New York University Tandon School of Engineering

Department of Computer Science and Engineering
CS-GY 6813 Information Security & Privacy
CS-UY 3923 Computer Security
Spring 2021
Professor Mo Satt

Teaching Assistants:

To contact professor:
Office hours:

Computer Security Course Pre-requisites
Prerequisite for Brooklyn Students: CS-UY 2214
Prerequisite for CAS Students: CSCI-UA 201
Co-requisite for ALL Students: CS-UY 3224

Information Security & Privacy Course Pre-requisites
Competency in Application Development in UNIX and Windows Environments.

Course Description
This class provides a firm grounding in computer security concepts and basics. Students learn about threat modeling, principles of secure design, security policies, access control technologies, and similar topics. The course is a lecture-oriented class.

Student Outcomes

The course is a component of the following student outcomes:

☑	1	an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
☑	2	an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
☑	3	an ability to communicate effectively with a range of audiences

☑	4	an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
☑	5	an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives
☑	6	an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
☑	7	an ability to acquire and apply new knowledge as needed, using appropriate learning strategies.

Course Objectives

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

- Think with a security mindset while remaining ethical.
- Describe the problems of physical security and online security.
- Use the security design principles.
- Explain the core concepts of access control, reference monitors, and security policies that are commonly used in modern OSes.
- Analyze and implement the basic secure systems.
- Compare different virtualization techniques and explain how they impact security and efficiency.

Course Structure

This course lectures are conducted entirely online, which means you do not have to be present on campus. You will also participate in the course discussions and complete online labs and programming labs using NYU Classes at: https://newclasses.nyu.edu .

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/

Grade Calculation

Exam 1 : 20%
Exam 2 : 20%

Final Exam: 25%
Discussions: 5%
Online Labs: 15%
Programming Labs: 15%

Course requirements

LEARNING TIME RUBRIC

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Lecture	Synchronous	2.5 hours	Students should make every effort to attend class on time.
Discussions	Asynchronous	0.5 hours	Students discuss the instructor's questions for each lesson.
Online Labs	Asynchronous	1.0 hour	Students independently work on Online cybersecurity labs. Students will submit a screenshot of their completion.
Programming Labs	Asynchronous	1.0 hour	Students independently work on programming labs. Students will submit their code to NYU classes.

*Asynchronous learning is defined as any non-real time student learning, such as recorded lecture, podcast, interactive module, articles, websites, etc. This also includes any student-to-student or faculty-to-student communication that may happen with an asynchronous tool, such as discussion board, chatroom, e-mail, text, etc.
**Synchronous learning is defined as any real-time student-to-student and/or faculty-to-student learning, such as an instructor-led lecture, live webinar session or other video/audio communication service.

COURSE COMMUNICATION

WEEKLY OFFICE HOURS

The Teaching Assistant (TA) will be available for weekly office hours by appointment. To schedule an appointment with your TA, or to ask any questions about the course content, please email them.

Course Schedule:

Lecture	Topic(s)	Date

Lecture 1	**Introduction to the Course**	2/2/2021
Lecture 2	**Security Design Principles**	2/9/2021
Lecture 3	**Threat Modeling**	2/16/2021
Lecture 4	**Security Policies**	2/23/2021
Exam 1	Covers Lectures 1-4	3/2/2021
Lecture 5	**Access Control (1): Operating Systems, phones**	3/9/2021
Lecture 6	**Authentication and IAM**	3/16/2021
Lecture 7	**Access Control (2): IFC, O-Cap**	3/23/2021
Lecture 8	**Containerization: VMs, SFI, DoS**	3/30/2021
Exam 2	Covers Lectures 5-8	4/6/2021
Lecture 9	**Privacy and Key Management**	4/13/2021
Lecture 10	**Software validity and rights**	4/20/2021
Lecture 11	**Injection attacks and defenses**	4/27/2021
Lecture 12	**Cryptography**	5/4/2021
Reading Day	**NO CLASS**	5/11/2021
Final Exam	Covers Lectures 1-12	5/18/2021

Discussion Board Grading Rubric:

Criteria	**0 Points - Unacceptable**	**1 Point - Needs Improvement**	**2 Points - Satisfactory**	**3 Points - Excellent**

Initial Posting Timing & Relevance	**Zero posts or does not meet the instructor's timeline and requirements.**	**Superficial thought. Addressed limited aspects relevant to the prompt and does not demonstrate an understanding of key concepts. Met partial elements of instructor timeline and requirements**	**Thoughts were well developed and addressed basic aspects relevant to the prompt and demonstrated base knowledge of concepts. The student mostly met instructor timeline and requirements.**	**Thoughts were well developed and fully addressed all aspects relevant to the prompt. Demonstrated excellent integration of key concepts. Met or exceeded instructor timeline and requirements.**
Reply Postings Timeline & Relevance	**Zero replies, or replies not relevant to discussion topics**	**Replies were limited in relevance or did not enrich discussion (e.g. agrees or disagrees) or met partial elements of instructor timeline and requirements.**	**Elaborated on posts with further comment or observation, relevant to the topic. The student mostly met instructor timeline and requirements.**	**Demonstrated analysis of others' posts, included meaningful comments. Offered thoughtful insight. Met or exceeded instructor timeline and requirements.**
Clarity & Mechanics & Reference	**Zero posts, or posted unorganized content that may contain multiple grammatical or spelling errors or may be**	**Communicated in a somewhat unorganized manner, with some errors in clarity and/or grammatical or spelling errors. Partially met instructor**	**Communicated and contributed valuable information with minor errors in clarity and/or grammatical or spelling errors.**	**Communicated and contributed to discussions with clear, concise comments formatted in an easy to read style with no grammatical or**

	inappropriate. The student did not meet the instructor's requirements for references and citations.	**requirements for references and citations.**	**The student mostly met instructor requirements for references and citations.**	**spelling errors. Met or exceeded instructor requirements for references and citations.**

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 3rd floor.

NYU School of Engineering Policies and Procedures on Academic Misconduct – complete Student Code of Conduct here

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 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.

NYU School of Engineering Policies and Procedures on Excused Absences – complete policy here

A. Introduction: An absence can be excused if you have missed no more than **10 days of school**. If an illness or special circumstance has caused you to miss more than two weeks of school, please refer to the section labeled Medical Leave of Absence.

B. Students may request special accommodations for an absence to be excused in the following cases:

1. Medical reasons
2. Death in immediate family
3. Personal qualified emergencies (documentation must be provided)
4. Religious Expression or Practice

Deanna Rayment, deanna.rayment@nyu.edu, is the Coordinator of Student Advocacy, Compliance and Student Affairs and handles excused absences. She is located in 5 MTC, LC240C and can assist you should it become necessary.
NYU School of Engineering Academic Calendar – complete list here.
The last day of the final exam period is May 19th, 2020. Final exam dates for undergraduate courses will not be determined until later in the semester. Final exams for graduate courses will be held on the last day of class during the week of May 18th, 2020. If you have two final exams at the same time, report the conflict to your professors as soon as possible. Do not make any travel plans until the exam schedule is finalized.
Also, please pay attention to notable dates such as Add/Drop, Withdrawal, etc. For confirmation of dates or further information, please contact Susana: sgarcia@nyu.edu