Syllabus for ECE/CS 8803 ECS: Empirical Computer Security

(Last Revision: Oct 25, 2022)

Instruction Information

Instructor Name:	Prof. Frank Li
Course Hours:	Tuesday / Thursday, 5:00PM - 6:15PM (3 Unit Course)
Course Location:	Van Leer C240
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

Strategic Performance Indicators (SPIs)

Outcome 1: Students will demonstrate expertise in a subfield of study chosen from the fields of electrical engineering or computer engineering. Upon successful completion of the course, the student should be able to:

- Explain different classes of empirical security methods and their benefits and limitations

Outcome 2: Students will demonstrate the ability to identify and formulate advanced problems and apply knowledge of mathematics and science to solve those problems. Upon successful completion of the course, the student should be able to:

- Determine an appropriate empirical method to apply given a security or privacy scenario to measure

Outcome 3: Students will demonstrate the ability to utilize current knowledge, technology, or techniques within their chosen subfield. Upon successful completion of the course, the student should be able to:

- Apply common software tools to collect data on a security or privacy phenomena

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	20%	Attend and engage with class meetings (ask and answer questions, provide comments).
Discussion Lead	10%	For one class during the semester, prepare and present a 25 minute presentation summarizing the class's reading, and help lead the class discussion. For each class, 1-2 student(s) will serve as discussion lead(s).
Paper Summaries (written)	20%	For each assigned paper, submit a brief paper summary, analysis, and questions. In total, 2 summaries can be skipped during the semester. If you lead a discussion solo, you can skip an additional summary (for a total of 3 summary skips).
Final Project	50% Total	Semester-long research project (groups of 2-3 students).
- Project Proposal	10%	Submit a project pre-proposal for feedback on project idea (due 2/17). Write and present a project proposal (on 3/8 and 3/10, subject to change).
- Project Presentation	10%	Present a talk and/or demo on your final project (starting 4/19).
- Project Writeup	30%	Submit a research-style paper on your final project (due 4/29).

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

We will use Canvas for course organization and Piazza for discussion and classwide communication.

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 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.

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 20% 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., students 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

Below is the current course schedule, which is subject to some change as the semester progresses.

===== Week 1 =====

1/10: First Class - Introduction to Empirical Computer Security
No readings, but will cover topics discussed in the following papers:
- SoK: Science, Security, and the Elusive Goal of Security as a Scientific Pursuit. https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/scienceAndSecuritySoK.pdf
- Strategies for Sound Internet Measurements: https://www.icir.org/vern/papers/meas-strategies-imc04.pdf
- The Base-Rate Fallacy and the Difficulty of Intrusion Detection. http://people.scs.carleton.ca/~soma/id-2007w/readings/axelsson-base-rate.pdf
- Outside the Closed World: On Using Machine Learning For Network Intrusion Detection. https://personal.utdallas.edu/~muratk/courses/dmsec_files/oakland10-ml.pdf
- Legal and Ethical Research:
    - http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.145.1147&rep=rep1&type=pdf
    - http://mdbailey.ece.illinois.edu/publications/wecsr10_final.pdf

1/12: Denial of Service + Backscatter Measurements (Classic)
Reading: Inferring Internet Denial-of-Service Activity.
https://cseweb.ucsd.edu/~savage/papers/UsenixSec01.pdf

===== Week 2 =====

1/17: Distributed Denial of Service (Modern)
Reading: Understanding the Mirai Botnet.
https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf

1/19: Network Scanning Applications

Reading: Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices.
https://factorable.net/weakkeys12.extended.pdf

===== Week 3 =====

1/24: Internet-wide Network Scanning
Reading: ZMap: Fast Internet-Wide Scanning and its Security Applications.
https://zmap.io/paper.pdf

1/26: Other Network Measurements
Reading: A Longitudinal, End-to-End View of the DNSSEC Ecosystem.
https://www.cs.umd.edu/~dml/papers/dnssec_sec17.pdf

