New York University Tandon School of Engineering
CS-GY 9163 Application Security
Spring 2021
Professor: Kevin Gallagher

To contact professor: **[REDACTED]**

Course Description

This online 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. | Prerequisite: Graduate standing

Course Objectives

By the end of this course students should be able to:

- Describe security threats faced in different application environments including software, web, database, cloud, and mobile.
- Incorporate measures to reduce the risk of application security breach.
- Locate resources that are up to date to address emerging application security issues.

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.

Grade Breakdown (%)

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

Learning Time Distribution

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Lecture	Asynchronous	2-3 hours	Interactive multimedia content with hands-on activities and quizzes throughout the module.
Assessment (homework)	Asynchronous	7 hours	Submit assignment **by the last day of class** unless otherwise specified. Assignments submitted by the soft deadline get a free resubmission.
Reading Assignment	Asynchronous	2-3 hours	Complete assigned readings and/or suggested readings of your interest
Live Webinar	Synchronous	1-2 hours	Hosted by the instructor or teaching assistants to answer questions. Held on Sundays at 6 PM Eastern.

Unit Assignment

Refer to **Unit Assignment Guideline** on NYU Classes to complete each weekly portion. The assignments are divided into weekly portions to help you stay on track. By the end of each week, you are encouraged to check in on the course Slack in the assignment channel with any questions you may have. You will receive feedback from me or teaching assistants and then modify your work accordingly. At the end of each unit, you are required to submit the final version of your project on NYU Classes via the "**Submit Assignments**," tabs.

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:
http://bobcat.library.nyu.edu/primo-explore/fulldisplay?docid=nyu_aleph005548728&context=L&vid=NYU&search_scope=all&tab=all&lang=en_US

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/

Additional reading outside the textbook might be required; Check the topic list below for reading assignment.

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)

Details are subject to change

Week	Topics	Readings	Assignment
1	Version control, build control, linter, test frameworks, CI/CD, packaging	Text: Ch 1 Common Threads	Assignment 1 Part 1
2	Code reviews, fuzzing, static analysis		Assignment 1 Part 2
3	Attack basics (Buffer memory, memory, stack) and defences	Text: Ch 5	Assignment 1 Part 2
4	Browser security model, HTTP, content rendering, isolation, communication, navigation, security user Interface and cookies	Text: Ch 17 HTTP	Assignment 1 Part 3
5	Session management and user authentication, content security policies, web workers, and extensions	Text: Ch 17 State & HTTP Authentication	Assignment 2 Part 1
6	Cross Site Scripting, CSRF and metacharacter vulnerabilities	Text: Ch 17 Common vulnerabilities Text: Ch 8 Metacharacter filtering	Assignment 2 Part 1
7	Basics of databases, access control, privileges and views in Databases, techniques for encrypting sensitive information in databases, threats to ecommerce transactions, protecting data integrity and ensuring accessibility.		Assignment 2 Part 1

Week	Topics	Readings	Assignment
8	Logging and recovery, ARIES & logging, key-value database		Assignment 2 Part 2
9	Docker, PID, Mount, Network, UTS, IPC, User; cgroups; capabilities; seccomp; container image scanning and signing and authorization plugins.		Assignment 3 Part 1
10	Kubernetes, Notary/TUF, SPIFFE, ISTIO, OPA		Assignment 3 Part 2
11	Core security concepts, platform and trends, Threat categories, system architecture and defenses.	Watson (2012)	Assignment 3 Part 2
12	Device controls, privacy controls, system security, encryption & data protection, app security		Assignment 3 Part 3
13	Device controls, privacy controls, system security, encryption & data protection, app security		Assignment 4
14	Finals Week		Assignment 4

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 Slack server. 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 [REDACTED]. You can expect a response within 48 hours.

Weekly Virtual Meetings –

On a regular basis, we will hold a virtual class meeting through the video conferencing tool listed on NYU Classes. This meeting is an opportunity for you to ask questions and gain clarification about the course content from myself and your peers. You are highly encouraged to attend these meetings. I understand that not all students will be available to attend these virtual meetings. Due to this fact, the meetings will be recorded so you can watch them when you are available.

Netiquette –

When participating in an online class it is important to interact with your peers in an appropriate manner. Always use professional language (no netspeak) 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:

1. 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.
2. Fabrication: including but not limited to, falsifying experimental data and/or citations.
3. 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.
4. Unauthorized collaboration: working together on work that was meant to be done individually.
5. 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.
6. Forgery: altering any academic document, including, but not limited to, academic records, admissions materials, or medical excuses.

Access the entire School of Engineering Student Code of Conduct here: engineering.nyu.edu/academics/code-of-conduct