CSE508: Network Security

Syllabus

Term: Fall 2025
Instructor: Tony Mione
Course Meeting Times: Mon & Wed, 3:30-4:50 PM
Office: B425
Phone: +82 032-626-1226
Email: antonino.mione@sunykorea.ac.kr
Office Hours:
Mon: 10:30-Noon, 1:00-2:00PM
Tue: 10:30-Noon
Wed: 11:00-Noon, 2:00-3:00PM
(or by appointment) [B425]

Course Homepage: ***https://www3.cs.stonybrook.edu/~amione/CSE508_Course/index.html***

Brigthspace: ***https://mycourses.stonybrook.edu/d2l/home/2208452***

Required Text:
None. Readings assigned will be mainly professional journals and scholarly papers.

Recommended Reference:
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]
William R. Cheswick, Steven M. Bellovin, and Aviel D Rubin. Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition, Addison-Wesley Professional, 2003, ISBN 020163466X.
Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography, CRC Press, ISBN 0849385237.

Course Overview

The course will cover a wide range of topics in network security and online privacy, trying to strike a balance between core concepts and recent advancements. The focus of the course will be on technologies, protocols, attacks, and defenses most closely related to the network rather than the end systems.

The main goal of the course is to provide an understanding of various network security concepts through, at times, a more adversarial way of thinking. By focusing on vulnerabilities and exploitation techniques, the course will cover a broad range of topics, including core network protocols, eavesdropping, scanning, DoS attacks,

firewalls, VPNs, proxies, intrusion detection, forensics, honeypots, encrypted communication, authentication, services and applications, botnets, targeted attacks, exfiltration, privacy, anonymity. After discussing some basic security concepts, we will work a bit bottom-up starting with lower level protocols followed by the primary protocols used to make the internet 'useful' and leading up to security protocols and security measures applied to this varied collection of code.

Topics are covered from a highly practical perspective, following a mixed format of lectures, research paper discussions, and case studies. Other requirements include three or four programming assignments, one or two short research papers and two exams.

Major Topics Covered in the Course

- Basic security concepts
- Ethics
- The threat landscape
- Lower layer protocols
- BGP
- DNS
- Denial of Service Attacks
- Symmetric and Public Key Cryptography
- Authentication
- TLS
- Firewalls and Tunnels
- Reconnaissance
- Malware
- Intrusion Detection
- Email
- Social Engineering
- Web Security
- Privacy
- Anonymity

Course Objectives/Outcomes

After completing this course, students will have:

- an understanding of the principles and practice of building and administering secure networks.
- an understanding of authentication and access control, key management, and network security.
- an ability to securely managing computer networks and deploying defenses against various threats.

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– *30% (150 points)* - Assignments [about 3 or 4] will be given that will involve using concepts learned in class related to Network Security, Cryptography, Malware, Attacks, and mitigation(s).
Research Papers – 30% (150 points) – Two papers, 1 short paper and one medium length term paper.
Class Attendance/Participation – 5% *(25 points)*
Midterm Exam – 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 assignments, papers, and exams (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.

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 some sort of emergency prevents you from submitting your assignment on time, supply me with suitable documentation and notification prior to the assignment deadline and I will be consider a short extension but there may be a small late penalty.

Course Schedule

Following is a tentative schedule for the class topics:

Week/Day	Lecture Topics	Readings	Tests/Vids/Assignments
W1: 8/25	Course Overview		
8.27	Basic security concepts		
W2: 9/1	Ethics		
9/3	The threat landscape		
W3: 9/8	Lower layer protocols I		
9/10	Lower layer protocols II		
W4: 9/15	BGP		
9/17	DNS		
W5: 9/22	Denial of Service Attacks		
9/24	Symmetric Cryptography		
W6: 9/29	Public Key Cryptography		
10/1	Authentication I		
W7: 10/6,10/8	Chuseok : No class		
W8: 10/13	Authentication II		
10/15	TLS		
W9: 10/20	Review for Midterm		
10/22	Midterm		Midterm
W10: 10/27	Firewalls and Tunnels		
10/29	Reconnaissance		
W11: 11/3	Recon lab		
11/5	Malware		
W12: 11/10	Intrusion Detection		
11/12	Email		
W13: 11/17	Social Engineering		
11/19	**Web Security**		
W14: 11/24	**Web Security lab**		
11/26	Privacy		
W15: 12/1	Anonymity		
12/3	Review for Final Exam		
12/8	Final Exam [3:15-5:45PM]		

Network Videos

Networking Basics Tutorial series
https://www.youtube.com/watch?v=9SIjoeE93lo [Part I]

Core Protocol Videos

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

DNS, ARP, other protocols / DOS and DDos Attacks

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

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 (except as indicated below) 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 letter 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.

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

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.

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.

.