Fall 2025	
Delivery: 100% Web-Based, Synchronous	**Offered on:** Canvas
Dates course: August 18 – December 11, 2025	

Instructor Information

Dr. Wenke Lee	Office: Coda E0964B
Weekly Office Hours via Zoom per announcements on Ed	Email: wenke.lee@gmail.com

General Course Information

Learning Objectives

This is a graduate-level network security course. It teaches the concepts, principles, techniques to secure networks. The main topics include:

1. Large-scale attacks and impacts**:** DDoS attacks, malware-based underground economy

2. Penetration testing and security measures: basic techniques and tools, social engineering and human factors

3. Security of Internet protocols: vulnerabilities of TCP/IP, BGP security, and DNS cache poisoning and DNSSEC

4. Advanced web security: browser security models, session management, and goals and pitfalls of HTTPS

5. Advanced malware analysis: malware obfuscation, mobile malware

6. Advanced network monitoring: botnet detection systems

7. Internet-scale threat analysis: mapping the Internet, domain/network reputation

8. Bitcoins and cryptocurrencies: basic concepts of blockchain and bitcoins, emerging technologies

9. Big data and security: applying machine learning to security analytics, and security of data analysis - data poisoning and model evasion

10.Cloud security: virtual-machine security, goals and pitfalls of property-preserving encryption, oblivious RAM

11.Attack-tolerant systems: secret-sharing, Byzantine fault-tolerant systems, diversification and moving-target defense

Pre-Requisites

You should have taken an introductory course on, or otherwise be familiar with, the basic concepts of information security (there is very little overlap between this course and CS6035).

The following prerequisite knowledge is recommended:

Basic Web Development Knowledge

- JavaScript: manipulating DOM elements (e.g., creating and appending)
- HTML: understanding form submission, frame navigation, and common DOM elements
- CSS: positioning and styling DOM elements
- Chrome or Firefox DevTools: debugging DOM/JavaScript, inspecting network traffic

Basic Knowledge of XSS and Related Concepts

- Reflected XSS
- DOM-based XSS
- Stored XSS
- Same-Origin Policy
- Using postMessage for communication between frames of different origins

Programming and Security Tools

- Basic Python scripting
- Some familiarity with disassembly (support will be provided during projects)
- Basic understanding of network protocols
- Awareness of common network attack traffic patterns:
  - DDoS
  - Password brute-forcing
  - Botnet command and control (C&C)
  - Web-based attacks

Security Tool Usage

- Prior experience with Wireshark (or willingness to learn during projects)
- Prior experience with Snort (or willingness to learn during projects)

Even if you don't have all of this prerequisite knowledge, you can still succeed in the course with dedication and effort. However, if you are not from a strong programming background, **it is strongly recommended that you take CS6035 first.**

Course Materials

Reading Materials

There is no required textbook. Papers and other reading materials for each topic will be posted. **It is very important** that you read these materials because the videos and slides only cover high-level concepts. If you really want to learn the material, you need to study the papers. Quiz and exam questions are based on both the slides and the papers, and the projects are also grounded in the papers. This is how we typically run a graduate-level course: read papers and work on projects.

Classroom Management Tools

Everything else can be accessed through Canvas, including all exams, quizzes, lectures, and readings. Our discussion board will be hosted on Ed and will also be accessible via Canvas.

Course Requirements, Assignments & Grading

Assignment Distribution and Grading Scale

Assignments	Weight
Quizzes	**10%**
Projects	**80%**
Exam	**10%**
Extra Credit(extra credit exam/project)	**<=8%**

Grading Scale

Your final grade will be assigned as a letter grade according to the following scale:

A	90-107%
B	80-90% (not including 90)
C	70-80% (not including 80)
D	60-70% (not including 70)
F	0-60% (not including 60)

