NYU TANDON SCHOOL OF ENGINEERING

CS GY 6813 Information Security & Privacy

Professors:
Kevin Gallagher, Ph. D.
Aspen Olmsted, Ph. D.

Teaching Assistants:

COURSE OVERVIEW

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.

LEARNING OBJECTIVES

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

- Apply a security mindset while remaining ethical.
- Implement security design principles.
- Explain the core concepts of access control.
- Implement reference monitors.
- Apply security policies that are commonly used in modern operating systems.
- Analyze the security of a basic secure system.
- Explain virtualization and the impact on security and efficiency.

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.

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 the instructor's questions for each lesson.
Reading & Research	Asynchronous	2.5 hour	Students complete recommended readings (online journal articles and tutorials) and work on their related research presentation.
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 in programming labs. Students will submit their code to Gradescope.

*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 a live webinar session or other video/audio communication service.

COURSE COMMUNICATION

WEEKLY VIRTUAL OFFICE HOURS

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 email them.

TAs email:

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/

COURSE OUTLINE

Lesson 1: Introduction to the Course

Lesson 2: Security Design Principles

Lesson 3: Threat Modeling

Lesson 4: Security Policies

Lesson 5: Cryptography

Lesson 6: Authentication

Lesson 7: Access Control (1): Operating Systems, phones

Lesson 8: Access Control (2): IFC, O-Cap

Lesson 9: Containerization: VMs, SFI, DoS

Lesson 10: Injection attacks and defenses

Lesson 11: Privacy and Anonymity

Lesson 12: Cryptocurrency and IoT security

Quizzes

Quizzes allow you to check your understanding of the content presented in the lesson. You may complete the assessment up to two times before the due date. Students have 3 hours to complete each quiz. The average score will be used in the gradebook. If students do not submit a quiz they can still submit up until the last day of classes but only one submission is allowed.

Labs

Several technical labs will be assigned to give the student hands-on applied experience with the topics covered in the lecture. There will be two types of labs; Online and Programming. The online labs will be completed on an online system called Immersive Labs. Students will upload a screenshot of their completion to the NYU Classes to receive credit for the lab. The

programming labs will use a secure sandbox environment for Python called RePy. Programming Labs will be submitted to Gradescope.

Discussions

NYU Classes will have threaded discussion topics where you can interact on lectures, assignments, labs or the related research project. The course contains 4 graded discussion boards that are to be graded using the standard grading rubric (provided). The last discussion forum is where students will upload their project and students will provide peer feedback. A minimum of 2 peer responses is expected for each initial post.

Research

Each student will pick a specific, applied technical problem related to the material in the course. The student will then hypothesize a solution to the problem. Using tools such as google scholar the student will research related articles and will create a recording of their presentation of these materials to other students. This process is not the complete scientific process as the student will just be gathering preliminary evidence and disseminating their results. The students will discuss how they would gather evidence and expected results. There are many scaffolding assignments with hard deadlines and students will be assigned peer reviews after each assignment. The scaffolding assignments and reviews are part of your research grade.

GRADING

Quizzes: 35%
Discussions: 5%
Online Labs: 20%
Programming Labs: 20%
Hypothesis & Related Research Presentation: 20%

PROGRAM POLICIES

MOSES CENTER STATEMENT OF DISABILITY

If you are a 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.

SUGGESTED STUDENT SCHEDULE

Most required assessments and activities in this course are asynchronous so students can complete them at their own pace as long as they are completed by December 13th. The following table represents a schedule dividing all work more or less equally across the semester.

Lesson	Activities	Proposed Completion Date
Lesson 1:	Watch: Introduction to the Course Read: Lesson 1 Readings Interact: Questions Discussion Forum Practice: Quiz Lesson 1 Apply: Online Labs Webinar: Aspen 1/31/2021 7PM EST Webinar: Kevin 02/01/2021 6 PM	2/7/2021
Lesson 2	Watch: Security Design Principles Read: Lesson 2 Readings Interact: Questions & Prompt Discussion Forum Practice: Quiz Lesson 2 Apply: Online Labs Webinar: Kevin 02/08/2020 6 PM EST	2/14/2021
Lesson 3	Watch: Threat Modeling Read: Lesson 3 Readings Interact: Questions Discussion Forum Practice: Quiz Lesson 3 Apply: Online Labs Webinar: Aspen 2/21/2021 7PM EST Kevin 02/15/2021 6 PM	2/21/2021
Lesson 4	Watch: Security Policies Read: Lesson 4 Readings Interact: Questions & Prompt Discussion Forum Practice: Quiz Lesson 4 Apply: Online Labs	2/28/2021

