Empirical Computer Security
ECE/CS 8803 ECS
Frank Li
Welcome!

Who am I?

• New assistant professor in ECE

• Research focus:
  • understand and improve how users tackle emergent security problems
  • understand abuse on online services

• Spent time working at Google, Facebook, and Microsoft Research

• Born & raised in Minnesota (go Vikes!)
  -> BS @ MIT
  -> PhD @ UC Berkeley
Introductions

Who are you?

- Name*
- Program (and advisor)
- Year in program

* Forgive me for mispronunciations or poor memory
Course Goals

Empirical Security: understand how security/privacy concerns manifest in practice

Expected background: familiarity with core computer security and networking

Goals:

• Understand the role of measurement in security research
• Learn to critically evaluate empirical methodologies
• Identify interesting research questions and topics
• Execute a quality research project (think workshop paper)
• Have a fun semester learning about interesting topics
Course Logistics

Class: Mon / Wed 2 - 3:15PM EST on BlueJeans (except optionally for touch points related to project presentations)

Office Hours: Fri 3-4pm EST on BlueJeans (or by appointment)

Course Resources:

• Canvas (all announcements, assignments, grades, surveys)
  • Piazza, accessible within Canvas (discussions/questions)
  • Course Website, linked to within Canvas (official syllabus/schedule)

Email me directly: frankli@gatech.edu
Empirical Computer Security - ECE/CS-8803-ECS

Welcome to Empirical Computer Security!

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. Students will analyze, critique, and discuss these works. Beyond broadening their knowledge of real-world computer security, students will gain a deeper understanding of sound and rigorous measurement methodologies for applying to their own work.

Course Info

Class: Mon / Wed 2-3:15PM EST
Location: Online via Bluejeans (https://bluejeans.com/471548646/5006)

Instructor: Frank Li
Email: frankli@gatech.edu
Office Hours: Fri 2-3pm EST

The course website (including the schedule) is at: https://frankli.ece.gatech.edu/courses/ece8803-ecs/

The official course syllabus is available here.
Course Website

Course website (with official schedule + syllabus): https://frankli.ece.gatech.edu/courses/ece8803-ecs/ (also listed on Canvas)

Empirical Computer Security (ECE/CS 8803 ECS) - Fall 2020

Course Info
Class: Mon / Wed 2-3:15PM
Location: Online via BlueJeans (link in Canvas)
Instructor: Frank Li
Email: frankli@gatech.edu
Office Hours: Fri 3-4PM on BlueJeans (link in Canvas)

Welcome!
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. Students will analyze, critique, and discuss these works. Beyond broadening their knowledge of real-world computer security, students will gain a deeper understanding of sound and rigorous measurement methodologies for applying to their own work.

Please see the course syllabus for course details, including course requirements and grading.

If you're not familiar with reading academic papers, take a look at this reference.

Schedule
Week 1
8/17: First Class - Introduction to Empirical Computer Security
No readings, but will cover topics discussed in the following papers:
- Strategies for Sound Internet Measurements.
- The Base-Rate Fallacy and the Difficulty of Intrusion Detection.
- Conducting Cybersecurity Research Legally and Ethically.

Week 2
8/24: Distributed Denial of Service (Modern)
Reading: Understanding the Mirai Botnet.

8/26: Network Scanning Applications
Reading: Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices.
Course Format

Course driven by discussion of academic papers.

- **Homework**: Paper readings (both classic and recent) + summary writeups
- **Class**: discuss readings critically.
  - Not lectures, nothing like today!
  - I'll help guide, along with 1-2 students per class.
- **Project**: propose, conduct, and present a high-quality semester-long research project.
## Course Requirements

In the syllabus:

<table>
<thead>
<tr>
<th>Assignment</th>
<th>Weight</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation</td>
<td>20%</td>
<td>Attend and engage with class meetings (ask and answer questions, provide comments).</td>
</tr>
<tr>
<td>Discussion Lead</td>
<td>10%</td>
<td>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 students will serve as discussion lead. If a student leads by themselves, they can skip 2 additional summaries during the semester (for a total of 4 potentially skipped summaries).</td>
</tr>
<tr>
<td>Paper Summaries</td>
<td>20%</td>
<td>For each assigned paper, submit a brief paper summary, analysis, and questions. In total, 2 summaries can be skipped during the semester, unless the student leads a discussion themselves, in which case 4 summaries can be skipped during the semester.</td>
</tr>
<tr>
<td>Final Project</td>
<td>50%</td>
<td>Semester-long research project.</td>
</tr>
<tr>
<td>- Project Proposal</td>
<td>10%</td>
<td>Submit a project pre-proposal for feedback on project idea (due 9/21). Write and present a project proposal (due 10/5).</td>
</tr>
<tr>
<td>- Project Presentation</td>
<td>10%</td>
<td>Present a talk and/or demo on your final project (due 11/16).</td>
</tr>
<tr>
<td>- Project Writeup</td>
<td>30%</td>
<td>Submit a research-style paper on your final project (due 12/4).</td>
</tr>
</tbody>
</table>
Course Requirements: Paper Summaries

Thoughtful (but **concise, 2-5 sentences**) reflection on the paper reading.