Description of Graded Components

- **Ten quizzes (10%)**: Each quiz will be released when the corresponding lessons are expected to be completed, according to the schedule. Quizzes are released on Fridays and due ten days later (typically on a Monday or the day after a holiday or break). Questions are based on slide materials and readings.
- **Five required individual projects (80%)**:
    - **Project #1 (10%)**: Vulnerability scanning and penetration testing – exploit a vulnerability in a network service
    - **Project #2 (15%)**: Advanced malware analysis – iterative program analysis and malware debugging
    - **Project #3 (15%)**: Advanced web security – attacks and defenses
    - **Project #4 (20%)**: Network monitoring – write NIDS rules to identify botnet traffic
    - **Project #5 (20%)**: Machine learning for security – build a normal traffic profile and design attacks to evade the model (if applicable)
    - **Extra credit project:** TBD-typically up to 3%. We may offer an extra credit

project later in the semester, typically worth up to 3%. Details and deadlines will be announced if offered. This is not guaranteed.

- **Exam (10%)**: True/False and multiple-answer questions. Closed-book. Administered at the end of the semester. Questions are based on slides and projects. A study guide will be released a couple of weeks before the exam. Closed-book exams will be proctored using Honorlock.
- **Extra credit exam (5%)**: True/False and multiple-choice questions. Closed-book. Administered mid-semester. Questions are based on material covered during the Professor's office hours. A study guide will be released a couple of weeks before the exam. Closed-book exams will be proctored using Honorlock.

Late Assignments

No late submissions (quizzes, exams, etc.) are allowed unless there are special circumstances as defined by Georgia Tech policies (e.g., medical or family emergencies, with instructor approval). There are no exceptions to this rule. Only projects may be submitted late, with a 20% grade deduction for each of the first two days after the deadline. After two days, late submissions will receive a zero. However, late submissions for the extra credit exam or final exam are not allowed under any circumstances.

Regrade Requests

You may submit one regrade request within one week of a project grade being released. You can use the "Regrade Request" tab on Ed or follow the project TA's instructions for submitting the request.

Note that your project grade may increase or decrease as a result of a regrade. If the TA identifies a grading error that resulted in a higher score than warranted, points may be deducted accordingly. You will receive an email notification once your regrade is complete. If you are still unsatisfied, you may post privately on Ed. Requests submitted after the one-week window will not be accepted. There are no exceptions to this policy.

Submission Errors

We understand that Canvas may occasionally experience submission errors, especially near deadlines. If this occurs, do not panic. Email the TA responsible for grading your assignment immediately. Include your completed project files and a screenshot of the Canvas error. However, missing files or documents cannot be submitted after initial grades have been returned. This is a graduate-level course, and students are responsible for ensuring that their submissions are complete and on time.

For project assignments that do not require submission through Canvas, you may see a "Missing" tag on Canvas after the deadline or even after the assignment has been graded. You can safely ignore this tag.

Grading and Feedback

After each project deadline, feedback on incorrect components will be posted on Canvas. Once a quiz is due, both the solution and your original responses will be released.

After the exam deadline, you will receive feedback only on the questions you answered incorrectly. Full exam solutions will not be released, as the exam is technically classified as an "Assignment" on Canvas. Feedback will be available under the exam assignment section once grades are posted.

We will not provide a working version of the solution code for any assignments. However, we are happy to continue guiding you in understanding the questions and helping you get closer to the solution after the deadline, if you're interested in learning more.

Technology Requirements

Computer Hardware and Software

Browser and Connection Speed

Use an up-to-date version of Google Chrome or Firefox. A broadband connection with at least 5 Mbps download and 1 Mbps upload speed is recommended for streaming lectures and participating in live sessions without interruptions.

Operating System

- Windows: Windows 10 or newer
- macOS: macOS 10.14 Mojave or newer. (*Note: Students using ARM-based Macs (e.g., M1/M2/M3 chips) have reported VM slowness for certain projects in the past. While we are working on providing workarounds for most of these cases, performance issues may still occur. We strongly recommend starting projects early to allow time for troubleshooting. For some assignments—such as Project 3—we may offer access to a limited number of cloud-based VMs. Requests must be submitted within the first week after the project is released. It is the student's responsibility to manage their setup and start early—issues due to VM slowness will not be accepted as excuses for late or incomplete submissions.*).
- Linux: A recent distribution capable of running Python3 and common libraries

Hardware Requirements

- At least 8 GB of RAM (16 GB or more recommended)
- At least 30 GB of free disk space (80 GB recommended if using VMs)
- A dual-core processor (quad-core or better recommended)
- A functioning webcam and microphone for exam proctoring

Virtual Machine Requirements

You will be provided with virtual machines (VMs) to complete many class assignments and projects. These VMs are the same environment used for grading. Setup instructions will be included in the project write-ups. Ensure your system can allocate sufficient memory and disk space for smooth operation.

