

CMPE455/CMSE456 Security of Computer Systems and Networks		
Department: Computer Engineering		
Instructor Information Name: Prof. Dr. Gürcü Öz E-mail: gurcu.oz@emu.edu.tr Office: CMPE 220 Office Tel: 1054		
Program Name: Computer/Software Engineering		Program Code: 25/29
Course Number: CMPE 455/CMSE456	Credits: (4,1) 4 Cr	Year/Semester: 2026-2027 Fall
☒ Required Course ☐ Elective Course (click on and check the appropriate box)		
Prerequisite(s): CMPE344/CMSE344 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. Symmetric and asymmetric cryptographic methods, DES, AES, RSA, ECC. Authentication, digital signature, certificates, one-time passwords, hash functions. Key management, Link, network and transport layers security. Wireless network security. Browser security. Ethical and legal issues. 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, 1 st New International Edition, Pearson, 2014, ISBN 10: 1292025409 2. William Stallings, Cryptography and Network Security. Principles and Practices, 7 th Edition, Pearson, 2018, 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], Physical Security: Methods providing physical security, hardware protection [1, Ch. 2] 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] Weeks 5-6 Authentication, digital signature, certificates, one-time passwords, hash functions. Key management [1, Ch. 8], [2, Ch. 11] Weeks 6-7 Midterm Exams Week 8 Network Security I: Network security concepts, Link layer, Network layer, Transport layer security [1, Ch. 5] Weeks 9-12 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]		

Weeks 10-12 Network Security II: Application layer and DNS, Tunneling, Wireless network security. [1, Ch. 6]

Weeks 14-15 Malware: Software and information protection, Malicious software [1, Ch. 4]. Ethical and legal issues [1, Ch. 9]

Weeks 16-17 Final Exams

Laboratory Schedule:

(2 hours of laboratory per week, Tentative)

Weeks 3-4 (05Oct -17Oct) Access control acquaintance

Weeks 5-6 (19Oct -28Oct) Cryptography (DES)

Weeks 10-12 (23Nov -12Dec) Network security

Weeks 14-15 (21Dec -30Dec) 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; Kerberos.
- (3) Know symmetric and asymmetric cryptographic methods, DES, AES, RSA, ECC
- (4) Know authentication, digital signature, certificates, one-time passwords, hash functions. Key management
- (5) Know Methods providing physical security, hardware protection
- (6) Know link, network, and transport layers security.
- (7) Know wireless network security, browser security
- (8) Know Software and information protection, malicious software, Ethical and legal issues
- (9) Develop a Secure Network Application for Term Project
- (10) Make Presentation for Final Project status with demo

Assessment	Method	No	Percentage
	Midterm Exam	1	35%
	Labs	3	10%
	Project	1	15%
	Final Exam	1	40%

Attendance and Participation: Attendance is taken in every lecture. **You should have regular attendance to the lectures for being successful in the course.** Course related materials, exercises, laboratory experiments, old exam questions and announcements will be published on the course web site and you will be responsible from all. Note that the course web site can update during the semester. Therefore, please check it regularly.

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.

Policy on labs:

- 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 conduct that attempts to gain unfair academic advantage is considered academic dishonesty. Copying labs and assignments, cheating during exams, substituting for another person are some examples of academic dishonesty. Cases of academic dishonesty will not be tolerated and will be punished according to EMU's disciplinary policies. **Also, on the grounds of reasonable doubt, the instructor reserves the right to invite students to an oral examination for further verification of knowledge, and this may be used as a basis for assigning a grade.**

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: 22 September 2026