CSE 509 : Computer System Security

Syllabus

Term: Fall 2021
Instructor: Tony Mione
Course Meeting Times: Tue & Thur, 3:30 – 4:50 PM
Office: B425
Phone: +82 032-626-1226
Email: antonino.mione@sunykorea.ac.kr
Office Hours:
Mon/Wed: 11:00-12:00 & 1:00-2:00PM, Tue/Thu: 1:00-2:00 PM

Course Homepage: www3.cs.stonybrook.edu/~amione/CSE509_Course/index.html
Recommended References:

- Stamp, Mark, *Information Security: Principles and Practice (2nd Edition),* Wiley, 2011, ISBN: 978-0-470-62639-9.

- Anderson, Ross, *Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition*, Wiley Publishing, Inc., 2008, ISBN: 978-470-06852-6 [https://www.cl.cam.ac.uk/~rja14/book.html]

Course Overview

Understanding the basics of computer security is essential for any technology worker today. There are persistent threats 'in the wild' seeking to break security, extract information, corrupt data, or hold data for ransom. These attacks are possible due to weaknesses primarily in software supporting modern complex systems but they may also occur in hardware.

In the class, we will discuss the principles and practice of computer system security, with particular emphasis on:

- software vulnerabilities and advances in exploit techniques
- source-code and binary transformations for security
- sandboxing and malware/untrusted code defense
- advanced attack campaign detection and forensics

One of the main objectives of this course is *adversarial thinking:* students should be able to quickly zoom in on the weakest link in any security technology, or system design. Students should be able to imagine how an attacker might break their system, and build in protection and mitigation measures to ward off such attacks.

There will be lectures in class but, in addition, the student is expected to study class notes, recommended references and supplemental videos to enhance their learning over the course of the semester.

Major Topics Covered in the Course:

- Principles and practice of building and administering secure systems.
- Authentication and access control
- Operating system security
- Program security
- Key management
- Information flow
- Assurance
- Vulnerability analysis and intrusion detection

Prerequisite

- C or higher in CSE 306 or CSE 376, or equivalent;
- limited to CSE graduate students; others, permission of instructor

Grades and Evaluation

The course provides a total of 500 points distributed across the below categories.
Your grade in the course will be based on the following work:

Assignments and Papers – *45% (225 points)* - A number of programming assignments will be given to help the student understand and apply the theoretical concepts in the class. A couple of short papers will also be given to help the student explore and research a couple of topic areas.
Class Attendance/Participation – 5% (25 points) – ***missing more than 20% of the classes will result in a grade of F***
Midterm Exam 1 – *15% (75 points)* - A midterm exam based on reading and concepts presented in the lecture.
Midterm Exam 2 – *15% (75 points)* - A midterm exam based on reading and concepts presented in the lecture.
Final Exam – 20*% (100 points)* - A cumulative final exam will provide questions that will cover the key concepts taught through the entire semester.

Final Grade Calculation

The final grade is based on the accumulated points from all quizzes, exams, and assignments (with the entire class comprised of 500 points). Letter grades are given on the following scale:

Letter	Minimum Percentage	Minimum 'points'
A	93	465
A-	90	450
B+	87	435
B	83	415
B-	80	400
C+	77	385
C	73	365
C-	70	350
D+	67	335
D	60	300
F	<60	<300

Attendance

The range of topics covered in this course is extensive, and due to the limited lecture time, these topics are covered in an intensive manner. Therefore, attendance at both lectures and lab are mandatory in order to keep up and perform well.

- Attendance will be taken in the beginning of each lecture and lab session.
- If a student has over 20% unexcused absences, the final course grade will be an F.

Re-grading

For re-grading of an assignment or exam, please email me to arrange a time to discuss (or state your reason for the regrade request.. All such requests that are later than one week from the date the graded work is returned will not be entertained.

Programming Assignments

Extensions

Programming assignments must be turned in on the day they are due. Students are urged to plan ahead to avoid problems such as congestion or failure of computer facilities at the last minute. If your assignment is incomplete or not working by the due date, turn in whatever you have. If some sort of emergency prevents you from submitting your assignment on time, supplying me with suitable documentation and notification ***prior*** to the assignment deadline will be considered. A penalty may be applied.

