Spring 2024	
Delivery: 100% Web-Based, Synchronous	**Offered on:** Canvas
Dates course: Jan 8 – May 2	

Instructor Information

Dr. Wenke Lee	Office: Coda E0964B
Weekly Office Hours via Blue Jeans per announcements	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 detections 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 be otherwise familiar with, the basic concepts of information security *(there is very little overlap between this course and CS6035).*
The following pre-requisite knowledge is recommended:

- Basic Web Development Knowledge
  - Basic Javascript to manipulate DOM elements including creating and appending.
  - Basic HTML knowledge to understand form submission, frame navigation, and usage of common DOM elements.
  - Basic CSS to understand what to use to position the DOM element and modify the style of DOM elements.
  - How to use DevTools of Chrome or Firefox to debug DOM and JavaScript as well as inspect the network traffic.
- Basic Knowledge of XSS
  - Reflected-XSS

    - DOM-XSS
    - Stored-XSS
- Same Origin Policy
    - How to use postMessage to communicate between frames with different origins
- Basic Python scripting.
- Some knowledge of disassembly recommended (but information is given in the relevant projects).
- Prior experience using Wireshark (can be learned within the relevant projects)
- Understanding of network protocols.
- Prior Understanding of typical attack network traffics.
    - DDoS
    - Password brute forcing
    - Botnet C&C
    - Web attacks
- Prior experience using Snort (can be learned within the relevant projects)

Even if you have most but not all of this pre-requisite knowledge, you can succeed in the class. However, if you have never programmed before, you may want to consider taking 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 the high-level concepts, and if you want to really learn the materials, you need to study the papers. The quiz and the exam questions are based on slides and papers, and the projects are based on the papers as well. This is how we typically run a graduate-level course - read papers and work on projects.

Georgia Institute of Technology

Course Syllabus: CS6262 Network Security

Classroom Management Tools
Everything else can be accessed here through Canvas. All exams, quizzes, lectures, and readings. Our discussion board will be hosted on Ed and also can be accessed via Canvas.

Course Requirements, Assignments & Grading

Assignment Distribution and Grading Scale

Assignments	Weight
Quizzes	**10%**
Projects	**80%**
Exam	**10%**
Extra Credit	**5%**

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

A 90-105%
B 80-90% (not including 90)
C 70-80% (not including 80)
D 60-70% (not including 70)
F 0-60% (not including 50)

Description of Graded Components

- **Ten quizzes for a total of 10%.** A quiz will be released when the lessons that it covers are expected to be completed by the students per the schedule. Each quiz is released on a Friday and due in ten days (on a Monday or the day after a holiday or recess). Quiz questions will be based on the slide materials and readings.
- **Five required individual projects for a total of 80%:**
  - Project #1: vulnerability scanning and penetration test - exploit a vulnerability of a network service (10%)
  - Project #2: advanced malware analysis - iterative program analysis and debugging of malware (15%)
  - Project #3: advanced web security - attacks and defenses (15%)
  - Project #4: network monitoring - write NIDS rules to identify botnet traffic (20%)
  - Project #5: machine learning for security - build normal traffic profile, design attacks to evade the model (20%)
- **10% exam:** T/F and multiple-choice, close-everything, at the end of semester. Exam questions are based on slide materials and projects.
- **5% extra credit:** You can make one suggestion for each project. It can be about how to improve the write-up or any part of the project for future release. If we agree with your suggestion, you will receive one extra point.

Late Assignments
No late submissions (quizzes, exams, etc.) are allowed unless special circumstances subject to Georgia Tech rules (e.g., medical/family emergencies, and instructor approvals). There are no exceptions to this rule. Projects can be turned in late for a 25% grade reduction for EACH of the first two days after the regular deadline, and a zero grade afterwards. However, **late submissions for extra credit projects are not allowed.**

Regrade Requests

Up to one week after each Project grade is released, you may submit one (and only one) regrade request. We will not accept regrade requests via email, Ed, or otherwise. We will only accept them through a Google Form submission. A link to each Project regrades form will be sent following each project's grade release on Canvas. You will only be able to submit this form once, so make sure you have worded out your request properly. Note that your grade for this project can go up or down if you request a regrade. If the TA grading it sees a grading mistake that costs you points, they will deduct them. Once your project has been regraded, you will receive an email notification. If, after your project has been regraded, you are still unsatisfied, please post privately on Ed. If you submit a regrade request after this one-week window, we will not answer or accept your regrade request. There are no exceptions to this rule.

