New York University Tandon School of Engineering
CS GY6803-CF01/02: Information Systems Security Engineering and Management
Summer 2022
S. Raj Rajagopalan, Ph.D.

To contact professor:
Email: sr6268@nyu.edu
Weekly Live Lectures: Wednesdays at 7-9PM EDT on Zoom https://nyu.zoom.us/j/95934673453
Office hours: Through Zoom by appointment

Course Prerequisites
Students will better benefit from the course if they have cybersecurity background such as have taken at least one course in the Cybersecurity program, for example Information Security and Privacy. Some familiarity with programming languages (Python) is necessary.

Course Description

This course provides an overview of the roles and responsibilities of a Cybersecurity architect in the creation and operation of products and systems. There will be an emphasis on the real-world aspects of making products and systems secure and new approaches to collaboration between various stakeholders towards this goal. Particular focus will be placed on learning from security incidents that have been reported and described in the public domain and the importance of cybersecurity architects keeping up with the changing security landscape. Throughout the course we will focus on keeping an open mind, creating solutions that are appropriate to the problems being addressed, and learning through dialog with peers. In addition, the importance of being an advocate for security in the face of cost and schedule pressures will be explored. Case studies and best practice examples will be used extensively.

Course Objectives

By the end of the course, students will be able to

- Describe the overall structure of the product lifecycle and the role of cybersecurity in the life cycle
- Summarize the cybersecurity best practices that apply to each phase of the life cycle
- Enumerate the roles and responsibilities of Cybersecurity architects and the various mechanisms for discharging those responsibilities
- Develop the skills to guide the security in product development and operation
- Evaluate new technologies and solutions in the context of product cybersecurity
- Analyze and evaluate the risks associated with a product with respect to its cybersecurity gaps

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://brightspace.nyu.edu/.

Grade Breakdown (Subject to change)

- Weekly Discussion Forum Participation: 10%

Every week there will be a discussion topic posted in the Discussion Forums.Every student is expected to participate in the discussions. Details posted in the forums.

- Weekly Quizzes: 20%

Every week there will be a short quiz on the materials of that week. You will get two attempts for each quiz. You will be assigned to one of two cohorts A or B each week and you will be able to take either Quiz A or Quiz B depending on your cohort. Quizzes will be taken individually.

- Written Assignments: 25% (Peer graded)

There will be one or more written homework assignments (depending on the time available) that will be done as a group. These will be peer-graded using the Peerceptiv platform. In addition to submitting your assignments you will also be required to grade some of your peers' submissions.

- Labs: 25% (Short coding assignments)

Labs are clustered around a simulator of a medical device on which the principles discussed in this course will be implemented. Labs are all about submitting Python code in Jupyter notebooks or submitting written assignments relating to Python code since the simulator is in Python. Labs will be either on a signleEvery two weeks there will be a Lab assignment that will be done in the same group as your written assignments. Labs will be graded by the Professor and/or Course Assistants.

- Final Project: 20%

The final project will be a combination of the last coding assignment and the last written homework assignment. This will also be done in the same group as the other labs.

- Extra Credit: Variable

From time to time there will be extra credit assigned for timely/early submission of assigned work.

- Peer Assessment

**Note: This course utilizes peer assessments. Part of your final group project grade is based on the feedback from your fellow group members. Please see the sample project survey at the end of this syllabus. While you may feel that your peers are not capable of judging your work correctly, this nevertheless reflects the real world. The professor and course assistants will be available to adjudicate in extreme cases.

- Surveys

There are a few surveys built into the course schedule. These are meant for the professor to get feedback and adjust the parameters of the course. These surveys are anonymous and you should feel free to express your opinions candidly and in detail.

Course schedule

Module 1: Introduction to security

- Brief history of cybersecurity in products
- Introduction to cybersecurity in different kinds of products

Discussion 1. What is the place of cybersecurity in your organization's processes?

Module 2: Security Principles

- Security Design Principles
- Cryptography and Key Management
- Authentication and Access Control

Discussion 2. Which security principles have you encountered and where

Module 3: Security Requirements

- The importance of setting down requirements before doing anything else
- Important standard that help define security requirements
- How to define security requirements using standards

Discussion 3. How are standard product requirements captured in your organization

Module 4: Secure-by-design

- Systems Engineering Models: Waterfall, Iterative, Spiral, Agile, etc
- Principles and Drivers in Dev models
- The challenges of security in each development model

Discussion 4. Which of the various models have you participated in and what are their advantages/disadvantages?

Module 5: Security in System Architecture

- Architectural level design and analysis
- The What and why of Threat modeling

Discussion 5. Have you participated in design reviews for security or non-security attributes in your organization?

Module 6: Threat Modeling

- Different approaches to Threat Modeling
- Tools for threat modeling

Discussion 6. How do Threat modeling techniques discussed in this course compare with any design reviews (of any kind) that you may have seen elsewhere?

Modules 7: Security Controls & Defenses

- Methods to determine appropriate security controls
- Constraints on choice of controls
- Advanced principles for design of defense

Discussion 7. Are you familiar with any security control or defense mechanisms in some role : user, developer, architect, auditor, etc.

Module 8: Security Risk Management

- Definitions of Risk in the security context
- Methods to measure risk

Discussion 8. How does security risk compare with other kinds of risk that you are familiar with?

Module 9: Cybersecurity in Software Development

- The importance of Cyber hygiene
- Common hygiene practices
- Tools for code hygiene: Static analysis and dynamic analysis tools

Discussion 9. What if any guidance do developers in your organization get for security hygiene and are they effective?

Module 10: Cybersecurity testing

- How cybersecurity testing is different from functional testing
- Why testing is still necessary
- Integrating testing with architectural analysis and threat modeling

Discussion 10. What kinds of cybersecurity testing have you come across? What were the challenges with the test results?

