|  |  |  |  |
| --- | --- | --- | --- |
| **CMSE456/ CMPE455 Security of Computer Systems and Networks** | | | |
| **Department:** FORMTEXT Computer Engineering | | | |
| **Instructor Information**  **Name:** Assoc. Prof. Alexander Chefranov  **E-mail:** Alexander.chefranov@emu.edu.tr  **Office:** CMPE 219  **Office Tel:** 1190 | | | |
| **Assistant Information**  TBD | | | |
| **Meeting times and places**  Tuesday 8:30-10:20, Room CMPE 128  Thursday 12:30-14:20, Room CMPE 134 (Labs)  Friday 8:30-10:20, Room CMPE 028 | | | |
| **Program Name:** Computer Engineering | | **Program Code: 29/25** | |
| **Course Number:**  CMPE 455 | **Credits:**  (4,1) 4 Cr | | **Year/Semester:**  2024-2025 Spring |
| FORMCHECKBOX   Required Course          FORMCHECKBOX   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. Methods providing physical security, hardware, software, and information protection. Access control models, discretionary, mandatory, and role-based access models; Kerberos. 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 | | | |
| **Course Web Page:**  <https://staff.emu.edu.tr/alexanderchefranov/en/teaching/cmse456/> | | | |
| **Textbook(s):**   1. Michael T. Goodrich, Roberto Tamassia, Introduction to Computer Security, International Edition, Pearson, 2011, 541 p., ISBN 10: 0-321-70201-8; ISBN 13: 978-0-321-70201-2 2. William Stallings, Cryptography and Network Security. Principles and Practices, 5th Edition, Pearson, 2011, 721 p., ISBN 10: 0-13-609704-9, ISBN 13: 978-0-13-609704-4 | | | |
| **Indicative Basic Reading List :** No | | | |
| **Topics Covered and Tentative Class Schedule:**  **(4 hours of lectures per week)**   |  |  |  | | --- | --- | --- | | **Week 1** | Computer systems and network security requirements, security threats, and attacks. Confidentiality, integrity, availability, assurance, authenticity, anonymity, nonrepudiation. [1, ch. 1] | | | **Weeks 2-3** | Access control models, discretionary, mandatory, and role-based access models; Kerberos. [1, ch. 9] | | | **Weeks 4-5** | Symmetric and asymmetric cryptographic methods, DES, AES, RSA, ECC. Authentication, digital signature, certificates, one-time passwords, hash functions. Key management [1, ch. 2], [2, ch. 10] | | | **Weeks 6-7** | Methods providing physical security, hardware protection [1, ch. 8] | | | **Weeks 8-9** | Problem sessions. Midterms. | | | **Week 10** | Midterms, | | | **Weeks 11-12** | Link, network, and transport layers security. Wireless network security. Browser security. [1, ch. 5-7], | | | **Week 13** | | Software and information protection.[1, ch. 3]. Malicious software [1, ch. 4]. Ethical and legal issues [1, , 8.4.5, 10.4] | | **Weeks 15-17** |  | Final Exams | | | | |
|  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Laboratory Schedule:**  **(2 hours of laboratory per week, Tentative)**   |  |  | | --- | --- | | **Weeks 4-5** | Access control acquaintance | | **Weeks 6-7** | 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 ccomputer 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(s) | 1 | | 30% |
| Attendance |  | | 0 % |
| Labs | 4 | | 10% |
| Project | 1 | | 20 % |
| Final Examination | 1 | | 40% |
| **Computation of the attendance grade:** Attendance is taken every lecture and entered to EMU portal. Those missing more than 20% of classes without valid excuse may get NG grade | | | | |
| **Policy on makeups:** If you miss a midterm or final exam, you can take a make-up exam (for the midterm or final exam) if you have valid excuses (e.g., you are sick) and provide material evidence for it (e.g., a doctor’s report which must be issued/approved by EMU Health Center) within 3 working days of the exam. Resit exam may be taken according to its rules. | | | | |
| **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:** Prof. Dr. Alexander Chefranov | | | **Date Prepared:** 20 February 2025 | |
|  |  |  |  |  |