CS 1699
Privacy in the Electronic Society

William Garrison
bill@cs.pitt.edu
6311 Sennott Square
http://cs.pitt.edu/~bill/1699

01: Course introduction
Course information

Lecture: TH 11:00–12:15, IS 403

Instructor: William Garrison
  • bill@cs.pitt.edu
  • SENSQ 6311 (OH TBA)

TA: Mingda Zhang
  • mzhang@cs.pitt.edu
  • OH TBA

Website: cs.pitt.edu/~bill/1699
  • Not much here, yet
Grade breakdown

Programming assignments: 40%
  • Roughly two week deadlines
  • Programming and writing components
    • Explain your code, interpret results
  • Any language the TA can reasonably run
    • Check with Mingda if you're unsure

Homework assignments: 20%
  • One week deadlines
  • Journaling, analyzing readings, etc.

Exams: 40%
This course is an experiment!

Expecting a course where every detail is planned and tested?
  • This isn’t it—you should shop around during add/drop

Expecting to learn a lot about privacy in an open-ended setting?
  • This is it! We’re all going to learn a lot.

This is an upper-level class, and I’m expecting you to work hard on open-ended projects
  • Writing components to explain your choices
What is this course about?

When engaging with the world around us, we share information *constantly*

- Likes/dislikes, habits, interests, career info, etc.

Sharing this information has *utility!*

- Targeted advertising, crowdsourced data, customized services

... but it also has a *cost!*

- Impersonation, embarrassment, targeted advertising
So what do we do about it?

First, we analyze the trade-offs

- What are the benefits and costs of this data sharing?

Then, we study technical approaches to improve them

- How can I get more benefit for less cost?
- These are PETs (Privacy Enhancing Technologies)
- Some for users, some for developers
A very rough course outline

Section I: Why privacy matters, and cryptography isn’t enough
  • Why is privacy important if I have nothing to hide?
  • How can cryptography help? What are its limits?
  • Side channels and other attacks

Section II: Authorization and data at rest
  • Who do I trust to play gatekeeper?
  • Is my computer doing what I think it is?
  • What environments require specialized policies?
A very rough course outline

Section III: Communication and data in motion
  • What am I **revealing** just by being online?
  • How can I secure my online **chats**?
  • **Anonymity** in unique circumstances

Section IV: Aggregation, surveillance, and big data
  • How does **massive scale** change the privacy equation?
  • How are **smart devices** and IoT affecting privacy?
  • Where are we going from here?
Discussion question

What information did you give up by attending this class today?

What (potentially private) observations about you could be made, and by whom?

What can be deduced about you from this information?