Submissions Errors
We are aware that Canvas' submissions system can have errors sometimes and can prevent you from submitting projects at the last minute (before the deadline). If this happens, please do not panic. Simply email the TA responsible for grading your submission about the error and attach your solutions of the project to this email along with a screenshot of your error on Canvas. However, you will not be allowed to submit documents that are missing from the submission after initial grades have been returned. This is a graduate course and students are responsible for their submissions.

Grading and Feedback
After every Project deadline, feedback on incorrect answers will be released on Canvas. After every Quiz is due, their respective solutions (including your original answers) will be released on Canvas. After Exam deadline, you will be given feedback on the questions you answered incorrectly only. We will not release full solutions to the exam, which is classified as an "Assignment" on Canvas for technical reasons. So, this feedback can be found under the exam assignment feedback on Canvas once the grades have been released.

Technology Requirements

Computer Hardware and Software

- Browser and connection speed: An up-to-date version of Google Chrome or Firefox is strongly recommended. 2+ Mbps is recommended.
- Operating System: Windows XP or higher with latest updates. Mac OS X 10.6 or higher with latest updates. Any Linux recent distribution will work so long as you can install Python and OpenCV.
- Virtual Machine: You will be provided with virtual machines (VM) for performing many of the class assignments and projects. For the projects, the supplied resources are identical to those used to test your submissions. Details for downloading and installing each VM can be found in the project write-ups. You should have at least 30GB of free storage (although more, e.g., 80GB, is recommended).

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, and other like resources are allowed unless any or all of these materials are allowed. These exams are delivered via a tool called Honor lock. Honor lock 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. Honor lock is available 24/7, and all that is needed is a computer, a working webcam/microphone, your ID, and a stable internet connection.

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 Honor lock authentication process, where you will take a picture of yourself, show your ID, and complete a scan of your room. Honor lock will be recording your exam session through your webcam, microphone, and recording your screen. Honor

lock 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 Education
Ed will be used as the main communications medium for this class. You are encouraged to post discussions on issues you are having with projects or otherwise. Please do not post solutions to Ed. If you do, we may revoke your access to our Ed page. Please do not post new messages addressing us individually (e.g., Wenke Lee). We have multiple TAs answering Ed posts on a rotating basis so you will not get a response from Wenke if you do this. Only if the TA feels the need to, they (the TA) will contact the Head TA to see if the situation can be resolved. If it cannot be resolved, the Head TA will contact the Instructor and the Instructor will have the final say on the situation.

Email & Communication Policy
In order to handle a class of this size, we must delegate specific topics/questions for each Instructor/Head TA/TA to handle/answer. Each Instructor/Head TA/TA will only read the types of emails delegated to them as listed below. They will delete and ignore any other types of emails.