Proctoring Information

The exam will be proctored. It is similar to the one you would take in the classroom. This means no open textbooks, notebooks, notes, or other similar resources are allowed unless explicitly permitted. These exams are delivered via a tool called Honorlock. Honorlock is an online proctoring service that allows you to take your exam from the comfort of your home. You **do not** need to create an account, download software, or schedule an appointment in advance. Honorlock is available 24/7, and all that is needed is a computer, a working webcam/microphone, your ID, and a stable internet connection. And yes, we typically require you to do a room scan with the camera.

To get started, you will need Google Chrome and download the Honorlock Chrome Extension.

When you are ready to complete your assessment, log onto Canvas, go to your course, and click on your exam. Clicking "Launch Proctoring" will begin the Honorlock authentication process, where you will take a picture of yourself, show your ID, and complete a scan of your room. Honorlock will be recording your exam session through your webcam, microphone, and screen. Honorlock also has an integrity algorithm that can detect search engine use, so please do not attempt to search for answers, even if it is on a secondary device.

Honor lock support is available 24/7/365. If you encounter any issues, you may contact them through live chat on the support page or within the exam itself. Some guides you should review are Honorlock MSRs, Student FAQ, Honorlock Knowledge Base, and How to Use Honorlock. Good luck!

Course Policies, Expectations & Guidelines

Ed Platform

The Ed platform will be used as the main communication medium for this class. You are encouraged to post discussions about any issues you're experiencing with projects or other course material. Please do not post solutions on Ed. If you do, we may revoke your access to the Ed page. Do not post new messages addressed to individual instructors (e.g., Wenke Lee). We have multiple TAs answering Ed posts on a rotating basis, so you will not receive a direct response from Wenke. Only if necessary, the TA will escalate the issue to the Head TA, who may then contact the Instructor. The Instructor will have the final say on the matter.

Communication Policy

To manage a class of this size efficiently, we assign specific responsibilities to the Instructor, Head TA, and TAs. All communication **should go through Ed** unless specifically directed otherwise. If you cannot access Ed or have an urgent issue that cannot be resolved through the platform, you may contact the Head TA or Instructor by email as a backup option.

- Head TA email: mchen461@gatech.edu
- Instructor email: wenke@cc.gatech.edu / wenke.lee@gmail.com
- If you are seeking a project extension, post on Ed **using the "extension" tag**.
- If you have a regrade request, follow the instructions provided by the project TAs, or post on Ed using the "regrade request" tag.
- To request a deadline extension (projects, quizzes, exams, etc.) due to a Georgia Tech-approved reason (e.g., medical emergency), post on Ed with the “extension” tag and a TA will follow up with next steps. If you are unable to access Ed, email the Head TA and CC the Instructor with appropriate documentation.
- If exam or quiz grades have been released but are not visible to you, post privately on Ed. If Ed is unavailable, contact the Head TA.
- For office hour-related questions, post on Ed using the “office hours” tag and address the relevant TA.
- For questions about unclear or incorrect wording in projects, quizzes, exams, etc., post publicly on Ed.
- For help or advice on a project, post publicly on Ed.

If a TA cannot resolve your issue on Ed after multiple exchanges, the TA will escalate the matter to the Head TA. If the Head TA cannot resolve it, they will contact the Instructor, who will make the final decision. Do not directly contact the Head TA or Instructor unless explicitly instructed to do so or if Ed is unavailable.
If a TA has not responded to your Ed post within 2 days, post again for visibility. If you still do not receive a response and it is urgent, you may email the Head TA and let the head TA know about the situation.
If you have taken the class previously or have .ova files from prior courses, do not use those files to complete the projects. Doing so will result in a zero.
Do not upload your projects to public GitHub repositories. If a future student copies your code, they will be in violation of the honor code—and you will also be implicated.
Please do not post about grade or solution release timelines. These will be shared only after all student submissions are received, including those with approved extensions.
Please do not post about your regrade request status after submission. You will be notified once regrading is complete. Please be patient.

