# ENEE 459-C: Computer Security

# Fall 2014

**Course description:**
Computer systems have become a vital part of our everyday professional and personal life and are being used for several critical tasks (e.g., online banking, social networking). These tasks can however expose the users to various security threats (e.g., credit card number theft, personal information leakage). Therefore there is a need for designing secure computer systems.

This course teaches both theoretical and practical concepts of computer systems security. It covers symmetric/asymmetric encryption, message authentication, digital signatures, access control, as well as network security, web security and cloud security. The class will provide the students with the necessary tools for designing secure computer systems and programs and for defending against malicious threats (e.g., viruses, worms, denial of service).

**Course prerequisites:**
ENEE 150 or CMSC132 or permission of the instructor.

**Topic prerequisites:**
Knowledge of programming and basic knowledge of algorithms and data structures.

**Core topics:**

1. Introduction to computer security (threat model, attacks, defenses).
2. Basic tools in computer security (symmetric and asymmetric encryption, message authentication, digital signatures, access control).
3. Security protocols (key exchange, secure and private communication, anonymous communication).
4. Systems security (permissions in Windows/Unix, buffer overflow, password-based authentication).

5. Cloud security (authenticated data structures, verifiable computation, homomorphic encryption).
6. Network security (basic internet technology, DNS, denial of service, WiFi security).
7. Web security (XSS attacks, browser vulnerabilities, SQL injection attacks)
8. Applications security (digital rights management (DRM), email security, e-cash).
9. Malicious software (backdoors, viruses, worms, rootkits, static and dynamic analysis).

**Grading policy:**
Class participation: 10%
5 Homeworks: 40%
Midterm exam: 20%
Final exam: 30%

**Readings:**
Slides and selected research papers will be provided.

**References:**

1. Introduction to Computer Security (Goodrich and Tamassia, Addison Wesley, 2011).
2. Introduction to Modern Cryptography (Katz and Lindell, Chapman & Hall/CRC, 2007).
3. Handbook of Applied Cryptography (Menezes, van Oorschot, Vanstone, CRC press, 1996).