

<b>CMPE455/CMSE456 Security of Computer Systems and Networks</b>		
<b>Department:</b> Computer Engineering		
<b>Instructor Information</b> <b>Name:</b> Prof. Dr. Gürcü Öz <b>E-mail:</b> gurcu.oz@emu.edu.tr <b>Office:</b> CMPE 220 <b>Office Tel:</b> 1054		
<b>Program Name:</b> Computer Engineering	<b>Program Code:</b> 25	
<b>Course Number:</b> CMPE 455	<b>Credits:</b> (4,1) 4 Cr	<b>Year/Semester:</b> 2025-2026 Fall
<input checked="" type="checkbox"/> Required Course <input type="checkbox"/> Elective Course     (click on and check the appropriate box)		
<b>Prerequisite(s):</b> CMPE344/CMSE356 Computer Networks		
<b>Catalog Description:</b> 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).		
<b>Course Web Page:</b> <a href="https://staff.emu.edu.tr/gurcuoz/en/teaching/cmpe455">https://staff.emu.edu.tr/gurcuoz/en/teaching/cmpe455</a>		
<b>Textbook(s):</b>  1. Michael T. Goodrich, Roberto Tamassia, Introduction to Computer Security, 1 <sup>st</sup> New International Edition, Pearson, 2014, ISBN 10: 1292025409 2. William Stallings, Cryptography and Network Security. Principles and Practices, 7 <sup>th</sup> Edition, Pearson, 2018, ISBN 10: 1292158581		
<b>Indicative Basic Reading List :</b>		
<b>Topics Covered and Class Schedule:</b> <b>(4 hours of lectures per week)</b> <b>Weeks 1-2</b> 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] <b>Week 2</b> Access control: Access control models, discretionary, mandatory, and role-based access models; Kerberos. [1, Ch. 1] <b>Weeks 3-4</b> 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] <b>Weeks 5-6</b> Authentication, digital signature, certificates, one-time passwords, hash functions. Key management [1, Ch. 8], [2, Ch. 11] <b>Week 7</b> Physical Security: Methods providing physical security, hardware protection [1, Ch. 2] <b>Weeks 7-9</b> <b>Midterm Exams</b> <b>Week 10</b> Network Security I: Network security concepts, Link layer, Network layer, Transport layer security [1, Ch. 5] <b>Weeks 11-13</b> 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]		

<b>Week 14</b>	Network Security II: Application layer and DNS, Tunneling, Wireless network security. [1, Ch. 6]
<b>Week 15</b>	Malware: Software and information protection, Malicious software [1, Ch. 4]. Ethical and legal issues [1, Ch. 9]
<b>Weeks 16-18</b>	<b>Final Exams</b>

#### Laboratory Schedule:

(2 hours of laboratory per week, Tentative)

**Weeks 4-5 (13Oct -24Oct)** Access control acquaintance

**Weeks 6-7** Cryptography (DES)

**Weeks 11-13** Network security

**Week 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; 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

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

**Attendance and Participation:** Attendance is taken every lecture. Those missing more than **20%** of classes without valid excuse may get NG grade

#### 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.**

<p><b>Policy on cheating and plagiarism:</b> 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.</p>	
<p><b>Contribution of Course to ABET Criterion 5</b> Credit Hours for:</p> <p>Mathematics &amp; Basic Science : 0 Engineering Sciences and Design : 4 General Education : 0</p>	
<p><b>Relationship of the course to Student Outcomes</b></p> <p>The course has been designed to contribute to the following student outcomes:</p> <ol style="list-style-type: none"> <li>1. an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics</li> <li>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</li> <li>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</li> </ol>	
<p><b>Prepared by:</b> Gürcü Öz</p>	<p><b>Date Prepared:</b> 22 September 2025</p>