CS6264 Syllabus

Information Security Lab: System and Network Defenses, O01 and OCY, 3.0

Sections O01 and OCY, Summer and Fall 2026

Instructor Information

Instructor: Wenke Lee

Email: wenke@cc.gatech.edu

General Course Information

Description

This course will help students develop both in-depth knowledge and hands-on skills in several important cybersecurity areas, including software security, malware and threat analysis, endpoint security, network security, web security, mobile security, and machine learning based security analytics. The lecture materials of each topic area are drawn from the 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 generating 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 safe and lively. 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, particularly 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. Mobile security: We will first review the iOS and Android security models. Then we will study Android malware and grayware, 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 classifies Android malware and grayware.

4. 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.

5. 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.

6. Web security: We will first review browser security models, such as the 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 comprehensively demonstrating two typical roles in web attacks: attackers who discover exploits and launch attacks, and forensic investigators who develop auditing tools and discover the evidence of the attacks.

7. Machine learning for security analytics: We will first study how machine learning algorithms, particularly 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 a more robust model.

Course Learning Outcomes

Upon successful competition of this course, you should have the in-depth knowledge and hands-on skills in several important cybersecurity areas, including software security, malware and threat analysis, endpoint security, network security, web security, mobile security, and machine learning based security analytics.

Required Course Materials

PowerPoint slides of the lectures will be made available.

Grading Policy:

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

A	90-110%
B	80-89%
C	70-79%
D	60-69%
F	0-59%

Assignments

- 7 projects include extra credits, for a total of 85 points
- 10 quizzes, for a total of 10 points
- 1 extra credit exam, for 5 points
- 1 exam for 10 points

Description of Graded Components

Your projects must be submitted to Gradescope and be graded according to the requirements specified in the project assignments.

Course Policies

Attendance and/or Participation

You are expected to study all the lecture materials and attend most of the lectures and office hours.

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. Review Georgia Tech's Honor Code and the student Code of Conduct.

Any student suspected of cheating or plagiarism 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.

Core IMPACTS

Core IMPACTS is the University System of Georgia's General Education curriculum. If you are teaching a course that counts towards Core IMPACTS, you should include a syllabus statement about the Core area and associated career competencies. This resource developed by the Center for Excellence in Teaching and Learning and Online Education at Georgia State University includes template syllabus statements for each of the Core IMPACTS areas that you may adapt for your course.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services (404-894-2563) 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. The Student-Faculty Expectations articulate 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.