STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

CS396 - Security, Privacy and Society

Department of Computer Science

Fall 2023

Instructor:	Abrar Alrumayh
Office:	Gateway S353
Contact Info:	aalrumay@stevens.edu
Office Hours:	MWF from 10:00 – 10:50 am and 2:00– 3:00 PM And by appointment
Course Schedule:	CS396-A: MWF 9:00am - 9:50 am (Edwin A. Stevens 330) CS396-B: MWF 11:00am - 11:50 am (North Building 105)
Course Web Address:	See Canvas
Prerequisite(s):	CS 392 (Systems Programming)

COURSE DESCRIPTION

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, and the consequences and costs of attacks to individuals, organizations and societies.
Topics include the security of cryptographic schemes, system software, networks, databases and programs, as well as the ethical, legal, and regulatory considerations surrounding data privacy and security.

STUDENT LEARNING OUTCOMES

After successful completion of this course, students will be able to:

- **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]
- **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]

COURSE FORMAT AND STRUCTURE

This course is comprised of three weekly lectures and weekly recitation sessions.

COURSE MATERIALS

Textbook (Optional):	*Security in Computing*, 5th edition, by Pfleeger, Pfleeger & Margulies, Prentice Hall
Lecture notes:	There will be slides in PDF available online on Canvas
Additional materials:	Covered via demos and whiteboard or in-class discussions

COURSE REQUIREMENTS

- **Attendance** is required, participation is mandatory.
- **Homework** There will be three (3) homework assignments throughout this course. Policy for late submissions: 2 points off for every hour past the deadline (After 48 hours, late work will not be accepted). If urgent or unusual circumstances prohibit you from submitting a homework assignment in time, please e-mail the instructor.
- **Recitations**: Recitations/ Labs must finished during the lab/recitation time. It will be posted at the beginning of recitation time, and it must be finished at the end of recitation time. There will not be a late submission for labs.
- **Exams** There will be two exams, a midterm, covering the first half of the course, and a final, covering the second half of the course.

GRADING PROCEDURES

There are 100 possible points that a student can earn in this course. Percentages are listed below.

Lab	20%
Research presentation & Participation	10%
Homework assignments	30%
Exam 1 (midterm)	20%
Exam 2 (final)	20%

TENTATIVE COURSE SCHEDULE

Week	Date	Topic(s)	Assignments
1	9/1	**Course logistics** o topic of study, course organization, learning materials & workload, objectives & outcomes, policies, tentative syllabus	
2	9/6, 9/8	**Introduction** • The 3 pillars of Security, Privacy & Society o definition of core concepts & their scope, how they intersect & why they interrelate • Security in the era of outsourced computation o threats in the *-as-a-service computing model, core security concepts, secure posture assessment & risk management for individuals & organizations *Real-world example: the Dyn DDoS attack*	
3	9/11, 9/13, 9/15	**Cryptographic Systems I** • Symmetric-key encryption o problem formulation, solution concept, Kerckhoff's principle, brute-force attacks, classical ciphers • An unbreakable cipher o perfect secrecy, One-Time Pad (OTP) encryption, security analysis & limitations • OTP encryption in practice o Computational security, pseudorandomness, stream & block ciphers, modes of operations, DES & AES • *Real-world example: cryptanalysis during WWII & cold war*	Lab 1
4	9/18, 9/20, 9/22	**Cryptographic Systems II** • Modern cryptography framework o formal definitions, precise assumptions, provable security • Message authentication o MACs, replay attacks, 3 MAC constructions • Cryptographic hash functions o Merkle-Damgård construction, birthday attacks, "Hash & Mac" & HMAC, SHA-2, application of cryptographic hashing to security *Real-world example: the RSA PRG crypto suite*	Lab 2 HW1 out
5	9/25,	**Cryptographic Systems III** • Public-key cryptography	Lab 3