Online Student Conduct and (N)etiquette

Communicating appropriately in the online classroom can be challenging. In order to minimize this challenge, it is important to remember several points of **“internet etiquette”**
that will smooth communication for both students and instructors:

1. *Read first, Write later*. Read the ENTIRE set of posts/comments on a discussion board before posting your reply, in order to prevent repeating commentary or asking questions that have already been answered.
2. *Avoid language that may come across as strong or offensive.* Language can be easily misinterpreted in written electronic communication. Review email and discussion board posts BEFORE submitting. Humor and sarcasm may be easily misinterpreted by your reader(s). Try to be as matter of fact and professional as possible.
3. *Follow the language rules of the Internet.* Do not write using all capital letters, because it will appear shouting. Also, the use of emoticons can be helpful when used to convey nonverbal feelings. ☺
4. *Consider the privacy of others*. Ask permission prior to giving out a classmate's email address or other information.
5. *Keep attachments small*. If it is necessary to send pictures, change the size to an acceptable 250kb or less (one free, web-based tool to try is picresize.com).
6. *No inappropriate material.* Do not forward virus warnings, chain letters, jokes, etc. to classmates or instructors. The sharing of pornographic material is forbidden.

NOTE*: The instructor reserves the right to remove posts that are not collegial in nature and/or do not meet the Online Student Conduct and Etiquette guidelines listed above.*

University Use of Electronic Email

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information in their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Plagiarism & Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools, and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, please visit
http://www.catalog.gatech.edu/policies/honor-code/ or
http://www.catalog.gatech.edu/rules/18/.

Any student suspected of cheating or plagiarizing on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

You are prohibited from posting course materials including quizzes, exams, and projects on the Internet (including public GitHub). If any student copies your work that you had posted on-line, you will be considered as having committed plagiarism as well.

Note: Note: You may use large language models (LLMs) such as ChatGPT, Grok, or Gemini as learning tools—e.g., to better understand JavaScript syntax or security concepts. However, submitting any content (code or text) directly generated by an LLM is strictly prohibited and will be treated as plagiarism. We actively check for such violations using detection tools and take Academic Honor Code violations seriously.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)894-2563 or **http://disabilityservices.gatech.edu/**, as soon as possible, to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Student-Faculty Expectations Agreement

At Georgia Tech we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. See **http://www.catalog.gatech.edu/rules/22/** for an articulation of some basic expectations that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Subject to Change Statement

The syllabus and course schedule may be subject to change. It is the responsibility of students to check Ed, email messages, and course announcements to stay current in their online courses.

Resources for Students

In your time at Georgia Tech, you may find yourself in need of support. Below you will find some resources to support you both as a student and as a person.

Academic support

- Center for Academic Success http://success.gatech.edu
    - 1-to-1 tutoring http://success.gatech.edu/1-1-tutoring
    - Peer-Led Undergraduate Study (PLUS) http://success.gatech.edu/tutoring/plus
- OMED: Educational Services (http://omed.gatech.edu/programs/academic-support)
    - Group study sessions and tutoring programs
- Communication Center (http://www.communicationcenter.gatech.edu)
    - Individualized help with writing and multimedia projects
- Advising and Transition (https://advising.gatech.edu)
    - Study Strategies Seminar course https://advising.gatech.edu/gt2801-study-strategies-seminar
    - Academic coaching https://advising.gatech.edu/academic-coaching
    - Advising in your major http://advising.gatech.edu/