Module 11: Cybersecurity in the field

- Patch management, Over-the-air updates, etc.
- Incident management
- Threat intelligence

Discussion 11. Have you been a participant in any security breach either as an affected party or the mitigator?

Module 12: Laws and regulations (Optional for Summer)

- The relationship between functional requirements, security requirements, and the law.
- The need for defined Cybersecurity governance for system development
- Policy definitions based on regulatory needs
- Infant incubator: medical laws and regulations, safety

Discussion 12. What is your knowledge of cybersecurity-related regulations in any domain, IT or elsewhere?

Module 13: Cybersecurity beyond the Product Lifecycle (Optional for Summer)

- External forces affecting cybersecurity inside the Lifecycle
- How to know that the security lifecycle is working as designed
- Evolving Standards: How to keep up

Discussion 13. How does the concept of “Double loop learning” apply here?

Module 14: Putting it all together

- Roles and responsibilities of Security personnel
- Social expectations from Security
- How to keep up with the changing security landscape

Discussion. None

Course Structure

This course is conducted entirely online through the approved e-learning platform (https://brightspace.nyu.edu). You do not have to be on-campus to complete any portion of it.

Since the course is designed to provoke-thought through instruction, we encourage and expect students to actively discuss their answers to the myriad of questions presented across the modules. As such, a larger than normal portion of the grade is allocated to engagements.

The following grade breakdown is tentative. Please consult the official breakdown at the beginning of the semester. Please contact the instruction with any additional questions and/or most up-to-date information.

Learning Time Rubric

The following is a breakdown if expected learning times for different components. Some students might spend more time and others less.

Learning Time Element	Asynchronous / Synchronous	Time on Task for Students (weekly estimate)	Notes
Weekly Lecture	Live	1	Interactive module format. It may take some students longer to complete. Expect low-stakes exercises throughout the module. That time is listed separately.
Reading Assignment	Asynchronous	2 hours	Reading references articles and other background material.
Assignments	Asynchronous	1.5 hours	Homework assignments are bi-weekly. These include mini-presentations on topics of interest. These can be solo or (preferably) in groups.
Weekly Discussions & Low-Stakes Exercises	Synchronous	1.5 hours	Discussions and engagement grades will be heavily influenced by fellow student feedback.
Labs & Group Project	Synchronous/Asynchronous	3 hours	Work with group members on project

Course Communications

Announcements -

Announcements will be posted on the course site 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 Discussions tab on Brightspace. This is an open forum in which you and your classmates are encouraged to answer each other's questions. Please email me at the address listed above if you need. You can expect a response within 48 hours. Also, please don't be shy. Send me a reminder if you don't hear back. I always appreciate friendly reminders.

Discussion Forums –

Discussion forums are an excellent way for you to engage with the course material and with your peers. Each module will have an accompanying discussion board question posted in the Forums tab. You are expected to read the discussion boards and engage in thoughtful discussions. I will read discussion posts and provide content clarification and feedback when necessary. Hearing the same exact point from a slightly different perspective can be very helpful. The discussion forum tries to tease out past work experiences of the students and look at these experiences again in a new light. Understanding that not everyone comes from a cybersecurity or even IT or engineering background, it is adequate if you respond to other students' posts or ask questions in response to experiences described by other students. For every week's discussion, in order to maintain topicality, you have two weeks past the week in which a discussion topic is raised. If you do not participate in that topic in that time period you will be marked absent for that topic. But do not be alarmed by this – there are 12-14 discussion topics in this semester and so each topic is worth less than 1% of the overall grade. Again, you are judged to have participated meaningfully in a particular topic if you have posted at least one answer or asked at least two questions.

Slack Channel –

There is a slack channel NYU-ISSEM SUMMER-2022 which can be used by the students of this class to discuss anything related to this course. Here is the invite:

https://join.slack.com/t/nyu-issemsummer-2022/shared_invite/zt-19snu2gv4-TcXKN6NtLHKy2lOEeBr5EA

(valid until Jun 23, 2022)

Weekly Live Lectures –

Every week there will be a live zoom lecture to discuss the topic of that week. We will discuss topical material and case studies in this lecture and it will be a high interaction session. This is

an opportunity for students to ask questions and gain clarification about the course content from your peers and myself. You are highly encouraged to attend these meetings live and participate in the lectures. I understand that not all students will be available to attend these meetings, so the meetings will be recorded. More importantly, questions are welcomed at any time.

Send me emails or ask your fellow students at any time.

Additional Note: Your attendance in the live lecture is not mandatory and will not impact your grade.

Assignments -

Labs & Final Project –

The final project will consist of applying a combination of techniques to the security of a particular product which will be a simulated medical device. The project will consist of both theoretical analysis and development of some of the code necessary to secure the product.

Netiquette –

Etiquette applies equally to online and in-person classes. Be respectful at all times. Use appropriate language in all communications. Disagreements and debates are great learning tools so use language that helps everyone learn.

Interaction Policy

In theory, systems are either secure or not secure. In practice, they are either secure enough or not, but everyone has a different definition of enough. The more we interact, the better we can understand and appreciate different measures of enough. As such, you are required to be an active online learner and are expected to participate in the Active Learning Modules, weekly discussion boards, weekly live lectures, etc. Students are also encouraged to discuss material/solutions with one another through the bulletin boards. Helping each other is encouraged, but make sure to abide by the Student Code of Conduct.

Readings

A textbook is not required for this course. Reference materials can be found in the lecture materials. Since new discoveries are made regularly, security architects should inculcate a habit of reading publications proactively. Every week there will be an assigned reading that you may be tested on in the weekly quiz.

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.

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.

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