	Webinar: Kevin 02/22/2021 6 PM	
Lesson 5	Watch: Introduction to Cryptography Read: Lesson 5 Readings Interact: Questions Discussion Forum Practice: Quiz Lesson 5 Apply: Online Labs Peer Review: Submit problem domain and review peers Webinar: Aspen 3/7/2021 7PM EST Kevin 03/01/2021 6 PM	3/7/2021
Lesson 6	Watch: Authentication Read: Lesson 6 Readings Interact: Questions Discussion Forum Practice: Quiz Lesson 6 Apply: Online Labs Peer Review: Submit Threat Model Webinar: Aspen 3/14/2021 7PM EST Kevin: 03/08/ 2021 6 PM	3/14/2021
Lesson 7	Watch: Access Control (1): Operating Systems, phones Read: Lesson 7 Readings Interact: Questions & Prompt Discussion Forum Practice: Quiz Lesson 7 Apply: Online Labs Peer Review: Submit hypothesis and review peers	3/21/2021

	Webinar: Aspen 3/21/2021 7PM EST Kevin: 03/16/2021 6 PM (Tuesday)	
Lesson 8	Watch: Access Control (2): IFC, O-Cap Read: Lesson 8 Readings Interact: Questions Discussion Forum Practice: Quiz Lesson 8 Apply: Online Labs Webinar: Kevin 03/22/2020 7 PM EST	3/28/2021
Lesson 9	Watch:Containerization: VMs, SFI, DoS Lesson 9 Readings Interact: Questions & Prompt Discussion Forum Practice: Quiz Lesson 9 Apply: Online Labs Peer Review: Submit metric and review peers Webinar: Aspen 4/4/2021 7PM EST Kevin: 03/29/2021	4/4/2021
Lesson 10	Watch: Injection attacks and defenses Read: Lesson 10 Readings Interact: Questions Discussion Forum Practice: Quiz Lesson 10 Apply: Online Labs Peer Review: Submit introduction and review peers	4/11/2021

	Webinar: Aspen 4/11/2021 7PM EST Kevin: 04/05/2021	
Lesson 11	Watch: Privacy and Anonymity Read: Lesson 11 Readings Interact: Questions Discussion Forum Practice: Quiz Lesson 11 Apply: Online Labs 7PM EST Peer Review: Submit related research section and review peers Webinar: Kevin 04/12/2021	4/18/2021
Lesson 12	Watch: Cryptocurrency Read: Lesson 12 Readings Interact: Questions Discussion Forum Apply: Online Labs Peer Review: Submit empirical evidence and review peers Webinar: Aspen 4/25/2021 7PM EST Kevin: 04/19/2021	4/25/2021
Lesson 13	Peer Review: Submit paper and present and review peers	5/6/2021

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 inappropriate. The student did not meet the instructor's requirements for references and citations.**	**Communicated in a somewhat unorganized manner, with some errors in clarity and/or grammatical or spelling errors. Partially met instructor requirements for references and citations.**	**Communicated and contributed valuable information with minor errors in clarity and/or grammatical or spelling errors. The student mostly met instructor requirements for references and citations.**	**Communicated and contributed to discussions with clear, concise comments formatted in an easy to read style with no grammatical or spelling errors. Met or exceeded instructor requirements for references and citations.**

Research Presentation Rubric:

Criteria	EXPERT 5 points	PROFICIENT 4 points	APPRENTICE 3 points	NOVICE 2 points
INTEGRATION OF KNOWLEDGE	The presentation demonstrates that the student fully understands and has applied concepts learned in the course. Concepts are integrated into the writer's own insights. The writer provides concluding remarks that show the analysis	The presentation demonstrates that the student, for the most part, understands and has applied concepts learned in the course. Some of the conclusions, however, are not supported in the body of the paper.	The presentation demonstrates that the student, to a certain extent, understands and has applied concepts learned in the course.	The presentation does not demonstrate that the student has fully understood and applied concepts learned in the course.

	and synthesis of ideas.			
TOPIC FOCUS	The topic is focused narrowly enough for the scope of this assignment. A thesis statement provides direction for the presentation by stating the hypothesis	The topic is focused but lacks direction. The presentation is about a specific topic but the writer has not established a position.	The topic is too broad for the scope of this assignment.	The topic is not clearly defined.
SOURCES	More than 5 current sources, of which at least 3 are peer-review journal articles or scholarly books. Sources include both general background sources and specialized sources. Special interest sources and popular literature are acknowledged as such if they are cited. All web sites utilized are authoritative.	5 current sources, of which at least 2 are peer-review journal articles or scholarly books. All web sites utilized are authoritative.	Fewer than 5 current sources, or fewer than 2 of 5 are peer-reviewed journal articles or scholarly books. All web sites utilized are credible.	Fewer than 5 current sources, or fewer than 2 of 5 are peer-reviewed journal articles or scholarly books. Not all web sites utilized are credible, and/or sources are not current.
Overall Score	**Level 4 15 Points**	**Level 3 12 or more**	**Level 2 9 or more**	**Level 1 0 or more**