CS396: Security, Privacy & Society

Fall 2022

Lecture 1: Introduction

Instructor: Abrar Alrumayh

September 2, 2022

Today

- Course logistics
  - topic of study, enrollment eligibility, sessions
  - staff, learning materials, course organization
  - expectations, grading, policies, announcements
  - syllabus overview, course objectives/outcomes

CS396: Security, Privacy, and Society

"**Security**" [= "information security" = "computer security" = "cybersecurity"]

- protection of information systems from theft or damage to the hardware, software, or information stored on them, and from disruption or misdirection of the services they provide

"**Privacy**"

- ability of individuals to seclude inherently special/sensitive information to them, and express themselves selectively
- partially overlapping with security – regarding appropriate use and protection of information
- lawful right of not be subjected to unsanctioned invasions against such ability by third parties

"**Society**"

- group of individuals interacting persistently over shared territorial, political & cultural domains

CS396: Security, Privacy, and Society

- This course presents:
  - the basic concepts of computer security
  - the different vulnerabilities that can occur throughout a system
  - how malicious attackers exploit these vulnerabilities
  - the defenses that can prevent or mitigate an attack
  - the consequences and costs of attacks to individuals, organizations and societies.

CS396: Who can take it

- **Undergraduate** course
- Prerequisite course is **CS 392** (Systems Programming)
- **Required** course for Computer Science concentration
  - in study plans of CS juniors
- **Full-credit** course (w/ grade)

CS396: Lectures & labs

CS396 is offered in **2 required sessions**, each offered in **multiple sections**

- lectures
  - CS396-A M,W,F 9:00am - 9:50am Babbio 122
  - CS396-B M,W,F 11:00am - 11:50am Gateway North 204
  - CS396-C M,W,F 12:00am - 12:50am Gateway North 204
- labs
  - CS396-Lx Thu x = A, B, ..., L (10 sections)

CS396: Staff

- Instructor
  - **Abrar Alrumayh**
  - Contact Info: aalrumay@stevens.edu
  - Online Hours: I will be available via email and respond as soon as I am available (generally within 24)
  - Virtual office hours: Tuesdays from 1 - 3 pm or by appointment.
  - Zoom link: https://stevens.zoom.us/j/93658722163
- Teaching assistants
  - assistance w/ labs, assignments, “help sessions” as needed, some grading, demos
  - TAs & office hours: TBA

CS396: COURSE FORMAT AND STRUCTURE

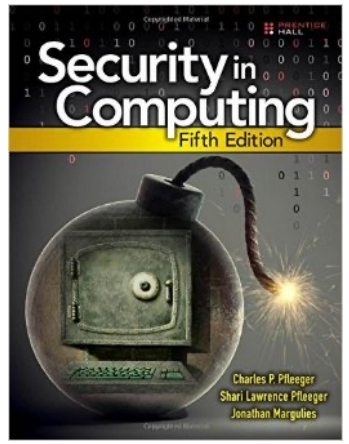
- This course is on-campus
- Course materials will appear on Canvas, To access the course, please visit stevens.edu/canvas .

CS396: Course organization

- **Weekly lectures**
  - materials covered via presentations, demos and whiteboard or in-class discussions
- **Weekly labs**
  - guided recitation of basic concepts, discussions, preparation of homework sets
- 3 - 4 homework sets
  - revision and application of covered materials
- TA hours
- Office hours by instructor

CS396: Learning materials

- Lectures
  - lecture notes: slides in pdf available online before class
  - additional materials covered via demos and whiteboard or in-class discussions
- Lab & homework assignments
  - Canvas quizzes, practice code, online resources
- Optional textbook
  - *Security in Computing*, 5th edition,
    by Pfleeger, Pfleeger & Margulies, Prentice Hall
  - available as hardcopy or e-book



CS396: Grading Procedures (tentative*)

- Grades will be based on:

Class Participation (attendance & in-class quizzes)	**20%**
Homework assignments	40%
Exam 1 (midterm)	20%
Exam 2 (final)	20%

- Tentative* grading scheme

A	90-100
B	80-89
C	70-79

CS396: Course workload

- Attend lectures & participate
  - e.g., you are expected to ask questions and provide comments
- Attend labs (and finish your work!)
- Hand-in homework assignments
- Pass exams
- Work independently (unless otherwise explicitly specified)
  - collaboration policy is governed by Honor System
- Provide feedback

Undergraduate Honor System

- Enrollment into the undergraduate class of Stevens Institute of Technology signifies a student's commitment to the Honor System. Accordingly, the provisions of the Stevens Honor System apply to all undergraduate students in coursework and Honor Board proceedings. It is the responsibility of each student to become acquainted with and to uphold the ideals set forth in the Honor System Constitution. More information about the Honor System including the constitution, bylaws, investigative procedures, and the penalty matrix can be found online at http://web.stevens.edu/honor/

CS396: Policies

- Attendance of lectures & labs is required
  - only one missed lab is allowed
  - there are no make-up labs or quizzes
- Laptops
  - **required**
- Late assignments
  - 10% per-day reduction

CS396: Announcements

- No lab session this week
- TA hours & office hours will start next week, from Monday, September 12

CS396: Tentative Course Schedule

Week	Topics
1	Introduction
2	Cryptography systems I
3	Cryptography systems II
4	Cryptography systems III
5	Applications
6	System security
7	Network security

CS396: Tentative Course Schedule

Week	Topics
8	**Midterm**
9	Software security
10	Web & cloud security
11	Privacy
12	Legal & ethical issues
13	Special topics
14	On-going tech/society challenges
15	**Final**

* w/ focus on what covered after midterm

CS396: Course outcomes

- **Cryptographic Systems:** Compare and contrast private and public key cryptosystems, and the strengths and potential pitfalls of cryptographic systems. [Analysis]

- **Systems Software:** Illustrate and detect vulnerabilities in systems, explain how attacks may exploit these vulnerabilities and explain what defense mechanisms can detect or prevent such attacks. Explain the concept of malware, how it infects a system and how it may be defended against. [Development]

- **Data privacy and security:** Analyze access control mechanisms to restrict database access, and the use of cryptography to maintain the privacy of data stored in databases. [Professionalism]

CS396: Course outcomes (cont.)

- **Network security:** Evaluate standard protocols to secure network communications and how to use them in different scenarios. Describe vulnerabilities in networking protocols that can be used to attack organizations and how they can be detected or prevented. [Development]
- **Programming for security:** Analyze how programs inadvertently create security vulnerabilities, and how these can be detected and prevented at the design, implementation, or deployment stage. [Development]
- **Social Impact:** Describe the implications to individuals, organizations and society of malicious attacks on computer systems. [Professionalism]
- **Ethics:** Explain ethical issues in cybersecurity, and state how the job of a typical IT professional might be connected to major technology-related ethical issues of the day. [Professionalism]

Questions?
&
Attendance

STEVENS
INSTITUTE OF TECHNOLOGY
1870

STEVENS
INSTITUTE OF TECHNOLOGY
1870

THANK **YOU**

Stevens Institute of Technology
1 Castle Point Terrace, Hoboken, NJ 07030