CS 576 Systems Security Syllabus

Department of Computer Science/SES
Spring 2022

Lecture:	Monday 03:00pm-05:30pm
Location:	1/18-1/30 Online 1/31-5/2 McLean 104 (monitor Stevens and course announcements for changes)
Lab:	Thursday 5:00pm-05:50pm
Lab Location:	1/18-1/30 Online 1/31-5/4 McLean 218B (monitor Stevens and course announcements for changes)
Instructor:	Georgios Portokalidis
Office hours:	Friday 4:15-6:00pm (Online)
TA:	Yuchen (Dennis) Zhang
TA Office hours:	**TBD (TBD)**
Web:	https://www.portokalidis.net/cs576_f2022.html
Canvas:	https://sit.instructure.com/courses/56733
Communication:	Piazza

COURSE DESCRIPTION

This course will cover a wide range of topics in the area of Systems Security. A computer system is composed of software, hardware, policies, and practices. Systems security involves

both designing and building secure systems, as well as improving and evaluating the security of existing systems. This course is giving a particular emphasis into providing hands-on experience to students through building, attacking, and securing systems. The class is programming intensive. Those who take the class should be skill programmers and should have some experience with the C programming language and programming on a Linux environment. It is recommended that students are also familiar with the assembly language and with network and operating system basics.

STUDENT LEARNING OUTCOMES

After the completion of this course students will (a) know the principles that can help them design secure systems, (b) be able to analyze systems from a security perspective, (c) understand why and how attacks work, and (d) be able to build defenses.

Applying cryptography in systems development and identifying its limitations	[BS-CyS A apply] [BS-CyS K construction]
Describing authentication and access control mechanisms	[BS-CyS B analyze] [BS-CyS C design]
Describing control-flow hijacking attacks on software and deploying countermeasures	[BS-CyS A apply] [BS-CyS B analyze] [BS-CyS C design] [BS-CyS I currency]
Describing attacks against web applications and deploying countermeasures	[BS-CyS A apply] [BS-CyS B analyze] [BS-CyS C design]
Describing and deploying network-level defenses	[BS-CyS A apply] [BS-CyS B analyze] [BS-CyS G impact]

COURSE FORMAT AND STRUCTURE

The course involves a lecture and a lab section (you must separately register for that). The course will be in person, but some lectures/labs may be online as demanded by circumstances.

To access the course, please visit stevens.edu/canvas. For more information about course access or support, contact the TRAC by calling 201-380-6599 or 201-216-5500.

Communication

This term we will be using Piazza for class discussion. The system is highly catered to getting you help fast and efficiently from classmates, the TA, and the instructor. Rather than emailing questions to the teaching staff, I encourage you to post your questions on Piazza. If you have any problems or feedback for the developers, email team@piazza.com. Piazza will also be used during lectures for live Q&A with the instructor.

Online Etiquette Guidelines

Your instructor and fellow students wish to foster a safe online learning environment. All opinions and experiences, no matter how different or controversial they may be perceived, must be respected in the tolerant spirit of academic discourse. You are encouraged to comment, question, or critique an idea but you are not to attack an individual. Our differences, some of which are outlined in the University's inclusion statement below, will add richness to this learning experience. Please consider that sarcasm and humor can be misconstrued in online interactions and generate unintended disruptions. Working as a community of learners, we can build a polite and respectful course ambience. Please read the Netiquette rules for this course:

- Do not dominate any discussion. Give other students the opportunity to join in the discussion.
- Do not use offensive language. Present ideas appropriately.
- Be cautious in using internet language. For example, do not capitalize all letters since this suggests shouting.
- Avoid using vernacular and/or slang language. This could possibly lead to misinterpretation.
- Keep an open mind and be willing to express even your minority opinion.
- Think and edit before you push the “Send” button.
- Do not hesitate to ask for feedback.

Office Hours

The TA and instructor will both have office hours either in-person or over a synchronous session (through Zoom) to discuss questions related to weekly readings and/or assignments. If both in-person and virtual office hours are needed the time will be divided between the two. Office hours are TBD.

COURSE REQUIREMENTS

Exploitation project	A large exploitation assignment to be done at home. It will be due 1-2 weeks before the last lecture of the semester.
Lab (schedule)	Exploitation and programming tasks performed during the lab section.
Exams	One midterm and one final exam.

