UC RIVERSIDE

CS 260 – Privacy Seminar

https://spalab.cs.ucr.edu/teaching/cs260

Emiliano De Cristofaro
https://emilianodc.com

Course Objectives

1. Learn the “basics” of privacy (and privacy technologies)
   - Its connection to security
   - Its societal, ethical, and legal aspects
   - Its relevance to engineering

2. Expose you to advanced research in CS and privacy in particular
   - How to find, read, understand, and explain research papers
   - Hands-on work on research projects

Think as an attacker

- One can't secure a system without being aware of ways to break it...
  - *“You can’t make something secure if you don’t know how to break it.”* (Marc Weber Tobias)
- Schneier’s “Law”:
  - *“Any person can invent a security system so clever that he or she can't imagine a way of breaking it.”*
  - https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html
- **Caveat emptor!**
  - The only reason we will be learning about attack techniques is to build better defenses
  - That is, don’t use this knowledge to perform attacks on real systems!!!

Enrolling

- Need explicit approval from me
- Pre-Requisites: Undergraduate or Graduate Security Class at UCR – not negotiable
- Not accepted past the 2nd week

Ethics & Law

- Malicious hacking/cracking is illegal
- Discussing vulnerabilities/how they are exploited is useful
  - E.g., for education, awareness, …
- Full disclosure policy
  - The information about vulnerability has been already distributed to parties that may provide a solution to the problem (e.g., vendors)
  - See: Responsible vulnerability disclosure process (IETF Internet Draft)
  - Preventing similar mistakes from being repeated

Academic Conduct

- High standards expected in academic conduct:
  - Regulations on how to avoid plagiarism
  - Reference and credit sources appropriately
  - University of California Electronic Communications Policy

- High standards expected in professional conduct:
  - State and federal laws
  - Procedures for research with human subjects
  - Responsible research and disclosure procedures
  - Compliance and risk-based assessments

Welcome!

- **Timetable**
  - 10 lectures, ~~Mon 3:30-4:50pm WCH 142~~ → pre-recorded lectures
  - 10 classes, Wed 3:30-4:50pm WCH 142 → mandatory attendance
- **Grading**
  - 50% Project
  - 25% Class Discussions
  - 25% Quizzes/Class Attendance/Class Participation
- **Office Hours (TBC)**
  - Mon 3:30-4:30 pm, in-person or on Zoom
    Please book a slot: https://calendly.com/emilianodc/cs260

Communication

- Piazza (https://piazza.com/ucr/spring2024/cs260) as the main communication channel
  - Announcements, slides, projects, polls, etc.
  - Discussion and Q&A

  privacydabest

Tentative Schedule

	Monday	Wednesday
Week 1	Intro to Privacy	Overview of the Projects
Week 2	Anonymity	Surveillance
Week 3	Privacy-oriented Crypto	Crypto Case Studies
Week 4	Differential Privacy (DP)	DP Case Studies
Week 5	Privacy in Machine Learning	Privacy and LLMs
Week 6	Tracking and Profiling	Tracking Case Studies
Week 7	Human Factors	Human Factor Case Studies
Week 8	Privacy and Cybersafety	Privacy and Law
Week 9	[Memorial Day]	Privacy by Design
Week 10	Project Presentations	

Lectures **Discussions**

Lectures

- **Pre-recorded** lectures, I will be presenting various topics
  - No midterm/exam but quizzes possibly
  - Expected Q&A discussion on Piazza (part of class participation)

Discussions

- Classes based on topics published in 1-3 research papers
- Each class will have an interactive discussion (no presentations)
  - A group of students will lead the discussion
  - All students have to do that at some point
- Papers need to be read by **everyone**, **before** class
  - Not just by the group leading
  - There will be quizzes
- Discussion: **everyone** should be involved
  - Not just by the group leading it
  - Remind: class participation counts for 25% of the grade

How to lead discussion (1)

- **High-level discussion points:**
  - What are things that you like and dislike about the paper?
  - Why is this a good or bad paper?
  - What assumptions (explicit and implicit) are made, and are they valid?
  - How you might do it differently? Any other suggestions to improve the paper?
  - What principles can you extract from the paper?
  - From the insights described in the paper, how might you apply them to solve other problems?

- **Low-level discussion points:**
  - Frame them as questions for the rest of the class to respond to
  - Aim to engage students in critical and creative thinking

Project

- You can work in groups of 2-3 students (non-negotiable)
  - The amount of expected *individual* work is an invariant
  - Each student will have to submit an *individual* project report

- Details on Wednesday