CSE 4095: Network Security

Spring 2017

January 16, 2017

1 Administrative

Description This courses teaches the security mindset and introduces the principle and practices of how to provide secure communication between computer systems. It includes protection techniques at the physical, network, transport layers, and major approaches in Internet security.

This class will briefly introduce concepts from cryptography in the context of how they are applied to network security. Topics include: denial-of-service, DNS, BGP, IPSec, SSL/TLS, Authentication, VPNs, PKI, firewalls, intrusion detection/prevention systems, blockchain, and wireless security.

Contact This course will be co-taught by Professors Benjamin Fuller and Bing Wang.

Benjamin Fuller, benjamin.fuller@uconn.edu, 6-2122, ITE room 243. Office hours: Tuesday 11-12, Wednesday 1-2pm.

Bing Wang, bing@uconn.edu, 6-0582, ITE (Information Technologies Engineering) room 367. Office hours: Office Hours: Monday 11-12, Thursday 11-12

Any changes to office hours will be posted on HuskyCT. We encourage attending office hours. If you cannot make office hours, please ask technical questions on HuskyCT or email both instructors to make appointments.

Lecture and Notes The class meets in E2 (Engineering II) room 322 on Tuesdays and Thursdays from 9:30-10:45am.

Lecture attendance is highly encouraged. The course will be interactive and discussions may not be captured in posted materials. We will not follow any text; class is the best resource to learn the material. In addition, periodic in-class quizzes will provide extra credit to students.

Textbook We will generate post class materials during the semester that will contain the major ideas and concepts. We will not follow any particular textbook. Some relevant materials that may be useful during the semester:

- Security Engineering by Ross Anderson is completely available online.
- Computer Security: Principles and Practice by William Stallings and Lawrie Brown.

Several books consider more practical aspects of implementing cryptography. These include:

- Handbook of Applied Cryptography by Alfred Menezes, Paul van Oorschot and Scott Vanstone
- Applied Cryptography by Bruce Schneier

Communication The class materials and projects will be posted on the course web site at: class web site. Announcements and discussion will be done on HuskyCT. Please ensure you receive emails from HuskyCT so you get announcements. In addition, we encourage students to post and answer questions about lecture and projects. We will also answer questions but have less availability than students. **Do not directly ask or solve project questions. If you are worried your question or answer is major piece of the solution, directly ask the instructors.**

Personal questions should be directly to our emails or handled in person during office hours.

Grading, assignments and exams There will be six projects throughout the semester, four of these projects will be practical and two will be written assignments. The practical assignments should be submitted through HuskyCT, the written assignments should be submitted on HuskyCT. Typed submissions are preferred, handwritten assignments may also be scanned and submitted. Students may use up to seven late days throughout the semester with no explanation needed. These days will be automatically deducted if a project is submitted late.

There will be a final exam to be scheduled by the registrar. There will be no midterm.

The class will be graded as follows:

- 70% projects.
- 30% final exam.
- 3% extra credit for in class quizzes.

The last day to drop a class without a 'W' is Monday, January 30. The last day to drop a class with a 'W' or convert to pass/fail is March 27. Since there will not be an exam before that date, mid semester evaluations will be based on project completion.

Collaboration The projects in this class are designed to measure your individual performance. Students should not consult with each other or outside materials for solutions to the projects. This includes using the Internet to solve the problem. Using public resources such as Wikipedia for background is permitted. Students should not seek solutions either through searching or asking a question on any forums.

Students may ask technical questions to each other or using HuskyCT. An example of a permitted question is requesting help in setting up a required program or asking suggestions on helpful resources. Bad questions include asking for code or a technique to solve the project. If you come across some resources that you think will benefit the class, posting it on HuskyCT or letting the instructors know will be highly appreciated.

On the final exam, students are not permitted any outside materials.

Ethics To defend a system you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law or the university's rules, and it may be unethical. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including expulsion, civil fines, and jail time. Our policy is that you must respect the privacy and property rights of others at all times, or else you will fail the course.

Any time you are being asked to "attack" a system it will be owned by the Instructors and you will have explicit permission to perform this action.

Acting lawfully and ethically is your responsibility. Carefully read the Computer Fraud and Abuse Act (CFAA), a federal statute that broadly criminalizes computer intrusion. This is one of several laws that govern "hacking." Understand what this law prohibits.

Academic Honesty The collaboration policy described above is designed to allow students the resources to succeed while ensuring they learn and master the material. If you are unsure if something is acceptable according to the collaboration policy, talk to one of us!

Violations of this policy will be considered violations of the academic integrity policy and will be reported to the Academic Integrity Hearing Board. Consequences may include (but are not limited to) failure of the class. Example violations include: jointly solving a project, copying or plagiarizing solutions from other sources, and cheating on the exam.

2 Course contents

This course will focus on network security through the lens of the multiple layers of the network stacks. We will start with basic cryptography, which is the foundation of network security. We will then do a bottom-up approach, going over security at MAC layer, network layer, transport layer and application layers.

Tentative Class Schedule Table 1 contains a tentative plan for the course topics. We'll adjust the schedule as needed.

Class	Topic
1/17	Class overview, the attack mindset.
1/19	Symmetric cryptography (ciphers and MACs)
1/24	Asymmetric/Public Key Cryptography
1/26	Hash functions
1/31	What is authentication and identity?
2/2	Public Key Infrastructure and Certificates
2/7	Wireless networks
2/9	WEP Protocol
2/14	WPA and WPA2 wireless protocols
2/16	IPSec
2/21	IPSec continued
2/23	BGP
2/28	Attacking and securing BGP
3/2	TCP Security
3/7	TLS Basics
3/9	The TLS Handshake
3/21	The history of TLS
3/23	Recent attacks on TLS (and TLS 1.3)
3/28	DNS
3/30	Attacking DNS
4/4	Defending DNS
4/6	Denial of Service (DOS)
4/11	Distributed Denial of Service
4/13	Network defenses (intrusion detection/prevention, firewalls)
4/18	Network defenses continued
4/20	What is a blockchain?
4/25	Applications of blockchains
4/27	Semester Review

Table 1: Tentative class schedule.