New York University Tandon School of Engineering CS-GY 9163 Application Security
Fall 2020

Professor: Brendan Dolan-Gavitt
Email: brendandg@nyu.edu

Office hours:
Office Hours Zoom:

Meeting ID:

TA: TBA

Course Description

This course addresses the design and implementation of secure applications. Concentration is on writing software programs that make it difficult for intruders to exploit security holes. The course emphasizes creating secure designs, writing secure programs and identifying vulnerable patterns in existing code for C/C++, web, and mobile applications.

Course Location and Schedule

Tuesdays at 6:00-8:30 PM
Dibner, Pfizer Auditorium

Course Structure and Grading

Grading consists of five major assignments, each of which has multiple parts. You will participate in the course using NYU Classes located at https://newclasses.nyu.edu and through weekly lectures. Most assignments will include an autograded component available on GradeScope (https://www.gradescope.com/).

Grade Breakdown (%)

- Unit Assignment 1: 25%
- Unit Assignment 2: 25%
- Unit Assignment 3: 25%
- Unit Assignment 4: 25%

There will also be one extra credit assignment, which can be used to replace your lowest homework grade.

IMPORTANT NOTE: There are no quizzes or exams in this course. This means that each assignment is important. Start them early, and seek out help when you get stuck.

Attendance Policy

Because the COVID-19 pandemic, Application Security is a "blended" course. Any student may attend in-person or online; you do not have to ask me for permission.

I expect that since this is the first time we (or anyone) have tried a blended course at NYU, there will likely be some bugs to work out in the first few weeks. In addition, we may have to switch to online-only format for part or all of the semester. Please let me know as soon as possible if you encounter any problems.

Should you need extra time for an assignment, please email me **before** the due date—I am usually happy to give extra time if there's a good reason!

Note that if you will be participating remotely, you are still encouraged to do so "synchronously". Video recordings will be available, but joining in real-time will give you the opportunity to ask questions live and help keep you on track.

In-Person Guidelines

1. Masks must be worn at all times.
2. At the beginning of the semester, you will pick a seat in Pfizer. You will be expected to use the same seat *every class* in order to help with contact tracing.
3. Two and a half hours is a long time. We will have a 10 minute break after the first hour. Please continue to observe social distancing during this time, though!

Everyone is expected to abide by the University's COVID-19 poclicy:
https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/building-access-policy.html

Readings

The recommended text for the course is:
The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities by Mark Dowd, John McDonald, & Justin Schuh.

Access to free eBook from NYU library:
https://bobcat.library.nyu.edu/permalink/f/ci13eu/COURSES000344691
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/

We will not have any required readings from it, but it is an excellent resource for learning how to audit software for security vulnerabilities.

Topics

- Unit 1: Software Development Security (3 Weeks)
- Unit 2: Web Security (3 Weeks)
- Unit 3: Database Security (2 Weeks)
- Unit 4: Cloud Security (2 Weeks)
- Unit 5: Mobile Security (2 Weeks)

Detailed Schedule

Week	Topics	Assignment
1 9/8/2020	C Programming Review Version control, build control, linter, test frameworks, CI/CD, packaging	Assignment 1 Released
2 9/15/2020	Code reviews, fuzzing, static analysis C Pitfalls, Undefined Behavior	
3 9/22/2020	Attack basics (Buffer memory, memory, stack) and defenses	
4 9/29/2020	Browser security model, HTTP, content rendering, isolation, communication, navigation, security user Interface and cookies	Assignment 1 Due Assignment 2 Released
5 10/6/2020	Session management and user authentication, content security policies, web workers, and extensions	
6 10/13/2020	Cross Site Scripting, CSRF and metacharacter vulnerabilities	
7 10/20/2020	Basics of databases, access control, privileges and views in Databases, techniques for encrypting sensitive information in databases, threats to e-commerce transactions, protecting data integrity and ensuring accessibility.	
8 10/27/2020	Logging and recovery, ARIES & logging, key-value database	Assignment 2 Due Assignment 3 Released
9 11/3/2020	Docker, PID, Mount, Network, UTS, IPC, User; cgroups; capabilities; seccomp; container	

	image scanning and signing and authorization plugins.	
10 11/10/2020	Kubernetes, Notary/TUF, SPIFFE, ISTIO, OPA	Assignment 3 Due Assignment 4 Released
11 11/17/2020	Core security concepts, platform and trends, Threat categories, system architecture and defenses.	
12 11/24/2020	Device controls, privacy controls, system security	
13 12/1/2020	Encryption & data protection, app security	
14 12/8/2020	Grab bag: feel free to suggest topics!	Assignment 4 Due
15	Finals Week (no class)	Extra Credit due by end of Finals period.

Course Communication

Announcements -
Announcements will be posted on NYU Classes on a regular basis. You can locate all class announcements under the *Announcements* tab of our class. Be sure to check the class announcements regularly as they will contain important information about class assignments and other class matters.

Email –
You are encouraged to post your questions about the course in the Forums discussions on NYU Classes. This is an open forum in which you and your classmates are encouraged to answer each other's questions. But, if you need to contact me directly, please email me at **brendandg@nyu.edu.** You can expect a response within 48 hours.

Netiquette –
When participating in an online class it is important to interact with your peers in an appropriate manner. Always use professional language in your discussion board posts and emails. Please be respectful of your classmates at all times even if you disagree with their ideas.

Moses Center Statement of Disability

If you are student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities (CSD) at 212-998- 4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information

about the Moses Center can be found at www.nyu.edu/csd. The Moses Center is located at 726 Broadway on the 2nd floor.

NYU School of Engineering Policies and Procedures on Academic Misconduct *(from the School of Engineering Student Code of Conduct)*

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 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.

You can find the full Student Code of Conduct here: https://engineering.nyu.edu/campus-and-community/student-life/office-student-affairs/policies/student-code-conduct