CS 576 Systems Security Syllabus

Department of Computer Science
Fall 2018

Lecture:	Monday 06:15pm-08:45pm (North Building 102)
Instructor:	Georgios Portokalidis
Lab:	Thursday 03:05pm-04:55pm (North Building 102)
TA:	Rahul Yadav
Web:	https://www.portokalidis.net/cs576.html
Communication:	https://piazza.com/stevens/fall2018/cs576/home
Canvas:	https://sit.instructure.com/courses/28802

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, hands-on labs, two exams, and software-based project. The course requires significant programming effort.

COURSE MATERIALS

Items in reading list (found in the course's schedule)

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

Security Engineering 2nd Edition by Ross Anderson

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

COURSE REQUIREMENTS

Exams	There is going to be one midterm exam (Exam I) and a final exam (Exam II).
Assignments	There are going to be 5-7 homework assignments that will be done individually or in small groups of two.
Lab	Hands-on training and tasks performed during the lab section.
Quizzes	Students will be asked to take an online quiz after each week's lecture, based on the reading list.

GRADING PROCEDURES

Grades will be based on:

Exam I	(25%)
Exam II	(25%)
Quizzes	(10%)
Lab participation	(10%)
Assignments	(30%)

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.

COMMUNICATING

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.

ACADEMIC INTEGRITY

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

Date	Topics	Reading	
	Introduction		
8/27/2018	Introduction		
	Software Security and Exploitation		
8/27/2018	Introduction to assembly, program memory layout, debugging	x86 Assembly	https://en.wikibooks.org/wiki/X86_Assembly
		Anatomy of a Program in Memory	https://manybutfinite.com/post/anatomy-of-a-program-in-memory/
		x86 calling conventions	https://en.wikipedia.org/wiki/X86_calling_conventions
		Beej's Quick Guide to GDB	https://beej.us/guide/bggdb/
		Call Stack	https://en.wikipedia.org/wiki/Call_stack
		Journey to the Stack	https://manybutfinite.com/post/journey-to-the-stack/
9/10/2018	Early memory corruption attacks	Smashing the stack for fun and profit	http://phrack.org/issues/49/14.html#article
		Introduction to Writing Shellcode	https://www.exploit-db.com/papers/13224/
		Linux assemblers	https://www.ibm.com/developerworks/library/l-gas-nasm/
		Online assembler	https://defuse.ca/online-x86-assembler.htm
		Stackguard	ftp://gcc.gnu.org/pub/gcc/summit/2003/Stackguard.pdf
9/17/2018	Early defenses and more attacks	Bypassing StackGuard and StackShield	http://phrack.org/issues/56/5.html
		w00w00 on Heap Overflows	https://www.cgsecurity.org/exploit/heaptut.txt
		Address Space Layout Randomization (ASLR)	https://0x00sec.org/t/exploit-mitigation-techniques-address-space-layout-randomization-aslr/5452
		Bypassing PaX ASLR protection	http://phrack.org/issues/59/9.html
		Exploiting Format String Vulnerabilities	https://www.win.tue.nl/~aeb/linux/hh/formats-teso.html
		Executable space protection	https://en.wikipedia.org/wiki/Executable_space_protection
		The advanced return-into-lib(c)	http://phrack.org/issues/58/4