Course Schedule

Following is a tentative schedule for the class topics:

Week/Day	Lecture Topics	Readings	Tests/Vids
W1: 8/31	Course Overview		
9/2	Memory Corruption / Vulnerabilities I / Stack Smashing Attacks/Defenses		
W2: 9/7	Stack Smashing Attack techniques / Code Injection and Reuse		
9/9	Homework I Discussion		
W3: 9/14	Memory Corruption / Vulnerabilities II: Heap Overflows, Format-string Attacks, Integer Overflows		
9/16	Categorization of memory error defenses, Randomization based defenses, memory errors: Definition, Detection, and Prevention		
W4: 9/21	Chuseok – No classes		
9/23	More Software Vulnerabilities: Injection Attacks, Taint-tracking		
W5: 9/28	Race Conditions, CVE, CWE, and Principles of Secure System Design		
9/30	Malware: Types and Goals / Stealth, Obfuscation, Challenges of Malware Defense		
W6: 10/5	Defenses for Untrusted Code and Malware: Reference Monitors, System call interception and sandboxing		
10/7	Defenses for Untrusted Code and Malware: Inline Reference Monitors, Software Fault Isolation, Control Flow Integrity, Native Client		
W7: 10/12	Midterm I Review		
10/14	Midterm I		Midterm I
W8: 10/19	Homework II Discussion		
10/21	Binary Analysis and Instrumentation : Disassembly and Binary Analysis		
W9: 10/26	Binary Analysis and Instrumentation: Static Binary Instrumentation, Dynamic Binary Translation		
10/28	Cryptography Basics: Symmetric Crypto Overview, Ciphers and Algorithms, Asymmetric (Public Key) Crypto, Public vs Secret Key Encryption, Cryptographic Random Numbers, Digital Signatures and Message Digests, Digital Certificates		
W10: 11/2	Identification and Authentication I		
11/4	Identification and Authentication II		
W11: 11/9	OS Security and Access Control: File Permissions and ACLs, OS Capabilities, Mandatory Access Control, Domain and Type enforcement, Linux Capabilities, Policies for Untrusted. Code, Policy Management.		
11/11	Virtual Machines		
W12: 11/16	Midterm II Review / Homework III Discussion		
11/18	Midterm II		Midterm II
W13: 11/23	Web Security: Web Overview: HTTP, Cookies, Javascript and DOM, Authentication, Same Origin Policy		
11/25	Web Security: CSRF and Clickjacking, XSS and related attacks, Network based Attacks, Click-side attacks and summary		
W14: 11/30	Vulnerability Analysis: Fuzzing and Symbolic Execution		
12/2	Side Channel Attacks / Intrusion Detection		
W15: 12/7	Review for Final		
12/9	Adjustment Dqy : Monday classes		

Academic Dishonesty

You may *discuss* the practice problems with anyone you like, however each students' *assignment (including coding)* which they submit must be **their own work, and only their own work. Any evidence that source code or solutions have been copied, shared, or transmitted *in any way* (this includes using source code downloaded from the Internet or written by others in previous semesters!) will be regarded as evidence of academic dishonesty.**

Guidelines for Assignments

Working together to find a good approach for solving a programming problem is cooperation; listening while someone dictates a solution is cheating. You must limit collaboration to a *high-level discussion of solution strategies*, and stop short of actually writing down a group answer. Anything that you hand in, whether it is a written problem or a computer program, must be written in your own words. If you base your solution on any other written solution, ***you are cheating***

Guidelines for Taking Exams

When taking an exam, you must work completely independently of everyone else. Any collaboration here, of course, is cheating. All examinations will be closed-notes and closed-book. No electronic devices of any kind will be permitted to be used during exams. All cell phones must be silenced or turned off during exams. You will be allowed one sheet of notes, both sides (8.5 x 11 or A4).

General Guidelines

Be advised that any evidence of academic dishonesty will be treated with utmost seriousness. *We do not distinguish between cheaters who copy others' work and cheaters who allow their work to be copied.*

If you cheat, you will be given an F on the assignment. Any incidence of cheating will be reported to Academic Affairs. If you have any questions about what constitutes cheating, please ask.

Students with Disabilities

If you have a physical, psychological, medical or learning disability that may impact your course work, please let the instructor know. Reasonable accommodation will be provided if necessary and appropriate. All information and documentation are confidential.

Critical Incident Management

The University expects students to respect the rights, privileges, and property of other people. Faculty are required to report to the Office of Judicial Affairs any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, or inhibits students' ability to learn.