CSE331 Computer Security Fundamentals

Syllabus

Term: Spring 2024
Instructor: Tony Mione
Course Meeting Times: Tue & Thurs, 10:30-11:50 AM
Office: B425
Phone: +82 032-626-1226
Email: antonino.mione@sunykorea.ac.kr
Office Hours:
Mon: 10:30AM-12 Noon
Tue: 1:00-2:00 PM
Wed : 10:30AM-12 Noon, 1:00-2:00PM
Thur: 1:00-2:00PM
(or by appointment) [B425]
Course Homepage:
www3.cs.stonybrook.edu/~amione/CSE331_Course/index.html

Required Text:

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

Recommended Reference:

- 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

Introduces the basic concepts and terminology of computer security. Covers basic security topics such as cryptography, operating systems security, network security, and language-based security.

Major Topics Covered in the Course

- Cryptography including symmetric cryptography, asymmetric cryptography, certificates and public key infrastructure, cryptographic hashes, and basic math background
- Cryptographic protocols (ssl, tls, ssh, Kerberos, etc), attacks, and defenses
- Operating System Security including memory protection, access control, authentication, authorization, and file system security
- Network Security including firewalls, intrusion detection/prevention, security protocols, attacks on protocols, and defenses
- Software security. Secure software engineering, defensive programming, buffer overruns and other implementation flaws.
- Web security including injection attacks, cross site scripting attacks, sql and code injection attacks, as well as defending against attacks.
- Malware including viruses, trojan horses, and botnets
- If time permits:
    - Information hiding (Steganography)
    - Secret Splitting
    - Forensics

Course Objectives/Outcomes

After completing this course, students will:

- be conversant with the basic terminology and concepts of computer security
- understand basic security threats to systems and networks
- be familiar with basic strategies used to protect systems and networks
- be able to analyze, design, and build secure systems of basic complexity

Prerequisite

- C or higher: CSE 220 and CSE major
- Advisory pre/co-requisite: CSE 320

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– *45% (225 points)* - Assignments [about 6] will be given that will involve using concepts learned in class related to System Security, Cryptography, Malware, Attacks, and mitigation(s). In addition to the assignments, a short paper will be assigned mid semester to be completed by the end of the semester.
Class Attendance/Participation – 5% *(25 points)*
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 all lectures is 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 meet with the person (instructor or teaching assistant) responsible for the grading. All such requests that are later than one week from the date the graded work is returned to the class will not be entertained. To promote consistency of grading, questions and concerns about grading should be addressed *first to the TA* and then, if that does not resolve the issue, to the instructor. You are welcome to contact the TA by email or come to his/her office hour. If you would like to speak with the TA in person, and have a schedule conflict with his/her office hour, you are welcome to make an appointment to meet the TA at another time.

Assignments

Extensions

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 is not working by the due date, turn in whatever you have. Note due to limited resources for grading, if the assignment involves programming and the program does not compile or run for testing, it may not be graded. 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 I will be consider a short extension but may take a small late penalty.

Course Schedule

Following is a tentative schedule for the class topics:

Week/Day	Lecture Topics	Readings	Tests/Vids
W1: 2/27	Course Overview		
2/29	Basic Security: Threat Models, Attack surface, security engineering	Stamp: 8.4-8.7	Recommended Videos
W2: 3/5	Network Protocols: Lower Layers		
3/7	BGP, Routing, Attacks on Routing		Recommended Videos
W3: 3/12	DNS, DNS Cache Poisoning / DOS Attacks		Recommended Videos
3/14	Cryptography : Early Crypto, Crypto Concepts	Stamp: 2	
W4: 3/19	Cryptography : Symmetric Crypto, Modes of Operation, etc	Stamp: 3	
3/21	Cryptography : Asymmetric Crypto – RSA, DH, ECC, Integrity, HMACs ,Authentication, Digital Signatures	Stamp: 4, 5.1-5.8	
W5: 3/26	Review for Midterm I		
3/28	Midterm I		Midterm I
W6: 4/2	Cryptography : Information Hiding, Steganography	Stamp: 5.9	
4/4	Case Studies - Cryptography		
W7: 4/9	Cryptography : Cryptanalysis	Stamp: 6	
4/11	Access Control : Authentication	Stamp: 7	
W8: 4/16	Access Control : Authorization	Stamp: 8.1-8.8	
4/18	Firewalls, Intrusion Detection/Prevention	Stamp: 8.9-8.10	
W9: 4/23	Protocols	Stamp: 9	
4/25	Security Protocols : SSL, SSH, IPSec/IKE	Stamp: 10.1-10.4	
W10: 4/30	Review for Midterm II		
5/2	Midterm II		Midterm II
W11: 5/7	Security Protocols : Kerberos, WEP, GSM, others	Stamp: 10.5-10.8	
5/9	Case Studies – Security Protocols / Attacks / Mitigations		
W12: 5/14	[Correction day: Weds classes]		
5/16	Software Flaws [S1] - Malware [S2]	Stamp: 11.1-11.2	
W13: 5/21	Insecurity in Software - Reverse Engineering [S3]	Stamp: 11.3-11.5	
5/23	Secure Software Development [S4]	Stamp: 12.1-12.3	
W14: 5/28	Case Studies – Malware / Botnets	Stamp: 12.4	
5/30	Operating System Security [S5]	Stamp: 13	
W15: 6/4	Review: Final		
6/6	[Memorial Day: No classes in session]		

Network Videos

TCP/IP Intro: https://www.youtube.com/watch?v=y9PG-_ZNbWg
IP Addressing: https://www.youtube.com/watch?v=v8aYhOxZuNg
IP Addressing in depth: https://www.youtube.com/watch?v=Tnjdk08z3HM
TCP/IP Model: https://www.youtube.com/watch?v=HFRU01uS9nA
TCP and UDP: https://www.youtube.com/watch?v=FfvUxw8DHb0
TCP Connection Establishment:
https://www.youtube.com/watch?v=fQC4v07gs5k
TCP Error handling and flow control:
https://www.youtube.com/watch?v=NaEHwrRHfqk

Core Protocol Videos

Basic Intro to BGP
https://www.youtube.com/watch?v=_aLmzq-23pE

How BGP Works

https://www.youtube.com/watch?v=AjkU7Hw2TY4&t=821s

DNS, ARP, other protocols / DOS and DDos Attacks

DNS
Query Resolution:
https://www.youtube.com/watch?v=mpQZVYPuDGU

https://www.youtube.com/watch?v=JkEYOt08-rU

What is DDos?
https://www.youtube.com/watch?v=ilhGh9CEIwM

5 Largest DDos Attacks:
https://www.youtube.com/watch?v=HBBEE2FcdOw

Academic Dishonesty

You may *discuss* the assignments at a *high level* 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). [This policy may vary slightly for online exams given due to COVID-19

conditions].

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.