm Exam
9	Electronic Mail Security
10	IP Security
11	Part III: System Security - Malicious Software
12	Intruders
13	Firewalls
14	Network Management Security
15	Legal and Ethical Issues
16	Final Exam

Prerequisites	The student must attend the course at a minimum rate of 75%.
Literature	• William Stallings – Network Security Essentials: Applications and Standards, 6th Edition, Pearson, 2017.
References	• Behrouz A. Forouzan – Cryptography and Network Security, McGraw-Hill, 2008. • Charlie Kaufman, Radia Perlman, Mike Speciner – Network Security: Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002. • Wenliang Du – Computer Security: A Hands-on Approach, 1st Edition, 2019.

Course Outcome

1	Students will understand the theoretical foundations of network security and cryptographic concepts.
2	They will apply protection techniques to prevent network attacks.
3	They will analyze threats and vulnerabilities in modern computer networks.
4	They will use protocols and security mechanisms in real-world applications.

Course Evaluation

In-term Studies	Quantity	Percentage
Midterms	0	0
Quizzes	0	0
Projects	0	0
Term Projects	1	60
Laboratory	0	0
Class Participation	0	0
Total in-term evaluation percent		**60**
Final exam percent		**40**
Total		**100**

ECTS Workload (Based on Student Workload)

Activities	Quantity	Duration (hours)	Total (hours)
Course duration (Including the exam week: 16x Total hours of the course)	16	4	64
Study hours outside the classroom (Preparation, Practice, etc.)	14	1	14
Duties	1	32	32
Midterms	0	20	0
Final Exam	1	40	40
Other	0	0	0
Total Work Load			**150**
Total Work Load / 25 (hours)			**6.00**
ECTS			**6.00**