Syllabus for ECE/CS 8803 ECS: Empirical Computer Security

(Last Revision: March 26, 2020)

Instruction Information

Instructor Name:	Prof. Frank Li
Lecture Hours:	Monday / Wednesday, 2:00PM - 3:15PM (3 Unit Course)
Lecture Location:	Room C457, Van Leer
Office Hours:	TBD
Email:	frankli@gatech.edu

General Information

Description

Empirical security research seeks to understand how computer security concerns manifest in practice. For example, what strategies and techniques do attackers actually use, and how do they profit from their actions? How do users behave in different security contexts, and why do they behave in those (often insecure) ways? Gaining this understanding is vital for driving improvements in real-world security.

This seminar-style course will cover both classic and recent empirical security studies across a wide range of security topics, including Internet security, underground ecosystems, usable security, and online privacy. You will analyze, critique, and discuss these works. Beyond broadening your knowledge of real-world computer security, you will gain a deeper understanding of sound and rigorous measurement methodologies for applying to your own work.

Pre- &/or Co-Requisites

You are expected to have familiarity with core computer security and computer networking concepts.

(Expected) ECE 4410 Internetwork Programming / CS 4251 Computer Networking *or equivalent*

(Expected) ECE 4115 Introduction to Computer Security / CS 4235 Introduction to Information Security *or equivalent*

(Helpful But Not Expected) ECE4112 Internetwork Security / CS 4237 Computer and Network Security *or equivalent*

Course Goals and Learning Outcomes

The goals of this course are to expand your understanding of real-world security and prepare you to:

- Recognize how theory and empiricism complement each other in computer security research
- Identify limitations or shortcomings in empirical security methodologies
- Engage in critical discussion around key research topics in computer security
- Write and present a paper conforming to the security research community's standards
- Propose sound and rigorous measurement methodologies for open-ended research problems

Course Requirements & Grading

As a seminar-style course, the grading will be based on reading and analyzing the assigned paper readings, engaging with class discussion, and conducting and presenting a research-oriented final project.

Assignment	Weight	Description
Participation	10%	Attend and engage with class meetings (ask and answer questions, provide comments).
Discussion Lead	10%	Present 1-2 paper summaries during the semester and help lead the discussion.
Paper Summaries (written)	20%	For each assigned paper, submit a brief paper summary, analysis, and questions.
Final Project	60% Total	Research-oriented project.
- Proposal	10%	Write a project proposal and present to the class for feedback.
- Project Writeup	40%	Submit a research-style paper on your project.
- Project Presentation	10%	Present a talk and/or demo on your project.

There are no extra credit opportunities.

Grading Scale

The course will not be graded on a curve. 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%

Course Materials

Course Text

There is no required course textbook.

For optional supplemental or background reading, we recommend: Introduction to Computer Security, Michael T. Goodrich and Roberto Tamassia, Addition Wesley, 2011.

Course Website and Other Classroom Management Tools

TBD

Course Expectations & Guidelines

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. 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 an assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

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 ap-

pointment 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.

Attendance and/or Participation

As this is a seminar-style course, attendance and engagement with class discussions is vital. While I will not be taking explicit attendance each class, I will track those who speak and participate. Participation is 10% of your grade.

In addition, students will be expected to present summaries of 1-2 papers throughout the semester and lead the associated class's discussion. This discussion leading accounts for an additional 10% of your grade.

You may need to miss a class for legitimate reasons (e.g., sick, onsite interviews). For illnesses or personal emergencies, contact the Office of Student Life, as described in the policies at http://www.catalog.gatech.edu/policies/student-absence-regulations/. For Institute Approved Absences, we adhere to the Institute policies at https://registrar.gatech.edu/info/institute-approved-absence-form-for-students.

Collaboration & Group Work

Paper summaries should be written and submitted separately by each student, but discussion about papers in groups is allowed and encouraged within reason (e.g., student should still submit distinct paper analyses).

Final projects can be done in groups of 2-3 people (depending on class size).

Extensions & Late Assignments

Assignments are due at the time listed in the schedule. There are no undocumented exceptions. **If you have an emergency situation or a school sanctioned exception, please contact me before the due date so we can adjust your assignment deadlines (some documentation may be needed).**

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.

Student Use of Mobile Devices in the Classroom

As this course is heavily based on class discussion, I ask that you stay engaged and limit your mobile device usage during class.

Course Schedule

The exact course schedule, including paper reading assignments, will be determined shortly.

The topics covered in this course will include:

- Ethics and Legality in Computer Security Research (particularly involving empirical measurements)
- Core Measurement Metrics, Concepts, and Common Flaws (e.g., Base-Rate Fallacy, machine learning limitations in practice)
- Network Security: Understanding Internet Attacks and Defenses in Practice
- Understanding Underground Cybercriminal Ecosystems: Spam, Malware, Social Networks
- Network/Internet-Wide Scanning and its Applications
- Measuring Censorship
- Empirical Attacks on Cryptography
- Usable Security and Quantifying User Behavior
- Internet and Web Privacy
- Software Vulnerabilities and Security
- Security in the Physical World
- Side-Channel Attacks on Cryptography and Hardware