CS 1657
Privacy in the Electronic Society

William Garrison
bill@cs.pitt.edu
6311 Sennott Square
http://cs.pitt.edu/~bill/1657

01: Course introduction
Course information

Lecture: M/W 9:30–10:45, Sennott Square 6110
  • Please be on time!

Instructor: William Garrison (bill)
  • bill@cs.pitt.edu
  • OH appointments on Canvas via Zoom
    • Email if you need to talk this first week

Syllabus: cs.pitt.edu/~bill/1657
  • Alternate: bill-computer.science/1657
  • No homework or projects released, yet
  • Please review course policies
Grade breakdown

Programming/project assignments (3 to 5): 35%
  • Roughly 2–3-week deadlines
  • Programming and writing components
    • Explain your code, interpret results
  • Any language I can reasonably run
    • Check with me if you're unsure

Homework assignments (2 to 4): 20%
  • Plan for 2–4 homeworks
  • One-week deadlines
  • Journaling, analyzing readings, etc.

Exams: 35%
  • Midterm and Final Exams (dates posted soon)

Participation: 10%
This course is different from most upper-level CS courses!

Expecting a course where every step of your assignments is described in detail?
  • 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 and analyze results
What is expected of you?

Read the assigned material

• There is no textbook, but I’ll assign technical blog posts, sections of academic papers, etc.
• Readings are required; I’ll expect you to know the details

Write thoughtfully for homework and projects

• I prefer to read original ideas, not repeating points I made in lecture

Explore the ideas of the course in your own way

• Projects give you lots of freedom... and responsibility
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?
- What makes cloud computing unique?
- 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 scenario

You and a few friends have an in-person conversation about a new smartphone, video game system, tablet, or other computing device. The next day, when browsing social media, you see several ads for this device, its accessories, and other related products.

You double-check that you have turned off microphone access for the social media app on your (current) smartphone. Explain how the platform may have determined that you would be interested in these products.

Next, you double check that microphone access is off for all apps, including system apps. Devise possible explanations for this (stricter) scenario as well.