CMPE455 Security of Computer Systems and Networks

Department: Computer Engineering

Instructor Information
Name: Assoc. Prof. Dr. Gürcü Öz
E-mail: gurcu.oz@emu.edu.tr
Office: CMPE 220
Office Tel: 1054

Program Name: Computer Engineering	**Program Code: 25**

Course Number: CMPE 455	**Credits:** (4,1) 4 Cr	**Year/Semester:** 2024-2025 Fall

☒ Required Course ☐ Elective Course (click on and check the appropriate box)

Prerequisite(s):
CMPE344 Computer Networks

Catalog Description:
Computer systems and network security requirements, security threats, and attacks. Confidentiality, integrity, availability, assurance, authenticity, anonymity, nonrepudiation. Access Control: Access control models, discretionary, mandatory, and role-based access models; Kerberos. Methods providing physical security, hardware, software, and information protection. Malicious software. Link, network, and transport layers security. Wireless network security.Symmetric and asymmetric cryptographic methods, DES, AES, RSA, ECC. Authentication, digital signature, certificates, one-time passwords, hash functions. Key management, Ethical and legal issues. Browser security. Operating systems security: process security (optional).

Course Web Page:
https://staff.emu.edu.tr/gurcuoz/en/teaching/cmpe455

Textbook(s):

1. Michael T. Goodrich, Roberto Tamassia, Introduction to Computer Security, 1st New International Edition, Pearson, 2014, ISBN 10: 1292025409
2. William Stallings, Cryptography and Network Security. Principles and Practices, 7th Edition, Pearson, 2018, ISBN 10: 1292158581

Indicative Basic Reading List :

Topics Covered and Class Schedule:
(4 hours of lectures per week)

Weeks 1-2	Introduction: Fundamental concepts. Computer systems and network security requirements, Confidentiality, integrity, availability, assurance, authenticity, anonymity, nonrepudiation. Security threats, and attacks. Cryptographic concepts. [1, Ch.1]
Week 2	Access control: Access control models, discretionary, mandatory, and role-based access models; Kerberos. [1, Ch. 1]
Weeks 3-4	Cryptography: Symmetric and asymmetric cryptographic methods(DES, AES, RSA, ECC). [1, Ch. 8], [2, Ch. 2(2.1-2.4), Ch. 3, Ch. 4(4.3-4.5), Ch. 5, Ch. 6,7,9,10]
Week 5-6	Authentication, Digital signature, Certificates, one-time passwords, Hash functions, Key management [1, Ch. 8], [2, Ch. 11]
Week 7	Physical Security: Methods providing physical security, Hardware protection [1, Ch. 2]
Weeks 8-9	Midterm Exams
Weeks 10	Network Security I: Network security concepts, Link layer, Network layer, Transport layer security [1, Ch. 5]
Weeks 11	Network Security II: Application layer and DNS, Tunneling, Wireless network security. [1, Ch. 6]

Weeks 12-13 Cryptography: Symmetric and asymmetric cryptographic methods(DES, AES, RSA, ECC). [1, Ch. 8], [2, Ch. 2(2.1-2.4), Ch. 3, Ch. 4(4.3-4.5), Ch. 5, Ch. 6,7,9,10]

Week 14 Malware: Software and information protection, Malicious software [1, Ch. 4]. Ethical and legal issues [1, Ch. 9]

Weeks 15-17 Final Exams

Laboratory Schedule:
(2 hours of laboratory per week, Tentative)

Weeks 3-5 **(7Oct -21Oct)**	Access control
Weeks 6-7	Cryptography (DES)
Weeks 11-13	Network Security
Weeks 14	Project presentation

Course Learning Outcomes

Upon successful completion of the course, students are expected to have the following competencies:

(1) Know computer systems and network security requirements, security threats, and attacks. Confidentiality, integrity, availability, assurance, authenticity, anonymity, nonrepudiation
(2) Know access control models discretionary, mandatory, and role-based access models
(3) Know methods providing physical security, hardware protection
(4) Know operating systems security, process security, memory and filesystem security, application program security
(5) Know software and information protection, malicious software
(6) Know link, network, and transport layers security.
(7) Know wireless network security. ,
(8) Know symmetric and asymmetric cryptographic methods, DES, AES, RSA, ECC
(9) Know authentication, digital signature, certificates, one-time passwords, hash functions, Key management.
(10) Development and Presentation of Project

	Method	No	Percentage
Assessment	Midterm Exam	1	35%
	Labs	3	10%
	Project	1	10%
	Final Exam	1	45%

Attendance and Participation: Attendance to every lecture is mandatory.

Policy on makeups:
- If you miss the midterm or the final exam and submit a written **medical report** to your instructor stating your excuse within 3 days of that examination, you will be able to take a makeup of the missed exam which will cover all the topics covered in the semester.

- If you miss both midterm and final exams and do not submit any written report, you will get an “NG” grade. In the same case, if you submit report for both missed exams, you will be able to enter make-up for one of them only.

- Re-sit exam may be taken according to its rules.

-There will be no makeup for the missed lab experiments. **If you miss three or more lab works, your lab grade will be zero.**

Policy on cheating and plagiarism: Any student caught cheating at the exams or assignments will automatically fail the course and may be sent to the disciplinary committee at the discretion of the instructor.

Contribution of Course to ABET Criterion 5
Credit Hours for:

Mathematics & Basic Science : 0
Engineering Sciences and Design : 4
General Education : 0

Relationship of the course to Student Outcomes

The course has been designed to contribute to the following student outcomes:

1. an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
2. an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
5. an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives

Prepared by: Gürcü Öz	**Date Prepared:** 23 September 2024