NYU TANDON SCHOOL OF ENGINEERING

Course Syllabus

Computer Science and Engineering

CS-GY 6823 -Network Security

Course Information

Course Pre-requisites

- Good working knowledge of networking and TCP/IP (e.g., CS 6843, EL5363/5373)
- Basic understanding of operating systems with a working knowledge of Linux (e.g., CS6233)

Course Description

This course begins by covering attacks and threats in computer networks, including network mapping, port scanning, sniffing, DoS, DDoS, reflection attacks, attacks on DNS and leveraging P2P deployments for attacks. The course continues with cryptography topics most relevant to secure networking protocols. Topics covered are block ciphers, stream ciphers, public key cryptography, RSA, Diffie Hellman, certification authorities, digital signatures and message integrity. After surveying basic cryptographic techniques, the course examines several secure networking protocols, including PGP, SSL, IPsec and wireless security protocols. The course examines operational security, including firewalls and intrusion-detection systems. Students read recent research papers on network security and participate in an important lab component that includes packet sniffing, network mapping, firewalls, SSL and IPsec.security and participate in an important lab component that includes packet sniffing, network mapping, firewalls, SSL and IPsec.

Upon completion of this course you will have acquired the following knowledge:

- Understand hacking techniques.
- Understand the fundamentals of secure network design.
- Understand the issues involved with providing secure networks.
- Understand underlying cryptography required for secure communications, authorization and authorization.

- Obtain hands on experience in cryptography and network security through laboratory work.

Course Structure

This course is conducted entirely online, which means you do not have to be on campus to complete any portion of it. You will participate in the course using NYU Classes located at https://newclasses.nyu.edu.

Grading Breakdown

- 30% Labs
- 35% Midterm
- 35% Final

Points to Letter Grade Mapping:

Grade	Minimum %
A	95
A-	90
B+	87
B	83
B-	80
C+	77
C	73
C-	70
F	Below

Weekly Structure

Week 1	Lesson 0: Introduction, Expectations, and Policies Lesson 1: Security Basics: Terms & Definitions, Risk Assessment
Week 2	Lesson 2: Recon
Week 3	Lesson 3: Vulnerabilities and Exploits Part I
Week 4	Lesson 3: Vulnerabilities and Exploits Part II
Week 5	Lesson 4: Attacks - Owning the Box, Post-Exploitation
Week 6	Lesson 5: Cryptography - Randomness, Primes, RSA, DH MIDTERM on Lessons 1-5 Only
Week 7	Lesson 6: Message Integrity, PKI and TLS Part I
Week 8	Lesson 6: Message Integrity, PKI and TLS Part II
Week 9	Lesson 7: Layer 2 Security

	Lesson 8: IPSec, Firewalls, and IDS

Week 10	Lesson 9: Authentication
Week 11	Lesson 10: Wireless Security
Week 12	Lesson 11: IPv6 Security
Week 13	Final Review
Week 14	FINAL EXAM on Lesson 6-11

Learning Time Rubric

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Lecture (Active Module)	Asynchronous	2 - 3 hours	Video and interactive text format. Expect quizzes throughout the module.
Discussions	Asynchronous	0.5 hours	Students discuss instructor's questions for each lesson.
Reading	Asynchronous	1.5 hour	Students complete recommended readings (online journal articles and tutorials).
Assignments	Asynchronous	1.5 hours	Students will read assignments and watch guided solutions. Students will submit a short write-up (1-2 paragraph) of what they learned

Course Communication

The Teaching Assistant (TA) will be available for weekly virtual office hours by appointment. To schedule an appointment with your TA, or to ask any questions about the course content, please post to the discussion forms in NYU Classes.

Questions About the Course & Contacting the Instructor

To schedule an appointment with your TA, or to ask any questions about the course content, please post to the discussion forms in NYU Classes.

Readings

RECOMMENDED READINGS are online journal articles provided in each lecture You can access NYU's central library here: http://library.nyu.edu/

You can access NYU Tandon's Bern Dibner Library here: http://library.poly.edu/

Assignments and Exams

Exams Administered and Proctored Online

Exams in this course are administered through NYU Classes. You are required to arrange an online proctor for your exams via ProctorU. More information on ProctorU and scheduling proctoring sessions can be found on Tandon Online's website.

