CSE331 Fundamentals of Computer Security

Syllabus

Term: Fall 2026
Instructor: Tony Mione
Course Meeting Times: Tue & Thurs, 10:30-11:50 AM - *B103*
Office: C520
Phone: +82 032-626-1226
Email: antonino.mione@sunykorea.ac.kr
Office Hours:
Mon: 1:00 – 3:30 PM
Tue: 1:00 – 3:00 PM
Wed: 10:30 – 12:00
(or by appointment) [C520]

Course Homepage:
https://www3.cs.stonybrook.edu/~amione/CSE331_Course/index.html

Brightspace: *https://mycourses.stonybrook.edu/d2l/home/2748872*

Required Text:

- "Information Security: Principles and Practice, 3rd Edition", Stamp, Mark, Wiley, 2021, ISBN: 978-1-119-50588-4

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– *40% (200 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 – 25*% (125 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. You are welcome to contact the graduate TA by email or come to his/her office hour. If the course has no graduate TA, you can address regrade requests directly to me.

Homework Submission Policy

- Assignments will be turned in on **BrightSpace**
- Assignments must be turned in by the due date and time.
- Any part of an assignment that's late means the entire assignment is late.
- If your assignment is incomplete or not entirely working by the due date, turn in what you have to get some partial credit.
- If you have an emergency situation, email me before the due date and I may be able to work something out
    - Strictly on a case-by-case basis.
    - A penalty may be applied to the score.

- ➔ Important: If I grant a short extension, the assignment must be turned in by the agreed on time/date. ***Under NO circumstances will an assignment be graded if grades and feedback have been posted to other students.***
- ***← Please go back and re-read the above bullet point!***

Course Schedule

Following is a tentative schedule for the class topics:

Week/Day	Lecture Topics	Readings	Tests/Vids
W1: 9/1	Course Overview		
9/3	Basic Security: Threat Models, Attack surface, security engineering	Stamp: 7.2-7.7	Recommended Videos
W2: 9/8	Case Studies: Recent Attack Survey		
9/10	Network Protocols: Lower Layers	Stamp: 8.1-8.3	
W3: 9/15	BGP, Routing, Attacks on Routing		Recommended Videos
9/17	DNS, DNS Cache Poisoning / DOS Attacks		Recommended Videos
W4: 9/22	Cryptography : Early Crypto, Crypto Concepts	Stamp: 2	
9/24	Chuseok – No class		
W5: 9/29	Cryptography : Symmetric Crypto, Modes of Operation, etc	Stamp: 3	
10/1	Cryptography : Asymmetric Crypto – RSA, DH, ECC, Integrity, HMACs ,Authentication, Digital Signatures	Stamp: 4, 5.1-5.8	
W6: 10/6 [Th]	Cryptography : Information Hiding, Steganography	Stamp: 5.9	
10/8	Case Studies – Cryptography / Special Topics: Secret Splitting, Blockchain		
W7: 10/13	Midterm I		Midterm I
10/15	Access Control : Authentication	Stamp: 6	
W8: 10/20	Access Control : Authorization	Stamp: 7	
10/22	Firewalls, Intrusion Detection/Prevention	Stamp: 8.4-8.6	
W9: 10/27	Protocols	Stamp: 9	
10/29	Security Protocols : SSL, SSH, IPSec/IKE	Stamp: 10.1-10.4	
W10: 11/3	Security Protocols : Kerberos, WEP, GSM, others	Stamp: 10.5-10.8	
11/5	Case Studies – Security Protocols / Attacks / Mitigations		
W11: 11/10	Midterm II		Midterm II
11/12	Software Flaws [S1], Attack Methodology, Web and Web [In]Security [S1a]	Stamp: 11.1-11.2	
W12: 11/17	Malware [S2]	Stamp: 11.3-11.4	
11/19	Insecurity in Software - Reverse Engineering [S3]	Stamp: 12.1-12.2	
W13: 11/24	Secure Software Development [S4]	Stamp: 12.3-12.4	
11/26	Case Studies – Malware / Botnets		
W14: 12/1	Special Topics		
12/3	Special Topics		
W15: 12/8	Review for Final		
12/10	Reading day – No class		
12/9	Final Exam [9:00-11:30]		

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.**

For additional information, see the **Academic Integrity Statement** section below.

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.

Wellness & Support Statement

SUNY Korea values student well-being, including mental health, and recognizes that a variety of factors can impact emotional wellness and academic success including stress, anxiety, depression, substance use, sexual violence, family or relationship concerns, and political conflict. If you experience challenges or wellness concerns that affect your ability to be successful in class, you are encouraged to reach out for help from the Counseling Center via counseling@sunykorea.ac.kr when you need it.

In the event of a short-term absence from class, students are encouraged to communicate immediately and work directly with instructors. However, if a student is struggling with an extended absence due a hospitalization, family illness or death, they are encouraged to reach out to the Student Support Team.

Students with Disabilities

If you have a physical, psychological, medical, or learning disability that may impact your course work, please contact the Student Accessibility Support Center, Academic Building A208, 032-626-1198, or at sas@sunykorea.ac.kr. They will determine with you what accommodations are necessary and appropriate. All information and documentation is confidential.
Students who require assistance during emergency evacuation are encouraged to discuss their needs with their professors and the Student Accessibility Support Center.

Academic Integrity Statement

Each student must pursue his or her academic goals honestly and be personally accountable for all submitted work. Representing another person's work as your own is always wrong. Faculty is required to report any suspected instances of academic dishonesty to Academic Affairs (academicaffairs@sunykorea.ac.kr). For more comprehensive information on academic integrity, including categories of academic dishonesty please refer to the academic judiciary website at http://www.stonybrook.edu/commcms/academic_integrity/index.html

Critical Incident Management

Stony Brook University expects students to respect the rights, privileges, and property of other people. Faculty are required to report to Student Affairs (student@sunykorea.ac.kr) any disruptive behavior that interrupts their ability to teach, compromises the safety of the learning environment, or inhibits students' ability to learn.

Understand When You May Drop This Course

If you need to drop or withdraw from the course, it is your responsibility to be aware of the tuition liability deadlines listed on the registrar's Academic Calendar. Before making the decision to drop/withdraw, please contact me or your department advisor.

For the detailed information about course drop, please refer to the University's policies:

- Undergraduate Course Load and Course Withdrawal Policy
- Graduate Course Changes Policy

Incomplete Policy

Under emergency/special circumstances, students may petition for an incomplete grade.
Circumstances must be documented and significant enough to merit an incomplete. If you need to request an incomplete for this course, contact me for approval as far in advance as possible.
You should also read the University's policies that apply to you:

Undergraduate Catalog - Grading and the Grading System
Graduate Catalog - Grading Policies

Course Materials and Copyright Statement

Course material accessed from Brightspace is for the exclusive use of students who are currently enrolled in the course. Content from these systems cannot be reused or distributed without written permission of the instructor and/or the copyright holder. Duplication of materials protected by copyright, without permission of the copyright holder is a violation of the Federal copyright law, as well as a violation of Stony Brook's Academic Integrity.