Course Syllabus	**EECS 4980 – Fundamentals of Cybersecurity**
Credits & Contact Hours	3 credit hours & 150 minutes lecture contact hours per week
Coordinator	Dr. Ahmad Y Javaid
Textbook(s)	1. Ross Anderson, Security Engineering. 2nd Edition. John Wiley and Sons. 2008, ISBN-13: 978-0470068526, Required. 2. Charles P. Pfleeger, Security in Computing, 5th Edition, Prentice Hall, 2015, ISBN-10: 0134085043, Recommended.
Course Information	This course introduces the concept of cyber security, its interdisciplinary nature and its relation to nation, businesses, society and people. Participating students would gain knowledge of various cyber security terminologies, technologies, protocols, threat analysis, security principles, security mechanisms, policies, forensics, incidence response and methods/practices to secure systems. Prerequisites: EECS 1500 or EECS 1510 Elective Course
Specific Goals-Student Learning Objectives	Upon successful completion of the course, the students will have: 1. Reasonable understanding of the fundamentals of the cyber-security domain and related issues 2. Practical knowledge of various tools, processes and methods to ensure security of systems through a minimum of two hands-on assignments involving attack and protection in a virtual environment 3. An understanding of the inter-disciplinary nature of cyber-security domain 4. Adequate level of cross-disciplinary knowledge of design, implementation, evaluation and testing of secure protocols, systems or applications 5. Basic knowledge to be able to build bug-free systems, dependable during malice or error 6. Foundational skills for developing expertise in one or more sub-domains of cyber-security 7. Foundational skills and knowledge of impact of security on economics, legal, business, warfare and social domains 8. Effective communication skills through an in-class project along with a presentation and project report

Topics

1. Introduction, Psychology, Usability, Thinking like a Hacker
2. CIA Triad, Security Terminologies, Security Protocols
3. Security Policies and Management, Multilevel and multilateral Policies, Security Mechanisms
4. Security Design Principles, Threat Analysis and Risk Assessment, Securing a System
5. Cryptography, Basic Techniques, Digital Signatures, Cryptanalysis
6. Software Security, Low-level attacks, Code Review and Testing, Defenses
7. Fall-Break, Student Project Idea Discussion
8. Network Security, Vulnerabilities, Attacks, Defenses
9. Internet and Smartphone Security, Anonymous vs Secure Browsing
10. Information Economics, Economics of Security, Physical Protection, Biometrics
11. Banking Security, Cyber Forensics, Cyber Warfare, Surveillance and Privacy
12. Incident Response and Mitigation, Business Continuity, Legal issues and Ethics