Personal Support

Georgia Tech Resources

- The Office of the Dean of Students: https://studentlife.gatech.edu/content/get-help-now; **404-894-6367**; Smithgall Student Services Building 2nd floor
    - You also may request assistance at https://gatech-advocate.symplicity.com/care_report/index.php/pid383662?
- Center for Assessment, Referral and Education (CARE) **404-894-3498**; **https://care.gatech.edu/**
    - Smithgall Student Services Building 1st floor
    - Students seeking assistance from the Counseling Center or Stamps Psychiatry need to visit CARE first for a primary assessment and referral to on and off campus mental health and well-being resources.
    - *Students in crisis may walk in during business hours (8am-4pm, Monday through Friday) or contact the counselor on call after hours at **404-894-2575 or 404-894-3498**. Other crisis resources:* https://counseling.gatech.edu/content/students-crisis
- Students' Temporary Assistance and Resources (STAR): https://studentlife.gatech.edu/content/star-services
    - Can assist with interview clothing, food, and housing needs.
- Stamps Health Services: https://health.gatech.edu; **404-894-1420**
    - Primary care, pharmacy, women's health, psychiatry, immunization and allergy, health promotion, and nutrition
- OMED: Educational Services: http://www.omed.gatech.edu
- **Women's Resource Center: http://www.womenscenter.gatech.edu; 404-385-0230**
- **LGBTQIA Resource Center: http://lgbtqia.gatech.edu/; 404-385-2679**
- **Veteran's Resource Center: http://veterans.gatech.edu/; 404-385-2067**
- **Georgia Tech Police: 404-894-2500; http://www.police.gatech.edu**

National Resources

- The National Suicide Prevention Lifeline | 1-800-273-8255
  - Free and confidential support 24/7 to those in suicidal or emotional distress
- The Trevor Project
  - Crisis intervention and suicide prevention support to members of the LGBTQ+ community and their friends
  - Telephone | **1-866-488-7386** | 24 hours a day, 7 days a week
  - Online chat | 24 hours a day, 7 days a week
  - Text message | Text “START” to **687687** | 24hrs day, 7 days a week

Statement of Intent for Inclusivity

As a member of the Georgia Tech community, I am committed to creating a learning environment in which all of my students feel safe and included. Because we are individuals with varying needs, I am reliant on your feedback to achieve this goal. To that end, I invite you to enter into dialogue with me about the things I can stop, start, and continue doing to make my classroom an environment in which every student feels valued and can engage actively in our learning community.

Course Schedule

Week	Modules	Quiz	Project
1 8/18	DDoS Attacks; Cybercrimes		
2 8/25	Penetration Testing; Browser Security Model	Quiz #1 released **Sat 8/30**, due **Sun 9/7**	Project #1 released **Sat 8/30**, due **Sun 9/14**
3 9/1	Web Session Management	Quiz #2 released **Sat 9/6**, due **Sun 9/14**	
4 9/8	HTTPS; Security of Internet Protocols	Quiz #3 released **Sat 9/13**, due **Sun 9/21**	Project #2 released **Sat 9/13**, due **Sun 9/28**
5 9/15	DNS Security; Advanced Malware Analysis	Quiz #4 released **Sat 9/20**, due **Sun 9/28**	
6 9/22	Mobile Malware; Cloud Security: VM Monitoring	Quiz #5 released **Sat 9/27**, due **Sun 10/5**	Project #3 released **Sat 9/27**, due **Sun 10/19**
7 9/29	Property-preserving Encryption; Oblivious RAM	Quiz #6 released **Sat 10/4**, due **Sun 10/12**	
8 10/6	Botnet Detection	Quiz #7 released **Sat 10/11**, due **Sun 10/19**	
9 10/13	Internet-scale Threat Analysis: Scanning; Domain and Network Reputation	**Extra Credit Exam:** Sat 10/18 – Tue 10/21 No weekly quiz this week	Project #4 released on **Sat 10/18** and due on **Sun 11/02**
10 10/20	Machine Learning for Security	Quiz # 8 Released **Sat 10/25**, due **Sun 11/2**	
11 10/27	Data Poisoning and Model Evasion	Quiz #9 Released **Sat 11/1**, due **Sun 11/9**	
12 11/3	Basics of Blockchains and Bitcoins	Quiz #10 Released **Sat 11/8**, due **Sun 11/16**	Project #5 released on Sat **11/1** and due on **11/23**
13 11/10	Topics in Cryptocurrencies; Attack Tolerant Systems	No more weekly quiz	

14 11/17	**One- Hour Close-Everything Exam** **Available time window: 11/21-25**	No more weekly quiz	