CS 576 Systems Security

CS/SES
Fall 2016

Lecture:	Tuesdays 06:15pm-08:45pm
Lab:	Thursdays 04:00pm-04:50pm
Classroom Location:	TBA
Instructor:	Georgios Portokalidis
TA:	Ioannis Agadakos
Office Hours:	By appointment (Lieb 214)
Course Web Address:	http://www.cs.stevens.edu/~gportoka/cs576.html
Canvas:	https://sit.instructure.com/courses/14582
Prerequisite(s):	(Graduate students) CS-631 Advanced Programming in the UNIX Environment or (Undergraduate students) CS-306 Introduction to IT Security and CS-392 Systems Programming

COURSE DESCRIPTION

This course will cover a wide range of topics in the area of Systems Security. A computer system is composed by 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 skilled 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.

LEARNING OBJECTIVES

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]

FORMAT AND STRUCTURE

The course involves lectures, a lab section, and weekly assignments. The course requires significant programming effort.

COURSE MATERIALS

Textbooks (optional): Computer Security: Principles and Practice, 3/E, William Stallings, Lawrie Brown ISBN-10: 0133773922 • ISBN-13: 9780133773927

Security Engineering 2nd Edition by Ross Anderson

Textbooks (recommended): 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

Other materials (required): Slides used in lectures and papers referenced in them

COURSE REQUIREMENTS

Homework	Individual programming assignments given out weekly
Lab Work	Attending and completing tasks during the lab section
Exams	There is going to be one midterm exam (Exam I) and a final exam (Exam II).

GRADING PROCEDURES

Grades will be based on:

Quizzes	(10%)
Home Work	(50%)
Exam I	(20%)
Exam II	(20%)

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, indicating certain understanding problems, but understanding of the basics, and F to failure to understand the basics.

After submitting an assignment, you need meet with the TA to go over the assignment on canvas. Your grade will be determined based on the correctness of the submitted solution and your ability to explain what you did to the TA. *Meetings with the TA for grading the assignments are mandatory. Failure to meet with the TA on time is the same as not submitting the assignment.*

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.

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 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.

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

Device	**Permitted?**	
	Yes	No
Laptops		X
Cell Phones		X
Tablets		X
Smart Watches		X
Google Glass		X

2. 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

3. Students **are not** allowed to work with or talk to other students during quizzes and/or exams.

LEARNING ACCOMODATIONS

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

Student Disability Files are kept separate from academic files and are stored in a secure location within the office of Student Counseling, Psychological & 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.

For more information about Disability Services and the process to receive accommodations, visit https://www.stevens.edu/sit/counseling/disability-services. If you have any questions please contact:

Lauren Poleyeff, Psy.M., LCSW - Disability Services Coordinator and Staff Clinician in Student Counseling and Disability Services at Stevens Institute of Technology at lpoleyef@stevens.edu or by phone (201) 216-8728.

INCLUSIVITY STATEMENT

Stevens Institute of Technology believes that diversity and inclusiveness are essential to excellence in education and innovation. Our community represents a rich variety of backgrounds, experiences, demographics and perspectives and Stevens is committed to fostering a learning environment where every individual is respected and engaged. To facilitate a dynamic and inclusive educational experience, we ask all members of the community to:

- be open to the perspectives of others
- appreciate the uniqueness their colleagues
- take advantage of the opportunity to learn from each other
- exchange experiences, values and beliefs
- communicate in a respectful manner
- be aware of individuals who are marginalized and involve them
- keep confidential discussions private

TENTATIVE COURSE SCHEDULE

	Topic(s)	**Additional Reading(s)**	**HW**
8/30/2016	Authentication and access control	Chapter 3	Assignment given
9/6/2016	How software executes: from idea to machine-level code. Memory safety.	Chapter 10 & 11	
9/13/2016	Memory corruption attacks. Control-flow hijacking and code injection.	Chapter 10 & 11, Handbook	Assignment given
9/20/2016	Early software defenses	Chapter 10 & 11, Handbook	

9/27/2016	Modern exploitation. Heap spraying, ROP, etc.	Handbook	Assignment given
10/4/2016	Control-flow Integrity		
10/18/2016	Midterm (Exam I)		
11/1/2016	Basic crypto and system failures of crypto systems	Stallings, Chapter 2 & 22	Assignment given
11/22/2016	Malware (Viruses, worms, etc.)	Chapter 6	
11/8/2016	Web security	Chapter 5	Assignment given
10/25/2016	Mobile security	Chapter 24	
11/15/2016	Firewalls and network intrusion detection	Chapter 8 and 9	Assignment given
11/29/2016	OS security, sandboxing	Chapter 12	
12/6/2016	Denial of service, Botnets	Chapter 7	
TBD	Final (Exam II)		