- **Head TA email:** mchen461@gatech.edu; **Instructor email:** wenke@cc.gatech.edu;
- If you are seeking **project extensions**, **please post on Ed** using the "extension" tag.
- If you have a regrade request, use the Google Forms link we send you after each project grade release.
- If, after your project has been regraded, you are still unsatisfied with your grade, please post privately on Ed.
- If you would like to request a deadline extension (projects, quizzes, exams, etc.) because of a Georgia Tech approved reason (e.g., medical emergency), please email the Head TA, CC the Instructor, and attach appropriate documentation (e.g., a doctor's note for a medical emergency) to your email. Your email's subject should be named "CS6262 - Deadline Extension Request". If you do not write the subject as such, your email will be deleted/ignored.
- If exam grades have been released but you do not see your grade, please email the Head TA with the subject "CS6262 - Exam Grade Issue". If you do not write the subject as such, your email will be deleted/ignored.
- If quiz grades have been released but you do not see your grade, please email the Head TA with the subject "CS6262 - Quiz Grade Issue". If you do not write the subject as such, your email will be deleted/ignored.
- If project grades have been released but you do not see your grade, please post privately on Ed.
- If you would like to ask a question about a particular Instructor/Head TA/TA's office hour (or office hours' content), email that particular Instructor/Head TA/TA with the subject "CS6262 - Office Hours".
- If you would like to ask a question about unclear (or incorrect) wording in projects, quizzes, exams, etc., please post publicly on Ed.
- If you would like to ask a question regarding help or advice on a project, please post publicly on Ed.
- If a TA cannot resolve your issue on Ed (after multiple posts with you), then that TA will contact the Head TA in order to resolve the situation. If the Head TA cannot resolve the situation, that Head TA will contact the instructor and they will have the final say on the situation. Do not directly contact the Head TA or the Instructor. They will not answer your emails unless otherwise noted here in this list.

- If a TA has not responded to your Ed post within 2 days, please email the Head TA with the subject "CS6262 - Ed Post Issue" and provide a link to that Ed post. If you do not write the subject as such, your email will be deleted/ignored.
- If you have taken the class previously or have .ova files from prior courses, please do not use those files to complete the projects because this will result in a zero.
- Please do not put your projects on public GitHub. Otherwise, if a student (in the future) copies your codes/projects, the student obviously violates the honor code, but you will also be implicated.
- Do not contact us about releasing grades and solutions. We will do this only when all student submissions are in (accounting for those who may have had a Georgia Tech approved reason such as a medical emergency) and we are ready to release them.
- Do not contact us about re-grading your project after you have submitted a regrade request but before we have sent you an email notifying you that your project has been regraded. Trust that we are diligently working on re-grading your project and we will notify you when we are finished.

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: Using chat GPT for your assignments will be considered plagiarism in this course.

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.

Georgia Institute of Technology
Course Syllabus: CS6262 Network Security

Course Schedule

Week	Modules	Quiz	Project
1 Jan 8	DDoS Attacks; Cybercrimes	Quiz #1 released on 1/13 and due on 1/21	Project #1 released on 1/20 due on 2/4
2 Jan 15	Penetration Testing; Browser Security Model	Quiz #2 released on 1/20 and due on 1/28	
3 Jan 22	Web Session Management		
4 Jan 29	HTTPS; Security of Internet Protocols	Quiz #3 released on 2/3 and due on 2/11	Project #2 released on 2/3 and due on 2/25
5 Feb 5	DNS Security; Advanced Malware Analysis	Quiz #4 released on 2/10 and due on 2/18	
6 Feb 12	Mobile Malware; Cloud Security: VM Monitoring	Quiz #5 released on 2/17 and due on 2/25	
7 Feb 19	Property-preserving Encryption; Oblivious RAM	Quiz #6 released on 3/2 and due on 3/10	Project #3 released on 2/24 and due on 3/17
8 Feb 26	Botnet Detection	Quiz #7 released on 3/9 and due on 3/17	
9 Mar 4	Internet-scale Threat Analysis: Scanning; Domain and Network Reputation	Quiz #8 released on 3/16 and due on 3/24	
10 Mar 11	Machine Learning for Security		Project #4 released on 3/16 and due on 3/31
11 (Mar 18-22 Spring break) Mar 25	Data Poisoning and Model Evasion	Quiz #9 released on 3/30 and due on 4/7	
12 April 1	Basics of Blockchains and Bitcoins		
13 April 8	Topics in Cryptocurrencies; Attack Tolerant Systems	Quiz #10 released on 4/6 and due on 4/14	Project #5 released on 3/30 and due on 4/21
16 April 19 – April 22	**One- Hour Close-Everything Exam** **Available time window:** April 19 9:00 AM EST – April 22 11:59 PM EST		