EE 406 Introduction to Computer and Network Security

Credits: 3

Categorization of credits: engineering topic

Instructor(s): Yingfei Dong. Revised Jan. 8th, 2021.

Textbook and Other Required Materials:

Introduction to Computer Security, M. T. Goodrich and R. Tamassia, Addison Wesley, ISBN-13:978-0-321-51294-9, ISBN-10: 0-321-51294-4, 2011.

Computer Security: A Hands-on Approach, 1st Edition. Wenliang Du. ISBN-10: 154836794X, ISBN-13: 978-1548367947, CreateSpace Independent Publishing Platform, Oct, 2017.

Handouts/Notes and Supplemental Text: will be available on-line or distributed in classes**.**

Designation: Technical Elective

Catalog Description:

We will discuss basic computer and network security issues in this course. We will first review basic cryptography concepts and theory. We will then introduce computer system security issues. We will further introduce network security concepts, algorithms and protocols for TCP/IP security, DNS security, wireless security, Web security, firewalls, etc. We will also introduce a few advance security topics. In particular, we will use multiple hands-on labs to emphasize some critical issues in computer system security, cryptography, and network security.

Pre- and Co-requisites: EE367 or equivalent.

Class/Lab Schedule: 3 lecture hours per week.

Topics Covered:

- Basic Computer Security Concepts, Technologies, and Principles
- Basics of cryptography:
    1. basic number theory
    2. symmetric encryption
    3. public-key encryption and certificates,
    4. cryptographic hash functions,
    5. pseudo-random number generators
- Computer System security
    1. Access Control: SETUID, buffer overflow attacks
    2. Authentication and key establishment
    3. Malicious software, Internet worms, viruses,
- Network Security basics

1. TCP/IP security: ARP, IP, TCP, DNS attacks, and Transport Layer Security (TLS)
2. Web security
3. Wireless security
4. Denial of service attacks on routing infrastructure
5. Firewalls and intrusion detection systems

- Other Advanced security topics:
  1. Distributed Authentication and key establishment: e.g., blockchain
  2. anonymous communication and sharing,
  3. data and network privacy

Grading: Homework, Projects, Quizzes 50%, midterm exam 20%, final exam 30%

Course Objectives and Their Relationship to Program Objectives:

The students apply the theory of probability and statistics for security analysis that can also be applied on other engineering applications in communications, control, networking, electrophysics and computers. Students also learn low-level deeper computer system skills to enhance their understanding of system design and performance. Class labs will lead students to conduct a series of self-learning explorations. Students will also learn the impacts of security and privacy on our society and make them think about the conflicts between engineering solutions and cultures. [Program Objectives this course addresses: 1, 2, 3, and 5.]

Course Outcomes and Their Relationship to Program Outcomes:

The following are the course outcomes and the subset of Program Outcomes (numbered 1-7 in square braces "[ ]") they address:

- Use of mathematics (probability, statistics, discrete math, basic graph theory,) to understand the theory behind modern cryptography. [1,4,6]
- Develop the ability to model engineering systems [1,6,7]
- Enhance the student's ability to design an experiment and to analyze the resulting data [1,6,7]
- Emphasize the societal issues and advance of technology affecting the design secure systems [4]

Contribution of Course to Meeting the Professional Component

Computer System, computer networks

Computer Usage:

Heavy computer usage is required. C programming and UNIX system programming are used in assignments. Students will use NSF SEED project labs and work on Ubuntu virtual machines to perform hands-on experiment for understanding computer systems and attack techniques.

Design Credits and Features: EE406 has 1 design credits.