EC521 Cybersecurity

Instructor Name: Gianluca Stringhini
Course Time & Location: Mon 10:10-11:55 565 Commonwealth Ave KCB 106
Wed 10:10-11:55 565 Commonwealth Ave KCB 106

Course Credits: 4

Email: gian@bu.edu
Office Hours: Wednesdays 12:30-2pm PHO331

GTF: Olawale Akanji
Email: olawalea@bu.edu
Office Hours: Thursdays 1-3 PHO 318

Course Description

Internet security has become part of everyday life where security problems impact practical aspects of our lives. Even though there is a considerable corpus of knowledge about tools and techniques to protect systems, information about what are the actual software vulnerabilities and how they are exploited is not generally available. This situation hampers the effectiveness of security research and practice. Understanding the details of attacks is a prerequisite for the design and implementation of secure systems.

This course deals with common programming, configuration, and design mistakes and ways to detect and avoid them. Examples are used to highlight general error classes, such as cross site scripting, stack, and heap overflows. Possible protection and detection techniques are examined. The course includes several practical homework assignments where participants are required to apply their knowledge. Students will learn how the security of systems can be violated, and how such attacks can be detected and prevented.

The course aims to make the students "security aware," and gain an in-depth understanding about security issues.

Course Topics

We will cover the following topics

- Basic security principles (authentication, threats, vulnerabilities, confidentiality, integrity, availability)
- Cryptography (symmetric and public key cryptography, cryptanalysis)
- Network security (spoofing, hijacking, network attacks, IPSec, SSL, TLS)
- Web security (SQL injections, Cookies, CSRF, XSS)
- Unix security (Authentication, filesystem, processes, environment, command injection)
- Assembly and reverse engineering

- Memory corruption attacks (stack and heap overflows, format string vulnerabilities)
- Defenses against memory corruption (stack canaries, ASLR, PIE, CFI)

If time permits, we will cover some of the following topics as well

- Mobile security (Android, iOS)
- Malware

Prerequisites

The class does not have any formal prerequisites, however the following knowledge is helpful to quickly grasp the material:

- Programming in C/C++
- Programming in a scripting language (e.g., python)
- Knowledge of Web technologies and languages (e.g., JavaScript, SQL)
- Knowledge of computer networks (EC441 or equivalent)
- Knowledge of operating systems (EC440 or equivalent)

Course Learning Outcomes

The learning outcomes for this class will be of two types:

- **General security concepts.** Students will learn the terminology commonly used in the field of computer security, as well as the theory behind common security vulnerability and defenses.
- **Practical security skills.** Students will practice how systems can be exploited and protected with practical homework assignments, where they will be asked to perform attacks against practice systems and describe what they did.

Instructional Format, Course Pedagogy, and Approach to Learning

This class will take a learn by doing approach to teaching students about computer security issues and defenses. Each lecture will alternate the theory behind a particular problem with practical examples (e.g., demonstrating how certain security vulnerabilities can be exploited), allowing students to practice the concepts being covered in real time on their own laptops, as well as practicing later at home.

Class attendance is not mandatory, but 5% of your grade is based on class participation either during the lectures or in discussions on Piazza. If you cannot attend more than 5 lectures during the semester please contact the professor.

Books and Other Course Materials

There is no required book for this class. The instructor will provide class material and online resources as needed through Blackboard.

Course components

Blackboard

You are responsible for checking the Blackboard page for EC521– Fall 2024 regularly. Blackboard will contain handouts, lecture notes and additional material. You will use Blackboard to submit the explanation to your homework assignments.

Piazza

You are responsible for checking the Piazza page for EC521 – Fall 2024 regularly. We encourage discussion in this class, and we will use Piazza for that. The instructor and the TA will post additional questions, recent news, and tutorials on Piazza to allow students to better grasp key concepts covered in the lectures and help fix potential misconceptions early. Students are encouraged to participate in online discussions, such as asking and answering questions.

CTF Scoreboard

We plan to release multiple homework assignments throughout the course, to allow students to get a practical knowledge of the various topics covered in class. The security challenges will be hosted on virtual machines, and students will submit their answers by using a Capture the Flag web application displaying a scoreboard. Additional information about the challenges and the scoreboard will be provided in due course.

Group projects

Starting from mid-semester, students will form groups of 3-4 people to study a specific security problem of their choice. At the end of the semester each group will present their work and produce a final report.

Grading

Raw scores will be computed based on the following weights. Grades will not be curved.

- Class participation (5%)
- Group project (25%)
- Two midterm exams (25%)
- Homework assignments (45%)

Community of Learning: Class and University Policies

1. **Assignment Completion & Late Work**. Each homework assignment is given a two-week period for you to complete it. Because of this, no late submissions will be accepted.
2. **Academic Conduct Statement.** All homework assignments must be completed individually, although you may discuss general suggestions and questions with others in the class. Homework assignments have been created for you to build your mastery of the core security concepts and material, and they are at the heart of the course. Any written code or answers that you submit must be completely your own work! You may not copy any code from anyone else, and you must never look at anyone else's code when working on your homework assignments. You must be able to fully explain your answers upon demand. The use of generative AI to produce writing material for the class (e.g., written reports) is not allowed. The general Academic Conduct Code is available here: *https://www.bu.edu/academics/policies/academic-conduct-code/*

3. **Ethical conduct.** A large part of this class is about learning how to exploit security vulnerabilities. While we believe that understanding attacks is key in becoming good security professionals, be aware that running computer attacks against systems that you do now own is illegal and can have serious repercussions. In this class we provide you with ample space to test your knowledge in a safe and controlled environment, so please leave it at that. Do not run any security tool or attempt to attack any system that has not been specifically designed for that purpose in this class.
4. **Inclusion.** This classroom is a place where you will be treated with respect, and I welcome individuals of all ages, backgrounds, beliefs, ethnicities, genders, gender identities, gender expressions, national origins, religious affiliations, sexual orientations, ability – and other visible and nonvisible differences. All members of this class are expected to contribute to a respectful, welcoming and inclusive environment for every other member of the class.
5. **Accommodations for Students with Documented Disabilities.** If you are a student with a disability or believe you might have a disability that requires accommodations, requests for accommodations must be made in a timely fashion to Disability & Access Services, 25 Buick St, Suite 300, Boston, MA 02215; 617-353-3658 (Voice/TTY). Students seeking academic accommodations must submit appropriate medical documentation and comply with the established policies and procedures *http://www.bu.edu/disability/accommodations/*