New York University
CS 3923 / 6813 INT Syllabus - Fall 2018
Information Security and Privacy
Prof. Efstratios Gavas

Contact Information:
egavas@nyu.edu
6 MetroTech, room RH 219 (OSIRIS LAB)
Office hours: Thur 6:30-8:30PM or by appointment

Graduate teaching assistants:
TBD

Course Description

This class provides a firm grounding in computer security concepts and basics. Students will learn about threat modeling, principles of secure design, security policies, access control technologies, and similar topics. Material and course design provide by Prof. Justin Cappos.

During this course, students will:

1. Understand physical security and online security.
2. Construct of a reference monitor that restricts access to network and disk resources for a virtual machine. Analysis of the implementations for security flaws.
3. Analyze flaws in a practical system. Implementation of an extension to fix at least one of these issues. An analysis of proposed fixes to understand their security properties.
4. Obtain a deep understanding of virtualization including Type 1 (which we further subdivide by those that virtualize hardware versus a set of kernel patches that jail different VMs) and Type 2 virtualization, their implementation, and the efficiency, security, simplicity, and resource savings tradeoffs. Students are tested on their knowledge of virtualization tradeoffs.
5. Learn about database topics related to security including Hashing and Encryption, Database access controls (DAC, MAC, RBAC, Clark-Wilson), Information flow between databases/servers and applications, and Common DBMS vulnerabilities such as SQL injection.

Course Objectives

1. Learn to think with a security mindset while remaining ethical.
2. Learn the core concepts of access control, reference monitors, and security policies that are commonly used in modern OSes.
3. Learn the basics of building and analyzing secure systems.
4. Understand virtualization, including different virtualization techniques and how they impact security and efficiency.

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 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.

Academic Dishonesty:

Students must follow collaboration guidelines for all projects. All tests and quizzes are individual. Students must behave ethically at all times.

> ***Academic dishonesty will be reported to the department and included on your permanent record.***

For more details, see the Code of Conduct:
https://engineering.nyu.edu/academics/code-of-conduct/academic-misconduct

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.

Students are encouraged to participate, both online and on-campus, in activities hosted by the computer security lab (https://www.osiris.cyber.nyu.edu/).

Readings

There is no textbook for this class. Lectures will include online materials that should be read.

Learning Time Rubric

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

Grading:

Discussions: 10%
Quizzes: 10%
Exam 1: 10%
Exam 2: 10%
Final: 20%
Assignments: 40%

Suggested Course schedule

Week	Topic/Review	Assignment
1	Watch: Introduction to the Course Read: Lesson 1 Readings	Interact: Lesson 1 Discussion Forum Complete: Assignment 1.1
2	Watch: Security Design Principles Read: Lesson 2 Readings	Interact: Lesson 2 Discussion Forum Complete: Assignment 1.2
3	Watch: Threat Modeling Read: Lesson 3 Readings	Interact: Lesson 3 Discussion Forum Complete: Assignment 1.3
4	Watch: Security Policies Read: Lesson 4 Readings	Interact: Lesson 4 Discussion Forum Complete: Assignment 2.1
5	Review: Lectures 1-4	Take: Exam 1
6	Watch: Access Control (1): OS, phones Read: Lesson 5 Readings	Interact: Lesson 5 Discussion Forum Complete: Assignment 2.2
7	Watch: Lesson 6 - Justin Cappos Interview	Interact: Interview Discussion Forum
8	Watch: Access Control (2): IFC, O-Cap Read: Lesson 7 Readings	Interact: Lesson 7 Discussion Forum Complete: Assignment 2.3
9	Watch: Containerization: VMs, SFI, DoS Read: Lesson 8 Readings	Interact: Lesson 8 Discussion Forum
10	Watch: Privacy and Key Management Read: Lesson 9 Readings	Interact: Lesson 9 Discussion Forum Complete: Assignment 3.1
11	Review: Lectures 5-9	Take: Exam 2
12	Watch: Software validity and rights Read: Lesson 10 Readings	Interact: Lesson 10 Discussion Forum Complete: Assignment 3.2
13	Watch: Injection attacks and defenses Read: Lesson 11 Readings	Interact: Lesson 11 Discussion Forum Complete: Assignment 3.3
14	Watch: Cryptocurrency and IoT security Read: Lesson 12 Readings	Interact: Lesson 12 Discussion Forum
15	**Review: Lectures 1-12**	**Take Final**