1. What are the paper's contributions (and what you liked about the paper)?

2. What are questionable parts of the paper and its limitations? (E.g., methodology issues, detail omissions, presentation problems)

3. What was unclear about the work, or what questions do you have?

4. Most readings will have a specific question or two.

**Due 5pm the day before class. Submit to Canvas assignment (but work on it elsewhere)**

2 lowest summary scores dropped (4 drops if you lead a discussion solo)

No papers are mine :)

Course Requirements: Discussion

Discussion Lead: Prepare a ~25 minute presentation discussing the paper. Assume folks have read the paper (but don't remember every detail).

- 1-2 students lead per class (if solo, 2 extra summary skips)
- Use slides (follow my example from next class)
  - Don't need to be terribly pretty, but good communication is important!!
  - Email me your slides the night before class
- Key parts: Background, Problem/Motivation, Relationship to Prior Work, Methodology, Evaluation/Results, Implications, Paper Summary Questions

Rest of the Class (including me): Ask questions and make comments. Participation is 20% of your grade.

- Anyone can ask questions, answer them, and make comments/observations! This is a class-wide discussion.
Course Requirements: Semester Project

Conduct a high-quality empirical security (interpreted loosely) research project.

**Group sizes:** 2-3 people (project scope should match group size)

**Timeline:**

- Sep 21: Email me Project Pre-Proposal (not binding, for feedback)
- Oct 5/7: Project Proposal Presentation *(optionally in-person)*
- Nov 16/18: Final Project Presentation *(optionally in-person)*
- Dec 4: Final Project Report (academic-style paper)

Details will be posted as Canvas assignments

Note: You should be engaging w/ me throughout the semester for feedback/direction
Tips for Success

Ask questions (pop into my OH)

Engage critically with the readings and discussions
• This is an acquired skill. The paper summaries and class discussion are to help you.

Don't procrastinate on the projects!
• Get feedback early, get it often!

Give me feedback!
• I want you to learn and do well. I want this class to be better. I'll ask for anonymous feedback.
To Do's For You

Read the website and syllabus

• Join Canvas + Piazza, look at the course website + syllabus

• Fill out the Pre-Semester Survey

• Ask me ASAP if anything is unclear or missing!

• Look over the class topics and think of the ones you might be interested in leading. I will send a schedule request shortly.

• Read Wednesday's paper (no paper summaries, but please read and think critically about it for our discussion)
So...what is this class?

Empirical computer security???
Security in Practice

The Dream: A perfect secure world of technology

In practice: Whack-a-mole / cat and mouse

What goes wrong? From group discussion:

Software evolves

Security formalism hard

Depends on humans, humans are hard :( 

Information asymmetry

Attackers are clever and react

Competing/misaligned incentives
What are attacker motivations?

From our group discussion:

Personal attacks (partner/friend spying)

Financial motivations (attackers making money, corporate espionage)

Political (including nation-states attacks)

Social (hacktivism)

Reputation (fame, recognition, being LEET, egos)
Traditional vs Empirical Security

Traditional Security:

• *Defensive*: For a given system/protocol, what are **security properties** we'd like, and how do we **provide** those properties (ideally w/ formal guarantees)

• *Offensive*: Given a system/protocol, how do we **violate** desired security properties

Empirical Security:

• Explore how security concerns manifest in practice

• Beyond considering a system/protocol in **isolation/abstract**, investigate how it is used in practice, how attackers actually attack it, and why.

• Insights inform defenses, including those beyond traditional technical ones

• Complementary to traditional security
# Traditional vs Empirical Security

Examples of differences

<table>
<thead>
<tr>
<th>Traditional Security</th>
<th>Empirical Security</th>
</tr>
</thead>
</table>

Traditional vs Empirical Security

Examples of differences

Traditional Security
Transport Layer Security (TLS) for secure communication

Empirical Security
Weak TLS parameters used in practice (ciphersuites, certificates, keys)
Traditional vs Empirical Security

Examples of differences

**Traditional Security**
- Transport Layer Security (TLS) for secure communication
- Two-Factor Authentication (2FA)

**Empirical Security**
- Weak TLS parameters used in practice (ciphersuites, certificates, keys)
- Usability of 2FA. Attacks on SMS 2FA.
Traditional vs Empirical Security

Examples of differences

**Traditional Security**
- Transport Layer Security (TLS) for secure communication
- Two-Factor Authentication (2FA)
- Fight Email Spam w/ Spam Filters

**Empirical Security**
- Weak TLS parameters used in practice (ciphersuites, certificates, keys)
- Usability of 2FA. Attacks on SMS 2FA.
- Fight Email Spam by Preventing Monetization Vector
To Do's For You

Read the website and syllabus

• Join Canvas + Piazza, look at the course website + syllabus

• Fill out the Pre-Semester Survey

• Ask me ASAP if anything is unclear or missing!

• Look over the class topics and think of the ones you might be interested in leading. I will send a schedule request shortly.

• Read Wednesday's paper (no paper summaries, but please read and think critically about it for our discussion)
END NOTE

For those viewing the slides, this is where we ended. Will continue the discussion next class.