===== Week 4 =====

1/31: Underground Ecosystem - Spam
Reading: Spamalytics: An Empirical Analysis of Spam Marketing Conversion.
https://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf

2/2: Underground Ecosystem - Malware
Reading: Measuring Pay-per-Install: The Commoditization of Malware Distribution.
https://www.usenix.org/legacy/events/sec11/tech/full_papers/Caballero.pdf

===== Week 5 =====

2/7: Underground Ecosystem - Underground Markets
Reading: Click Trajectories: End-to-End Analysis of the Spam Value Chain.
https://cseweb.ucsd.edu/~savage/papers/Oakland11.pdf

2/9: Underground Ecosystem - Social Networks
Reading: Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse.
http://www.inwyrd.com/blog/wp-content/uploads/2010/03/usenix20131.pdf

===== Week 6 =====

2/14: Web Measurements - Security
Reading: Thou Shalt Not Depend on Me: Analysing the Use of Outdated JavaScript Libraries on the Web.
https://www.ndss-symposium.org/wp-content/uploads/2017/09/ndss2017_02B-1_Lauinger_paper.pdf

2/16: Web Measurements - Privacy
Reading: The Web Never Forgets:Persistent Tracking Mechanisms in the Wild.
https://core.ac.uk/download/pdf/34609562.pdf
Project Pre-Proposals Due

===== Week 7 =====

2/21: Web Measurements - Human Factors

Reading: Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_akhawe.pdf

2/23: Authentication / Passwords
Reading: The Tangled Web of Password Reuse.
https://www.cs.umd.edu/class/spring2017/cmsc818O/papers/tangled-web.pdf

===== Week 8 =====

2/28: No Class: NDSS Conference
Work on your projects

3/2: No Class: NDSS Conference
Work on your projects

===== Week 9 =====

3/7: Project Proposal Presentations (Subject to change based on class enrollment)
No readings

3/9: Project Proposal Presentations (Subject to change based on class enrollment)
No readings

==== Week 10 =====

3/14: Usable Security (Classic)
Reading: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.40.9279&rep=rep1&type=pdf

3/16: Usable Security (Modern)
Reading: Android Permissions: User Attention, Comprehension, and Behavior
https://www.cs.ucy.ac.cy/courses/EPL682/papers/usable-1.pdf

==== Week 11 =====

3/22: Spring Break (No Class)

3/24: Spring Break (No Class)

==== Week 12 =====

3/28: Security in Society - Censorship
Reading. Encore: Lightweight Measurement of Web Censorship with Cross-Origin Requests.
https://conferences.sigcomm.org/sigcomm/2015/pdf/papers/p653.pdf

3/30: Security in Society - Nation-State Attacks
Reading: When Governments Hack Opponents: A Look at Actors and Technology.
https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-marczak.pdf

==== Week 13 =====

4/4: Security in Society - Beyond Traditional Computing
Reading: The Spyware Used in Intimate Partner Violence.
https://pages.cs.wisc.edu/~chatterjee/papers/IPV_Spyware.pdf

4/6: Software Security - Zero-Day Vulnerabilities
Reading: Before we knew it: An empirical study of zero-day attacks in the real world.
http://users.umiacs.umd.edu/~tdumitra/papers/CCS-2012.pdf

==== Week 14 =====

4/11: Software Security - Patching Vulnerabilities
Reading: The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching.
http://users.umiacs.umd.edu/~tdumitra/papers/OAKLAND-2015.pdf

4/13: Cyber-Physical Security
Reading: Comprehensive Experimental Analyses of Automotive Attack Surfaces.
http://www.autosec.org/pubs/cars-usenixsec2011.pdf

==== Week 15 =====

4/18: Final Project Presentations
No readings

4/20: Final Project Presentations
No readings

==== Week 16 =====

4/25: Final Project Presentations
No readings

Final Project Report due 4/29

DONE WITH CLASS!