ECE 8813: Advanced Computer Security

General Information:

Digital technologies impact every aspect of our daily lives. As such, good cybersecurity practices are now essential for protecting not only our nation's critical infrastructure, but also for ensuring the privacy of our data, the secrecy of our communications, and the everyday functioning of global economies. The goal of the course is to help spur engaging discussions on selected research topics in computer security/privacy that propose solutions for building resilient and secure digital ecosystems. Unlike other areas of computer science (e.g., software development), where practitioners can leverage simplifying assumptions to quickly complete a task derived from an external need, cybersecurity practitioners need to be aware of, and repeatedly question, the validity of any simplifying assumptions to either prove a system's security or find exploitable weaknesses. As such, in this specific field, being able to ask the right questions and finding the right problems to solve is perhaps just as important as being able to solve them.

This course is research-oriented and structured around research papers that students must read before each session. Students will also work on a course project that involves validating or extending ideas covered in one or more topics discussed in class. Potential projects will be suggested, but students are encouraged to work on topics that they are passionate about. Students will be required to read the papers assigned during the semester and be able to competently discuss the material in class. Each student will be responsible for jointly leading (with the instructor) a discussion based on the assigned paper(s) for the week. The instructor will provide a comprehensive overview of the topic. Each student will be responsible for submitting a constructive written critique of the main paper(s) assigned each week. The critique will follow a standard format that critically evaluates the paper(s) (e.g., questioning the assumptions, questioning whether the experiments met the stated objectives, discussing flaws or omissions in the methodology and/or findings, suggesting areas for improvement, etc). The overall goal is to assess the student's understanding and critical thinking.

Basic Info:

Class location: TBD
Office: Klaus 3360
Email: fabian@ece.gatech.edu
Class date/time: T/TH 12:30 - 1:45 pm
Office hours: M/W 10-11am and by appointment

Prerequisites

This is a graduate course, therefore, students are expected to have undergraduate-level background on computer architecture, operating systems, and networking. ECE 4115 or equivalent is also strongly advised as a prerequisite. In addition, familiarity with low-level systems
programming (e.g., C and assembly) will be necessary for understanding the details of some of the assigned readings, and will be helpful in completing in-class exercises.

Materials:

There is no required textbook for this course. Instead, we will study published research papers from top-tier academic venues in computer security. Topics to be covered include (but are not limited to), software security attacks (e.g, memory disclosure exploits, non-control data attacks) and defenses, computer forensics techniques (e.g, recovery of forensic information from memory snapshots), securing the software supply chains (e.g., automated techniques for software bill of materials), directed vulnerability discovery (e.g, fault isolation and fuzzing), software and hardware-based side channel attacks, protocol reverse engineering, malware classification and provenance, transparent and privacy-preserving systems, and techniques for countering cybercrime.

Learning Objectives

Given that the course assignments and project will focus on applied systems topics, students will be assessed in several ways (e.g., whether they can apply learned knowledge in a previously demonstrated way, can apply learned knowledge in contexts not seen before, can independently close any knowledge gaps when completing a task, or can demonstrate mastery by being able to teach others). Upon successful completion of the course, students will:

- Be able to understand fundamental notions within the field of computer security, and engage in critical discussions thereof.
- Be able to identify threats, vulnerabilities, attacks (and associated countermeasures) to critical cyber infrastructure.
- Have a better appreciation for concerns about security and privacy, and be better able to analyze proposals to protect user privacy.
- Be able to study cutting-edge research papers and provide constructive feedback based on the scientific merit, novelty, and thoroughness of the work.
- Be able to describe technical computer security concepts to their peers.
- Be able to propose ideas to open-ended research problems and to rapidly prototype their solutions.

Assignments & Grading

There will be three mini-projects (with 1 or 2 week deadlines) related to topics in the course. In addition, students are expected to work in small teams on a half-semester long research project. While several project ideas will be suggested, students are encouraged to pursue projects that align with their own graduate research — as long as that research has applicable security or privacy components.
Breakdown:

30% for programming assignments.
50% for research project (including final writeup).
20% for paper presentation and class participation.

Each team must prepare a final presentation and report on the outcomes of their research project during the final instruction days of class.

**Honor Code**

Students are expected to abide by the Georgia Tech Academic Honor Code. Honest and ethical behavior is expected at all times. All incidents of suspected dishonesty will be reported to and handled by the Office of Student Integrity. You will have to do all assignments individually unless explicitly told otherwise. You may discuss with classmates but you may not copy any solution (or any part of a solution).

**Learning Accommodations**

Whenever needed, the instructor will make accommodations for students with documented disabilities. These accommodations must be arranged in advance and in accordance with the Office of Disability Services.

**Academic Honor Code**

Students are expected to abide with Georgia Tech’s academic honor code.