Spring 2020	
Delivery: 100% Web-Based, Synchronous	**Offered on:** Canvas/edX
Dates course will run: Jan 6 – April 30, 2020	

Instructor Information

Dr. Wenke Lee	Office: CODA E0964B (9th Floor)
Weekly Office Hours via Blue Jeans per announcements	Email: wenke.lee@gmail.com

General Course Information

Description

This course will help students develop both in-depth knowledge and hands-on skills in a number of important cybersecurity areas, including software security, malware and threat analysis, end-point security, network security, web security, mobile security, and machine learning based security analytics. The lecture materials of each topic area are drawn from latest research papers and prototypes, and comprehensive projects are assigned to help students master each area. The main topics include:

1. Software security: we will study software vulnerabilities such as memory safety errors and protection mechanisms such as CFI, ASLR, and DEP. We will also study program analysis techniques such as symbolic execution and fuzzing for finding software vulnerabilities and generate exploits. A project can involve applying and extending program analysis tools to find exploitable bugs in programs and generate input that can trigger these bugs.

2. Malware analysis: we will study how to build a malware analysis environment that is both save and live. In particular, we will study how to analyze malware to find its triggering, or, dispatching behaviors, and configure a virtualized environment where that malware gets the input it needs so that it reveals its intended activities. We will also study threat analysis, in particular, how to obtain and share threat intelligence. A project can involve applying and extending a malware analysis system to examine the behaviors of a new malware family.

3. End-point security: we will study how to monitor computer activities through system call hooking and virtual machine introspection. We will also study forensic analysis using system-wide record-and-replay technologies. A project can involve using a record-and-replay system to identify the root cause, or, the entry point, of a long-running attack.

4. Network security, we will first review vulnerabilities of network protocols such as spoofing and standard prevention mechanisms such as TLS. We will then study network monitoring, including network intrusion detection and alert correlation. A project can involve extending an open-source intrusion detection system to detect stealthy network attacks.

5. Web security: we will first review browser security models such as same-origin policy and content-security policy. We will then study more advanced topics including how to provide fine-grained access control to third-party scripts, and the security vulnerabilities of WebView. A project can involve implementing a phishing attack using iframes/popups in WebView and then implementing a defense.

6. Mobile security: we will first review the iOS and Android security models. Then we will study Android malware and gray-ware, that is, those that leak user privacy. We will also discuss the attack ecosystem including rooting attacks and third-party app stores. A project can involve implementing an Android malware clustering algorithm that atomically classify Android malware and gray-ware.

7. Machine learning for security analytics: we will first study how machine learning algorithms, in particular, deep learning, can be used to automatically produce security models such as malware classifiers and intrusion detection rules. We will then study how the machine learning process can be subverted by attackers and how to improve the robustness of machine learning. A project can involve using and extending an evaluation system to generate evasion attacks against a machine learning based model and produce the more robust model.

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).* Ideally, you should also have taken a network security course (*there is only a small amount of overlap between this course and CS6262*). Prior programming experience with C or Java *(or similar language)* is required.

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 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

Course Requirements, Assignments & Grading

Assignment Distribution and Grading Scale

Assignments	Weight
Projects	**100%**
Exam	**10%**
Extra Credit	**5%**

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%

Description of Graded Components

- **Seven required individual projects for a total of 90%:**
  - Project #1: Use program analysis tools, e.g., AFL, and Angr, to find vulnerabilities in a program and produce exploits accordingly (10%)
  - Project #2: Use and extend the malware analysis and experiment environments on new malware families to enumerate the input conditions and behaviors of the malware. (15%)
  - Project #3: Implement a host-based intrusion detection system using system-call hooking. The system should be able to detect anomalous or known malicious system call sequences when a program is exploited or when a malware is executed. (15%)
  - Project #4: Using a virtualized malware experiment system, extend an open-source IDS to include a sandbox-based malware detection system, which can be based on the host-based IDS in Project 3. That is, the IDS will automatically identify an attached executable in network traffic, send it to the sandbox for analysis and receive result from the sandbox. (10%)
  - Project #5: Implement a vulnerable WebView Android app and the corresponding web server to demonstrate that untrusted iframe/popup inside WebView can be used to launch attacks such as accessing sensitive mobile functionalities. (15%)
  - Project #6: Android repackaging attack: obtain an Android app and install it, then disassemble it, inject malicious code into it, and then repack the app. Install the repackaged app and trigger the malicious code to launch attack. (15%)
  - Project #7: Use MLsploit to evaluate and improve a ML-based security model: build an anomaly detection model using system call sequence data, have MLsploit show evasion attacks, improve the model, and show existing attacks provided by MLsploit no longer work. (10%)
- **10% exam:** T/F and multiple-choice, close-everything, at the end of semester. Exam questions are based on the 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.

You will be given Google form for each project. There is no regrade the extra credit submission.

Late Assignments

No late submissions 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 submit late because you overslept, forgot to post, etc. we will not accept your submission. Even if your submission is only 1 minute late, it won't be accepted.

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.

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 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 a virtual machine (VM) useful for performing class assignments and projects. For the projects, the supplied resources are identical to those used to test your submissions. Details for downloading and installing the VM can be found on Canvas.

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 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/**.

Course Policies, Expectations & Guidelines

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.

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.

- 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 Piazza.
- 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 "CS8803 - 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 "CS8803 - 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 "CS8803 - 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 Piazza.
- 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 "CS8803 - Office Hours".
- If you would like to ask a question about unclear (or incorrect) wording in projects, quizzes, exam, etc., please post publicly on Piazza.
- If you would like to ask a question regarding help or advice on a project, please post publicly on Piazza.
- If a TA cannot resolve your issue on Piazza (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 Piazza post within 2 days, please email the Head TA with the subject "CS8803 - Piazza Post Issue" and provide a link to that Piazza 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've submitted a regrade request but before we've 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're 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 as 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.

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.

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.

Course Schedule

Week	Date(s)	Topics	Project
Week 1	(1/7)	Lesson 1: Software vulnerabilities	
	(1/9)	Lesson 2: Software Protection	
Week 2	(1/14)	Lesson 3: Program analysis	Project #1 released 1/14 due 1/28
Week 3	(1/21)	Lesson 4: Fuzzing and symbolic execution	
Week 4	(1/28)	Lesson 5: Malware analysis environment	Project #2 released 1/28 due 2/11
Week 5	(2/4)	Lesson 6: Threat Intelligence analysis	
Week 6	(2/11)	Lesson 7: Host-based monitoring	Project #3 released 2/11 due 2/25
Week 7	(2/18)	Lesson 8: Forensics analysis	
Week 8	(2/25)	Lesson 9: Network protocol vulnerabilities	Project #4 released 2/25 due 3/10
	(2/27)	Lesson 10: Network attack prevention and detection	
Week 9	(3/3)	Lesson 11: Browser access control	
	(3/5)	Lesson 12: Third-party scripts and WebView	
Week 10	(3/10)	Lesson 13: Mobile security models	Project #5 released 3/10 due 3/24
Week 12	(3/24)	Lesson 14: Mobile ecosystem	Project #6 released 3/24 due 4/7
Week 13	(3/31)	Lesson 15: ML for security	
	(4/2)	Lesson 16: Adversarial machine learning	
Week 14	(4/7)		Project #7 released 4/7 due 4/21
Week 15	(4/13)	EXAM: Required One-Hour Close - Everything Exam; available time	

		window: 4/17 9:00 AM ET through 4/19 11:59 PM ET