COURSE MATERIALS

Readings:

- Articles given by the instructor each week

- Lecture slides

Suggested books:

- The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd Edition, Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte, ISBN: 978-0-470-08023-8
- Hacking: The Art of Exploitation, 2nd Edition. Jon Erickson. No Starch Press, 2008, ISBN 1593271441

Google cloud-hosted virtual machine (VM)

COURSE SCHEDULE

Topic	**Reading**
Introduction to software systems security	TBD
Command injection and path traversal vulnerabilities	TBD
Web: XSS, CSRF, and SQL injection vulnerabilities	TBD
Introduction to C/C++ vulnerabilities: overflows and other memory corruption bugs	TBD
Exploitation primer: ELF binaries, x86 assembly, disassembling and debugging	TBD
Smashing the stack: stack overflows and shellcoding	TBD
Defenses: Data Execution Prevention (DEP), Address space layout randomization (ASLR), Stack Canaries.	TBD
Format string vulnerabilities	TBD
Code-reuse attacks: return-to-libc, return-oriented programming	TBD
Other exploitable pointers in C/C++ programs and more defenses	TBD
Use-after-free, type confusion, and uninitialized memory vulnerabilities	TBD
Control-flow Integrity (CFI) and data-only attacks	TBD

Network: Internet worms, firewalls, and monitoring	TBD
How do software vulnerabilities affect authentication and access control? (Sandboxing and privilege escalation attacks)	TBD
Non-cryptographic attacks against cryptosystems.	TBD
Optional topics: botnets, distributed denial of service attacks, heap spraying, hardware vulnerabilities, Rust	TBD

GRADING PROCEDURES

Grades will be based on:

Exploitation project	20%
Labs	30%
Midterm exam	25%
Final exam	25%

You will **not** need a 97% to get an A in this course. Generally, A corresponds to excellent performance, B to good, C to fair, and F to failure to understand the basics.

Late Policy

Deadlines are an unavoidable part of being a professional and this course is no exception. Course requirements must be completed and posted or submitted on or before specified due date and delivery time deadline. Due dates and delivery time deadlines are defined as Eastern Time (as used in Hoboken, NJ). Please note, students living in distance time zones or overseas must comply with this course time and time and due date deadline policy. Avoid any inclination to procrastinate. To encourage you to stay on schedule, due dates have been established for each assignment and the project.

ACADEMIC INTEGRITY

Graduate students in 500-level courses are bound by the Graduate Student Code of Academic Integrity, while undergraduate students in those courses have special provisions that have been agreed upon by the Dean of Graduate Academics and the Honor Board.

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.

Graduate Student Code of Academic Integrity

All Stevens graduate students promise to be fully truthful and avoid dishonesty, fraud, misrepresentation, and deceit of any type in relation to their academic work. A student’s submission of work for academic credit indicates that the work is the student's own. All outside assistance must be acknowledged. Any student who violates this code or who knowingly assists another student in violating this code shall be subject to discipline.

All graduate students are bound to the Graduate Student Code of Academic Integrity by enrollment in graduate coursework at Stevens. It is the responsibility of each graduate student to understand and adhere to the Graduate Student Code of Academic Integrity. More information including types of violations, the process for handling perceived violations, and types of sanctions can be found at www.stevens.edu/provost/graduate-academics.

Special Provisions for Undergraduate Students in 500-level Courses

The general provisions of the Stevens Honor System do not apply fully to graduate courses, 500 level or otherwise. Any student who wishes to report an undergraduate for a violation in a 500-level course shall submit the report to the Honor Board following the protocol for undergraduate courses, and an investigation will be conducted following the same process for an appeal on false accusation described in Section 8.04 of the Bylaws of the Honor System. Any student who wishes to report a graduate student may submit the report to the Dean of Graduate Academics or to the Honor Board, who will refer the report to the Dean. The Honor Board Chairman will give the Dean of Graduate Academics weekly updates on the progress of any casework relating to 500-level courses. For more information about the scope, penalties,

and procedures pertaining to undergraduate students in 500-level courses, see Section 9 of the Bylaws of the Honor System document, located on the Honor Board website.

EXAM 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.

1. Students may use the following materials during quizzes and exams. Any materials that are not mentioned in the list below are not permitted.

Material	**Permitted?**	
	Yes	No
Handwritten Notes		X
Typed Notes		X
Textbooks		X
Readings		X

2. Students **are not** allowed to work with or communicate with other students during quizzes and exams.

LEARNING ACCOMMODATIONS

Stevens Institute of Technology is dedicated to providing appropriate accommodations to students with documented disabilities. Student Counseling and Disability Services works with undergraduate and graduate students with learning disabilities, attention deficit-hyperactivity disorders, physical disabilities, sensory impairments, and psychiatric disorders 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 SCDS staff. The SCDS staff will facilitate the provision of accommodations on a case-by-case basis. These academic accommodations are provided at no cost to the student.

Disability Services Confidentiality Policy

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.

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.

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). CAPS is open daily from 9:00 am – 5:00 pm M-F. Evening hours are available by appointment in the Fall / Spring semesters and up-to-date information regarding the availability of evening appointments can be found by visiting www.stevens.edu/CAPS (Links to an external site.). To schedule an appointment, call 201-216-5177.

Due to the pandemic, in-person appointments may be limited until further notice. Up-to-date information about the availability of in-person services can be found at www.stevens.edu/CAPS (Links to an external site.). Teletherapy (therapy via secure video platform) is available to registered students physically located in the states of New York or New Jersey. Students located outside of NY / NJ are encouraged to pursue local treatment through their personal health insurance. To learn more about the process of finding a therapist please visit the CAPS webpage on Seeking Help Off-Campus (Links to an external site.).

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.