
Course Objectives. This course provides an overview of computer security principles, ranging from cryptography to network security, to operating systems and software security. Specific objectives include: (1) Knowledge of the fundamental goals of Information Security (confidentiality, integrity, availability), and experience achieving them using cryptography; (2) Understanding of the relative advantages of symmetric vs. public-key cryptography; (3) Ability to analyze existing protocols and design new variants; (4) Knowledge of network security threats (spoofing, snooping, DoS) and defenses (SSL/TLS, SSH, firewalls); (5) Understanding of the fundamentals issues in web privacy (threats and defenses); (6) Knowledge of software security threats (viruses, worms, covert channels), and of the specifics of common implementation flaws (buffer overflows, TOCTTOU bugs); (7) Knowledge of access control policies (DAC, MAC, RBAC) and basic authentication mechanisms in mainstream Operating Systems.


Recommended Texts.

Required Software. Libdcrypt C crypto library (http://www-es.ccny.cuny.edu/~fazio/F11-csc48000/lab0/install-libs.html).


Major Topics Covered in the Course. Introduction to Computer Security: Basic concepts (vulnerabilities, threat models, adversaries, security goals). Cryptography: Information security goals (secrecy, integrity, authentication); Basic primitives (cryptographic hash functions, one-way functions); Symmetric primitives (encryption, message authentication codes); Public-key primitives (asymmetric encryption, digital signatures) Cryptographic protocols (key exchange, key distribution, authentication). Network Security: Basics of computer networks; Network security threats (viruses, worms, spoofing, snooping, denial of service); Network security defenses (SSL/TLS, SSH, firewalls, intrusion detection systems); Web privacy threats and defenses. Operating Systems Security: Resource separation and memory protection; Access control, authentication and authorization; Audit logs and accountability. Software Security: Buffer overflow and other implementation flaws; Isolation and sandboxing techniques; Software engineering best practices (defensive programming, fail-safe defaults, least-privilege, and privilege-separation principles). Additional Topics: Content protection, anonymity and privacy, e-voting, e-cash, e-
commerce.

**Homework.** Projects will be written in C, based on the Libdencrypt crypto library. Programming labs will be assigned to help students explore computer security concepts first hand and learn how to implement basic cryptographic tools and simple protocols (*e.g.*, encryption/decryption utility; man-in-the-middle attacks).

**Grading.** Class participation (10%), Programming Labs (40%), Midterm & Final exams (50%). The global exams grade will be computed as follows:

```
   exmGrade = max(finalGrade, avg(midGrade, finalGrade))
```

**Course webpage.** [http://www-cs.ccny.cuny.edu/~fazio/F11-csc48000/](http://www-cs.ccny.cuny.edu/~fazio/F11-csc48000/)

**Lectures.** Tuesdays and Thursdays, 6:30-7:45pm. NAC 7219.

**Office Hours.** Thursdays, 3:00-4:00pm. Shepard Hall 279.