	9/27, 9/29	o motivation, PK encryption & digital signatures, PKI & digital certificates • Specific PK-crypto schemes o number theory basics, discrete log problem & ElGamal encryption, factoring problem & RSA • PK cryptography in practice o key agreement, hybrid encryption, authenticated encryption, Web security (HTTPS, TLS) • *Real-world example: Quantum computers*	
6	10/2, 10/4, 10/6	Applied Cryptography • Database-as-a-service authentication model o Merkle tree, authenticated data structures • Blockchain technologies o blockchains, cryptocurrencies • Transparency logs o secure logging, fork consistency • *Real-world example: do you Crypto?*	Lab 4 HW1 due Friday 11:59pm
7	10/10, 10/11, 10/13	Tuesday, October 10, 2023. Monday Class Schedule. System Security • User authentication o secrets, biometric, tokens, federated identity management, SSO • Access control o authentication Vs. authorization, AC policies, discretionary Vs. mandatory AC models • Domain Name System security o DNS, DNSSEC, NSEC, NSEC3, NSEC5 *Real-world example: Privacy is dead, long live privacy*	Lab 5 HW 2 out
8	10/16, 10/18, 10/20	Network Security • The Dyn DDOS attack (revisited) o denial of service attacks, DDOS, IoT security • Information-based security o Advanced persistent threats, IDS & IPS systems, SIEM, security analytics • Cryptography in network security o TOR, VPNs, PillarBox, Falcon codes *Real-world example: Bias in AI algorithms*	Lab 6
9	10/23, 10/25, 10/27	Review + Midterm (10/25)	
10	10/30, 11/1, 11/3	Software Security • Programming oversights o buffer overflow attacks	Lab 7

		• Malware o viruses, trojans, worms • Secure programming o specification, testing, analysis *Real-world example: IoT/Smart devices collecting user data*	HW 2 due Friday 11:59pm
11	11/6, 11/8, 11/10	Web & Cloud Security • Brower security o authentication, identification, content integrity • Secure data outsourcing o searching over authenticated & encrypted data *Real-world example: Electronic voting*	Lab 8 HW3 out
12	11/13, 11/15, 11/17	Privacy • Database security • Information leakage *Real-world example: COVID tracking applications*	Lab 9
13	11/20	Legal & Ethical Issues • Copyright, patents, and trade secrets Thanksgiving Recess: No Classes (11/20 & 11/24)	
14	11/27, 11/29, 12/1	Legal & Ethical Issues • Legal protections related to computer security • Computer crime • Ethical issues related to computer security & professional codes of ethics *Real-world example: Backdoor in iPhone; Privacy Vs. National Security*	Lab 10 HW 3 due Friday 11:59pm
15	12/4, 12/6, 12/8	On-going Technical & Societal Challenges • Self-driving cars, VW emission scandal, the Social Media bubble, facial recognition issues, telemedicine, Google as search monopoly, Deep Fakes, cryptography as a state secret *Real-world example: Secure deletion & the right to be forgotten* *Real-world example: Censorship, Misinformation, Virtual Influencers, etc.*	Lab 11
16	12/11, 12/13	Final Exam Review	

ACADEMIC INTEGRITY

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/

The following pledge shall be written in full and signed by every student on all submitted work (including, but not limited to, homework, projects, lab reports, code, quizzes and exams) that is assigned by the course instructor. No work shall be graded unless the pledge is written in full and signed.

"I pledge my honor that I have abided by the Stevens Honor System."

Reporting Honor System Violations

Students who believe a violation of the Honor System has been committed should report it within ten business days of the suspected violation. Students have the option to remain anonymous and can report violations online at www.stevens.edu/honor.

GENERATIVE AI TECHNOLOGY:

While the vast majority of your work should be original, if at any point you use a (very small!) part of someone else's solution you MUST cite the source. Copying from other sources (online, classmates, ChatGPT, etc.) without citation results in an automatic zero for the assignment and additional possible penalties (including course failure and / or escalation to the Honor Board).

Any plagiarism or other form of cheating will be dealt with under relevant Stevens policies.

EXAM ROOM CONDITIONS

The following procedures apply to quizzes and exams for this course. As the instructor, I reserve the right to modify any conditions set forth below by printing revised Exam Room Conditions on the quiz or exam.

- During exams, you are not permitted to use notes, books, or computing or communication devices.
- Students are not allowed to work with or talk to other students during quizzes and/or exams.

LEARNING ACCOMMODATIONS

Stevens Institute of Technology is dedicated to providing appropriate accommodations to students with documented disabilities. The Office of Disability Services (ODS) works with undergraduate and graduate students with learning disabilities, attention deficit-hyperactivity disorders, physical disabilities, sensory impairments, psychiatric disorders, and other such disabilities in order to help students achieve their academic and personal potential. They facilitate equal access to the educational programs and opportunities offered at Stevens and coordinate reasonable accommodations for eligible students. These services are designed to encourage independence and self-advocacy with support from the ODS staff. The ODS staff will facilitate the provision of accommodations on a case-by-case basis.

