CS 576 Secure Systems

CS/SES
Fall 2015

Meeting Times:	Tuesdays 06:15pm-08:45pm
Classroom Location:	Babbio Center 310
Instructor:	Georgios Portokalidis
Contact Info:	Lieb 213
Office Hours:	By appointment
Course Web Address:	http://www.cs.stevens.edu/~gportoka/cs576.html
Prerequisite(s):	Graduate students: CS 506 Introduction to IT Security (test-out option available) and CS 590 Algorithms / Undergraduate students: CS 385 Algorithms or CS 182 Introduction to Computer Science Honors II
Corequisite(s):	CS 577 Cybersecurity Lab

COURSE DESCRIPTION

Attacks on computer systems have become part of everyday life. It is the goal of this class to teach a thorough understanding of the possible security failures, as well as the protection mechanism. The class will cover network and host security concepts and mechanisms; basic cryptographic algorithms and protocols; authentication and authorization protocols; access control models; common network (wired and wireless) attacks; typical protection approaches, including firewalls and intrusion detection systems; and operating systems and application vulnerabilities, exploits, and countermeasures; distributed denial of service attacks and botnets. The class will not only cover the subjects in theory but instead also provide the students with an extensive hands-on experience. The class will involve a fair amount of programming. Those who take the class are expected to be able to program in C/C++, have some basic knowledge of assembly language, and be familiar with network basics and programming, as well as Unix-like operating systems.

LEARNING OBJECTIVES

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

- Explain the attacks on basic cryptographic algorithms and protocols in the context of networked computer systems.
- Explain the security models, including the access control matrix and role-based access control. Explain where cryptography cannot help with system security.

- Explain the limits of intrusion detection (both signature-based and anomaly-based) and firewalls. In particular how do intrusion detection systems and firewalls fail?
- Explain exploits of systems and networks (including DDoS attacks), and why they still affect us today.
- Explain some countermeasures to system and network attacks, including deceptive techniques.
- Explain the intricacies of malware, including obfuscation techniques to defeat detection at both host and network levels.
- Explain the use of both technical and non-technical means of securing a networked site.

FORMAT AND STRUCTURE

The course involves lectures and a final project including significant programming effort.

COURSE MATERIALS

Textbook(s):	Computer Security - Principles and Practice 3rd Edition by William Stallings and Lawrie Brown
Other Readings:	Security Engineering 2nd Edition by Ross Anderson
Materials:	Slides used in lectures and papers referenced in them

COURSE REQUIREMENTS

Participation	Highly encouraged but not graded.
Quizzes	Pop quizzes will be given during the course of the semester
Project(s)	The students are called to demonstrate what they have learned in this course by completing a project that includes building a significant piece of software. This way students learn both to secure a system they build, as well as create a system that improves security. Students will form teams of three-four students. The maximum size of teams will be decided after the final number of students taking the course is finalized to ensure not students are equally distributed in teams.
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%)
Team Project	(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.

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

Week #	Topics	Readings (beyond slides)	Project Milestones
1	Course logistics. Overview. Legal and ethical aspects. Management aspects. The human factor.	Chapter 1, 19, 14, 15, 17	
2	Basic crypto. Message authentication. Hashing. Random number generation.	Chapter 2, 20, 21 Appendix D	
3	Authentication. Access control, authorization. PKI. Certificate authorities. Biometrics.	Chapter 3, 4, 23	Proposal due 6pm on Tuesday
4	Buffer overflows. Stack smashing. Heap overflows. Format string attacks. Code injection. Return-to-libc attacks.	Chapter 10, 11	Design due 6pm on Ruesday
5	ASLR. Heap-spraying. Return-oriented programming. Use-after-free.	Articles provided in classroom	
6	Firewalls. Network intrusion detection. Honeypots.	Chapter 8,9	

7	Midterm (On Thursday instead of CS-577)		
8	Malware. Obfuscation. Drive-by downloads. Sandboxing. DoS	Chapter 6, 7	Alpha system due 6pm on Tuesday
9	Control-flow integrity.		
10	Mobile security - Guest lecturer	Articles provided in classroom	
11	Web and database security. SQL injection, XSS, CSRF.	Chapter 5	Beta system due 6pm on Tuesday
12	Physical and infrastructure security. Hardware security	Chapter 16	
13	CS-577 lab instead of lecture.		
14	OS security. Null-pointer dereferences. Code-integrity	Articles provided in classroom	Final system due 6pm on Tuesday
15	Final project presentation and demo		