		exploits	.html#article
9/24/2018	Modern exploitation and defenses	Chained return-to-libc	https://sploitfun.wordpress.com/2015/05/08/bypassing-nx- bit-using-chained-return-to-libc/
		Practical return-oriented programming	https://trailofbits.files.wordpress.com/2010/04/practical-rop.pdf
		Heap spraying	https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/
		Heap feng-shui	https://www.blackhat.com/presentations/bh-europe-07/Sotirov/Presentation/bh-eu-07-sotirov-apr19.pdf
		Control-flow integrity	https://en.wikipedia.org/wiki/Control-flow_integrity
10/1/2018	More defenses, sandboxing	Chromium sandbox	https://chromium.googlesource.com/chromium/src/+/b4730a0c2773d8f6728946013eb812c6d3975bec/docs/design/sandbox.md
		seccomp	https://wiki.mozilla.org/Security/Sandbox/Seccomp
		Software-based Fault Isolation	https://www.cs.cornell.edu/courses/cs513/2007fa/L13.html
		Adapting Software Fault Isolation to Contemporary CPU Architectures	https://ai.google/research/pubs/pub35649.pdf
		Native Client: A Sandbox for Portable, Untrusted x86 Native Code	https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/34913.pdf
	Web		
10/9/2018	Introduction to web, TLS/SSL, certificates	An overview of HTTP	https://developer.mozilla.org/en-US/docs/Web/HTTP/Overview
	Tuesday instead of Monday	HTTP: Response Codes	https://dev.opera.com/articles/http-response-codes/
		Multitier architecture	https://en.wikipedia.org/wiki/Multitier_architecture
		DNS Explained	https://scotch.io/tutorials/dns-explained-how-your-browser-finds-websites
		Transport Layer Security (TLS)	https://hpbn.co/transport-layer-security-tls/
		Analysis of the HTTPS Certificate Ecosystem	http://conferences.sigcomm.org/imc/2013/papers/imc257

			-durumericAemb.pdf
		TLS attacks	https://mitls.org/pages/attacks
10/15/2018	Midterm		
10/22/2018	Authentication and access control	The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes	https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf
		Dos and Don'ts of Client Authentication on the Web	https://pdos.csail.mit.edu/papers/webauth:sec10.pdf
		Designing an Authentication System: a Dialogue in Four Scenes	http://web.mit.edu/Kerberos/dialogue.html
10/29/2018	Web security	Regular Expressions Considered Harmful in Client-Side XSS Filters	http://www.adambarth.com/papers/2010/bates-barth-jackson.pdf
		Robust Defenses for Cross-Site Request Forgery	http://www.adambarth.com/papers/2008/barth-jackson-mitchell-b.pdf
		Excess XSS	https://excess-xss.com/
		Cross Site Request Forgery	https://www.isecpartners.com/media/11961/CSRF_Paper.pdf
		Blind Sql Injection with Regular Expressions Attack	https://www.exploit-db.com/docs/english/17397-blind-sql-injection-with-regular-expressions-attack.pdf
		Content Security Policy	https://developers.google.com/web/fundamentals/security/csp/
11/5/18	Malware, botnets	How to 0wn the Internet in Your Spare Time	https://www.usenix.org/legacy/event/sec02/full_papers/staniford/staniford.pdf
		Manufacturing Compromise: The Emergence of Exploit-as-a-Service	http://cseweb.ucsd.edu/~savage/papers/CCS12Exploit.pdf
		Drive-by download	https://en.wikipedia.org/wiki/Drive-by_download
		Scareware	https://en.wikipedia.org/wiki/Scareware
		Understanding and fighting evasive malware	https://www.rsaconference.com/writable/presentations/file_upload/hta-w10-understanding-and-fighting-evasive-malware_copy1.pdf
		Botnet	https://en.wikipedia.org/wiki/

			Botnet
		Linux userland rootkits	https://ketansingh.net/overview-on-linux-userland-rootkits/
		Kernel rootkits	https://pdfs.semanticscholar.org/presentation/09a2/485eccb32488cc8c8a496dc63375c80b38aa.pdf
	Network Security		
11/12/2018	Network defenses	Bro intrusion detection system	https://www.usenix.org/legacy/publications/library/proceedings/sec98/full_papers/paxson/paxson.pdf
		Computer Security book: Chapter 9	
		SweetBait: Zero-hour worm detection and containment using low- and high-interaction honeypots	https://www.portokalidis.net/files/sweetbait_tr05.pdf
11/19/2018	Denial of service	IP-Spoofing Demystified	http://phrack.org/issues/48/14.html
		Inferring Internet Denial-of-Service Activity	http://cseweb.ucsd.edu/~savage/papers/UsenixSec01.pdf
		China's Great Cannon	https://citizenlab.ca/2015/04/chinas-great-cannon/
		A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms	https://www.isi.edu/~mirkovic/publications/ucla_tech_report_020018.pdf
11/26/2018	Other topics (case studies, recent advances, niche topics)		
12/3/2018	Final **		