ENEE457: Computer Systems Security

Credits: 3

Description

Prerequisite: Minimum grade of C- in ENEE350; and permission of ENGR-Electrical & Computer Engineering department.

Restriction: Must be in one of the following programs (Engineering: Electrical; Engineering: Computer) ; and permission of ENGR-Electrical & Computer Engineering department.

Credit only granted for: CMSC414, ENEE459C or ENEE457.

Formerly: ENEE459C.

Theoretical and practical aspects of computer systems security. Topics covered include symmetric/asymmetric encryption, message authentication, digital signatures, access control, as well as network security, web security and cloud security. Students acquire tools necessary for designing secure computer systems and programs and for defending against malicious threats (e.g., viruses, worms, denial of service).

Semesters Offered

Fall 2017, Fall 2018, Fall 2019, Fall 2020

Testudo

Learning Objectives

- Understand the mathematics foundations of modern cryptography
- Get familiar with the modern cryptosystems
- Understand the major topics in system security
- Ability to analyze the security of a network
- Learn the basics and industry practice on digital right management
- Understand the security and trust issues in software
- Understand the security and trust issues in hardware

Topics Covered

- Cryptography basics: ciphers, cryptanalysis, modern cryptosystems (DES, AES, RSA), public key cryptography (encryption/decryption, digital signature, key exchange)
- System security: intruders, viruses, malicious programs, Trojan horse; intrusion detection, password protection, firewall; case study on UNIX system

- Network security: authentication (Kerberos and X.509), E-mail security (PGP and S/MIME), IP security, Web security (SSL and SET), access control, endpoint security standards (NAC, TNC)
- Digital right management: copyright, patent, trade secrets, trademark; legal protection of users, fair use, fared use, P2P system, digital watermarking, DRM software and hardware, privacy on the web, case study
- Hardware based trust and security: trusted platform module, storage protection, trusted software stack, hardware assisted security systems, trusted IC and hardware
- Trusted software: hacking, software reliability, writing secure code