Exams Administered On Paper and Proctored Remotely

Exams in this course are administered via paper and pencil. If you are not able to attend an exam session on-campus, you are required to secure in-person proctoring arrangements near your location. Tandon Online's website

---

Course Schedule

Week 1

Weekly learning objectives:

- Lesson 0: Introduction, Expectations, and Policies
- Lesson 1: Security Basics: Terms & Definitions, Risk Assessment

Readings:

Lesson 1 Readings

Assignments:

- Complete: Lab 1

Week 2

Weekly learning objectives:

- Lesson 2: Recon

Readings:

- Read: Lesson 2 Readings

Assignments:

- Complete: Lab 2

Week 3:

Weekly learning objectives:

- Lesson 3: Vulnerabilities and Exploits Part I

Readings:

- Read: Lesson 3 Readings

Assignments:

- Complete: Lab 3

Week 4:

Weekly learning objectives:

- Lesson 3: Vulnerabilities and Exploits Part II

Readings:

- Read: Lesson 4 Readings

Assignments:

- Complete Lab 4

Week 5:

Weekly learning objectives:

- Lesson 4: Attacks - Owning the Box, Post-Exploitation

Readings:

- Read: Lesson 5 Readings

Assignments:

Complete: Lab 5

Week 6: Topic

Weekly learning objectives:

- Lesson 5: Cryptography - Randomness, Primes, RSA, DH

Readings:

- Read: Lesson 5 Readings

Assignments:

Complete: Lab 5

Week 7:

Weekly learning objectives:

- Lesson 6: Message Integrity, PKI and TLS Part I

Readings:

- Read: Lesson 6 Readings

Assignments:

Complete: Lab 6

Week 8:

Weekly learning objectives:

- Lesson 6: Message Integrity, PKI and TLS Part II

Readings:

- Read: Lesson 7 Readings

Assignments:

- Complete: Lab 7

Week 9:

Weekly learning objectives:

- Lesson 7: Layer 2 Security
- Lesson 8: IPSec, Firewalls, and IDS

Readings:

- Read: Lesson 8 Readings

Activities:

- Complete: Lab 7

Week 10:

Weekly learning objectives:

- Lesson 9: Authentication

Readings:

- Read: Lesson 9 Readings

Activities:

- Complete: Lab 8

Week 11:

Weekly learning objectives:

- Lesson 11: IPv6 Security

Readings:

- Read: Lesson 10 Readings

Activities:

- Complete: Lab 9

Week 12:

Weekly learning objectives:

- Lesson 10: Wireless Security

Readings:

- Read: Lesson 8 Readings

Activities:

- Complete: Lab 9

Week 13:

Weekly learning objectives:

- Final Review

Week 14:

Weekly learning objectives:

- Final Exam Week

University Policies

Moses Center Statement of Disability

Academic accommodations are available for students with disabilities. Please contact the Moses Center for Students with Disabilities (212-998-4980 or mosescsd@nyu.edu) for further information. Students who are requesting academic accommodations are advised to reach out to the Moses Center as early as possible in the semester for assistance.

NYU Tandon School of Engineering Policies and Procedures on Academic Misconduct[1]

A. Introduction: The School of Engineering encourages academic excellence in an environment that promotes honesty, integrity, and fairness, and students at the School of Engineering are expected to exhibit those qualities in their academic work. It is through the process of submitting their own work and receiving honest feedback on that work that students may progress academically. Any act of academic dishonesty is seen as an attack upon the School and will not be tolerated. Furthermore, those who breach the School's rules on academic integrity will be sanctioned under this Policy. Students are responsible for familiarizing themselves with the School's Policy on Academic Misconduct.
B. Definition: Academic dishonesty may include misrepresentation, deception, dishonesty, or any act of falsification committed by a student to influence a grade or other academic evaluation. Academic dishonesty also includes intentionally damaging the academic work of others or assisting other students in acts of dishonesty. Common examples of academically dishonest behavior include, but are not limited to, the following:
    a. Cheating: intentionally using or attempting to use unauthorized notes, books, electronic media, or electronic communications in an exam; talking with fellow students or looking at another

[1] Excerpted from the Tandon School of Engineering Student Code of Conduct

person's work during an exam; submitting work prepared in advance for an in-class examination; having someone take an exam for you or taking an exam for someone else; violating other rules governing the administration of examinations.

b. Fabrication: including but not limited to, falsifying experimental data and/or citations.
c. Plagiarism: intentionally or knowingly representing the words or ideas of another as one's own in any academic exercise; failure to attribute direct quotations, paraphrases, or borrowed facts or information.
d. Unauthorized collaboration: working together on work that was meant to be done individually.
e. Duplicating work: presenting for grading the same work for more than one project or in more than one class, unless express and prior permission has been received from the course instructor(s) or research adviser involved.
f. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.