OVERVIEW

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 model, 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

PREREQUISITES

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 6035).* Prior programming experience with C or Java *(or similar language)* is recommended.

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 the 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.

CLASSROOM MANAGEMENT TOOLS

All video lectures are located on **Udacity**. Everything else can be accessed here through Canvas. Below summarizes all the course-related activities and provides a link to their location in edX or Canvas.

- **Video Lectures:** All video lectures are located on **Udacity**.
- **Projects:** are located on **Canvas**.
- **Quizzes:** are located on **Canvas**.
- **Reading Materials:** are located on **Canvas**.
- **Piazza Discussion:** are located on **Canvas**.
- **Grades:** are located on **Canvas**.

PROCTORING INFORMATION

All course exams will be proctored - the proctored exams will be your Exam 1 and Exam 2. A proctored exam 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 Proctortrack. Proctortrack uses multi-factor biometric authentication to verify the identity of students, upon entry. Each student will provide a face, ID, and knuckle scans, which will be measured against the student's baseline biometric profile, stored on file. You may also be asked to scan the room around you. Please have a small mirror handy for the room scan. You will have the opportunity to take an onboarding quiz to become familiar with how it all works. The onboarding quiz will be a practice quiz that will not affect your grades in the course. You can take the onboarding quiz as many times as you want. All potential violations are reviewed by a human. If you have any issues with Proctortrack while taking the graded exam, reach out to Proctortrack 24/7 support: **https://www.proctortrack.com/support/**.

PIAZZA

Piazza will be used as the main communications medium for this class. You are encouraged to post discussions on issues you're having with projects or otherwise. Please do not post solutions to Piazza. If you do, we may revoke your access to our Piazza page. Please do not post new messages addressing us individually (e.g., Wenke Lee). We have multiple TAs answering Piazza 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.

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.

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 expectation 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.

COURSE POLICIES

All work for this class is to be done individually. You are strongly urged to familiarize yourselves with the GT Student Honor Code rules. Specifically, the following is not allowed:

- Copying, with or without modification, someone else's work when this work is not meant to be publicly accessible (e.g., a classmate's program or solution).
- Submission of material that is wholly or substantially identical to that created or published by another person or persons, without adequate credit notations indicating authorship (plagiarism).
- Putting 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.

You are encouraged to discuss problems and papers with others as long as this does not involve copying of code or solutions. Any public material that you use (open-source software, help from a text, or substantial help from a friend, etc...)

should be acknowledged explicitly in anything you submit to us. If you have any doubt about whether something is legal or not please do check with the class Instructor or the TA.

PROBLEM ESCALATION POLICY
If you need help and/or have a problem, you should contact the following people in the following order:
(1) Your TA
(2) Your Head TA
(3) Your Instructor (via email)

If you are not comfortable talking to your TA about a particular issue, please contact the instructor ASAP. ***TA schedules will be posted in Canvas via a separate document.***

GRADING AND FEEDBACK

After every Project deadline, their respective solutions will be released on Canvas. After every Quiz is due, their respective solutions *(including your original answers)* will be released on Canvas.

After each Exam deadline, you will be given feedback on the questions you answered incorrectly only. We will not release full solutions to the exams. Each exam 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

ASSIGNMENT DISTRIBUTION AND GRADING SCALE

Assignments	Weight
Quizzes	**10%**
Projects	**80%**
Exams	**10%**

GRADING SCALE
Your final grade will be assigned as a letter grade according to the following scale:
A 90-100%
B 80-89%
C 70-79%
D 60-69%
F 0-59%

Grading will be based on:

- **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 web security - attacks and defenses (15%)
  - Project #3: advanced malware analysis - iterative program analysis and debugging of malware (20%)
  - Project #4: network monitoring - write NIDS rules to identify botnet traffic (15%)
  - 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 the slide materials and projects.

LATE ASSIGNMENTS

No late submissions (projects, 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. If you submitted late because you overslept, forgot to post, etc. we will not accept your submission. Even if your submission is only 1 minute late, we will not accept it.

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, Piazza, or otherwise. We will only accept them through a Google Form submission. A link to each Project regrade 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've worded 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 Piazza. 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.

APPEALING GRADES

You have the right to question your grade on any assignment; but you must initiate discussion about the grade within one week of receiving the grade. All regrade requests should be submitted through the google-form which will be available after the evaluation of the project.

Grade issues addressed outside of the requirements will not be considered. Pay attention to your grades. If something doesn't look right, address it immediately! Be sure to follow the guidelines outlined in the "Problem Escalation Policy". It is your responsibility to ensure that all the grades on Canvas are correct before the final 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.

CLASS SCHEDULE

Week	Date(s)	Topics	Quiz	Project
Week 1	(1/7)	DDoS Attacks		

	(1/10)	Cybercrimes	Quiz #1	
Week 2	(1/14)	Penetration Testing	Quiz #2	**Project #1**
	(1/16)	Browser Security Model		
Week 3	(1/21)	Web Session Management		
Week 4	(1/28)	HTTPS	Quiz #3	**Project #2**
	(1/31)	Security of Internet Protocols		
Week 5	(2/4)	DNS Security	Quiz #4	
	(2/6)	Advanced Malware Analysis		
Week 6	(2/11)	Mobile Malware	Quiz #5	**Project #3**
	(2/13)	Cloud Security: VM Monitoring		
Week 7	(2/18)	Property-preserving Encryption, Oblivious RAM	Quiz #6	
Week 8	(2/25)	Botnet Detection	Quiz #7	
Week 9	(3/4)	Internet-scale Threat Analysis: Scanning		**Project #4**
	(3/6)	Domain & Network Reputation	Quiz #8	
Week 10	(3/11)	Machine Learning for Security		
Week 11	**Spring Break March 18th – March 24th**			
Week 12	(3/25)	Data Poisoning and Model Evasion	Quiz #9	
	(3/27)	Basics of Blockchains and Bitcoins		**Project #5**
Week 13	(4/1)	New & Alternative Cryptocurrencies		
Week 14	4/8)	Attack Tolerant Systems	Quiz #10	

Week 15	**EXAM (4/15)**	**Required One-Hour Close - Everything Exam; available time window: 4/19 9:00 AM ET through 4/22 11:59 PM ET**
Week 16	**READING WEEK NO ASSIGNMENTS**	

SUBJECT TO CHANGE STATEMENT

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