For more information about Disability Services and the process to receive accommodations, visit https://www.stevens.edu/office-disability-services. If you have any questions please contact: Phillip Gehman, the Director of Disability Services Coordinator at Stevens Institute of Technology at pgehman@stevens.edu or by phone 201-216-3748.

Disability Services Confidentiality Policy

Student Disability Files are kept separate from academic files and are stored in a secure location within the Office of Disability Services. The Family Educational Rights Privacy Act (FERPA, 20 U.S.C. 1232g; 34CFR, Part 99) regulates disclosure of disability documentation and records maintained by Stevens Disability Services. According to this act, prior written consent by the student is required before our Disability Services office may release disability documentation or records to anyone. An exception is made in unusual circumstances, such as the case of health and safety emergencies.

INCLUSIVITY

Name and Pronoun Usage

As this course includes group work and class discussion, it is vitally important for us to create an educational environment of inclusion and mutual respect. This includes the ability for all students to have their chosen gender pronoun(s) and chosen name affirmed. If the class roster does not align with your name and/or pronouns, please inform the instructor of the necessary changes.

Inclusion Statement

Stevens Institute of Technology believes that diversity and inclusiveness are essential to excellence in academic discourse and innovation. In this class, the perspective of people of all races, ethnicities, gender expressions and gender identities, religions, sexual orientations, disabilities, socioeconomic backgrounds, and nationalities will be respected and viewed as a resource and benefit throughout the semester. Suggestions to further diversify class materials and assignments are encouraged. If any course meetings conflict with your religious events, please do not hesitate to reach out to your instructor to make alternative arrangements.

You are expected to treat your instructor and all other participants in the course with courtesy and respect. Disrespectful conduct and harassing statements will not be tolerated and may result in disciplinary actions.

Statement on Religious Observances

Stevens is a very diverse community in which many different religious and ethnic groups are represented. Religious observance is an important reflection of diversity. Stevens is committed to providing equal educational opportunities and supporting students of all belief systems. Students will not be subject to any grade penalties for missing a class, examination or any other course requirement due to a religious observance. Students will not be asked to choose between religious observance and academic work. Therefore, students should inform the instructor in the beginning of the semester if a requirement for this course conflicts with religious observance so that accommodations can be made for students to observe religious practices and complete the requirements for the course.

In addition, please remember that there are several holidays – such as Rosh Hashanah, Yom Kippur, the Mid-Autumn Festival, Diwali, the Lunar New Year, Holi, Passover, Good Friday, Easter Sunday, Eid al-Fatr and Eid al-Adha – that are observed by a significant portion of the Stevens community. Every effort must be made to avoid scheduling quizzes, exams and class presentations that conflict with these holidays.

The dates of many of these holidays are listed on Stevens' Academic Calendar and are shared with the Stevens community via email each semester. The Division of Human Resources sent an email with this information on August 8. Note that Rosh Hashanah, Yom Kippur, Holi, Passover, Eid al-Fitr and Eid al-Adha begin the evening before the listed date and end on the evening of the indicated date.

MENTAL HEALTH RESOURCES

Part of being successful in the classroom involves a focus on your whole self, including your mental health. While you are at Stevens, there are many resources to promote and support mental health. The Office of Counseling and Psychological Services (CAPS) offers free and confidential services to all enrolled students who are struggling to cope with personal issues (e.g., difficulty adjusting to college or trouble managing stress) or psychological difficulties (e.g., anxiety and depression). Appointments are can be made by phone (201-216-5177).

EMERGENCY INFORMATION

In the event of an urgent or emergent concern about the safety of yourself or someone else in the Stevens community, please immediately call the Stevens Campus Police at 201-216-5105 or on their emergency line at 201-216-3911. These phone lines are staffed 24/7, year round. For students who do not reside near the campus and require emergency support, please contact your local emergency response providers at 911 or via your local police precinct. Other 24/7 national resources for students dealing with mental health crises include the National Suicide Prevention Lifeline (1-800-273-8255) and the Crisis Text Line (text “Home” to 741-741). If you are concerned about the wellbeing of another Stevens student, and the matter is *not* urgent or time sensitive, please email the CARE Team at care@stevens.edu. A member of the CARE Team will respond to your concern as soon as possible.