**Csc 38000 Computer Security Fall 2024**

# Class Hours: Tuesday, Thursday 2:00 – 3:15 pm

**Tuesday, Thursday 3:30 – 4:45 pm**

**Instructor**

Saurabh Sachdeva Available Via email/Zoom

E-mail: [ssachdeva@ccny.cuny.edu](mailto:ssachdeva@ccny.cuny.edu)

**Office hours:**

Zoom Link: https://ccny.zoom.us/j/89185589102?pwd=k8jwyjdETLXM5aewaFkDAbeA94apEG.1

Csc 38000 – P - Wednesday 11 am – 12 pm

Csc 38000 - R - Wednesday 12 pm – 1 pm

### **Specific course information**

* An introduction to computer security. The student will develop the ability to reason about security in a variety of practical contexts and will learn best practices for mitigating threats and implementing secure systems. Topic will include software and hardware security, network security and protocols, operating systems security, and elemental cryptography.
* Prereq.: [CSc 21100](https://www-cs.ccny.cuny.edu/~akira/ABET-2022/Docs/Syllabi/21100.html) and [CSc 22000](https://www-cs.ccny.cuny.edu/~akira/ABET-2022/Docs/Syllabi/22000.html)
* Required course

# Graded Work

Class Assignments: 30% Final Examination : 40%

Midterm: 30%

A+: 97~100; A: 93~96; A-: 90~92; B+: 87~89; B: 83~86; B-: 80~82; C+: 77~79; C: 73~76; C-: 70~72; D: 60~69; F: under 60

### **Specific goals for the course and Relationship to student outcomes**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | |  | **1** | **2** | **3** | **4** | **5** | **6** | | a. knowledge of best practices for mitigating and preventing software security  vulnerabilities | R | R |  | P |  | R | | b. understanding of elementary concepts in cryptography, and gain practical  knowledge and experience in using cryptographic primitives | I | I |  | P | R | I | | c. awareness of the most common network security threats, including the required  resources, the extent to which they can be mitigated, and the available  countermeasures when applicable | P | R |  | P |  | R | | d. knowledge of best practices for securing a modern operating system, including  practical techniques in isolation and sandboxing | P | P |  | P |  | R | |
| |  | | --- | | I - introductory-level; R - reinforced-level; P - program-level | |

**Midterm and Final Examination:** We will have a Midterm and Final Exam. The format and the details shall be discussed in Class

CONTINUED ON REVERSE

### **Brief list of topics to be covered**

|  |  |
| --- | --- |
| **Week** | **Topics** |
| 1 | Introduction, Basic definitions of models |
| 2 | Stack smashing attacks and control-flow integrity: Return to libc attacks |
| 3 | Stack smashing attacks and control-flow integrity: Return Oriented Programming; ASLR, Non executable stacks (W^X), canaries |
| 4 | Hardware vulnerabilities and side-channel attacks: Spectre; Meltdown and Raw Hammer |
| 5 | Hardware vulnerabilities and side-channel attacks: Cold boot attacks |
| 6 | Elementary cryptography: Symmetric and asymmetric encryption |
| 7 | Elementary cryptography: Hashing, MACs, signatures |
| 8 | Authentication |
| 9 | Network security and protocols: TCP/IP, TLS/HTTPS, Certificate transparency logs |
| 10 | Network security and protocols: SSH |
| 11 | Network security and protocols: DoS attacks; IP Spoofing |
| 12 | Principle of Least Privilege; Privilege separation |
| 13 | Isolation and Sandboxing |
| 14 | Contemporary tools |