CS489/698
Privacy, Cryptography, Network and Data Security

Introduction and Administrivia

Spring 2024, Monday/Wednesday 11:30am-12:50pm

Instructors

Diogo Barradas

- dbarrada@uwaterloo.ca
  - cs.uwaterloo.ca/~dbarrada
- Instructor office hours:
  - Mondays 3:00-4:00pm in DC 2631
  - (Starting next week)

TA’s: Sara Sarfaraz, Shreya Arun Naik, Sina Kamali

What is this course? Learning Outcomes

- Evaluate the use of cryptography to protect data assets in storage, transit, and use
- Evaluate the use of network security hardware and software to protect data assets in transit and use
- Compare various network security mechanisms, and articulate their advantages and limitations
- Analyze security and privacy threats to data assets

Other Logistics

- TA office hours posted to LEARN
- Lectures will take place in MC 2035 (are you here?)

Course Website

- The course website is at:
    - https://cs.uwaterloo.ca/~dbarrada/courses/cs489-priv/S24/index.html
    - We will use LEARN for linking the syllabus, calendar, notes, additional materials, assignments
    - It is your responsibility to keep up with the information on both LEARN and the course site
    - We will use Piazza for communication, questions, and discussion

Course Syllabus

- Be familiar with the content in the course syllabus
- It is available on the course website

If you haven't reviewed the syllabus, do so after this lecture.

Plagiarism and Academic Offenses

We take academic offenses very seriously

- Nice explanation of plagiarism online
  - https://uwaterloo.ca/arts/current-undergraduates/student-support/ethical-behavior/
- Read this and understand it
  - Ignorance is no excuse!
  - Questions should be brought to instructor
- Plagiarism applies to both text and code
- You are free (and encouraged) to exchange ideas, but no sharing code or text

Plagiarism Con’t

- Common mistakes
  - Excess collaboration with other students
  - Using solutions from other sources
  - Asking public questions containing (partial) solutions online
  - Posting (partial) solutions to public websites (e.g.,github)
- Possible penalties
  - First offense (for assignments; exams are harsher), 0% for that assignment, -5% on final grade
  - Second offense, more severe penalties, including suspension
  - Penalties for graduate students are more severe
  - More information on course syllabus

Grading Scheme

- 60% three homework assignments (20% each)
  - Due May 29th, July 3rd, and July 24th at 3:00pm
- Midterm 1
  - To take place June 26th
- Midterm 2
  - To take place July 29th

For graduate students: the above scaled to 80% + 20% for a survey paper

- Proposal due June 12th, survey due July 31st

Regular Assignments

- Due 3pm on the day of the deadline
- Late submissions will be accepted up to 48 hours after the deadline (no penalty) and no documentation needed

- Note:
    - No assistance (from TAs or Instructors) is available after the deadline
    - No submissions after the 48 hour window
    - All assignments must be submitted via LEARN (Dropbox)

Midterms

- Midterm 1, in-class June 26th
- Midterm 2, in class July 29th

- Written questions only (no programming)

A note on security…

- In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks
- You are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network without express consent
- You will comply with all applicable laws and policies

Security and Privacy?

What is security?

Confidentiality

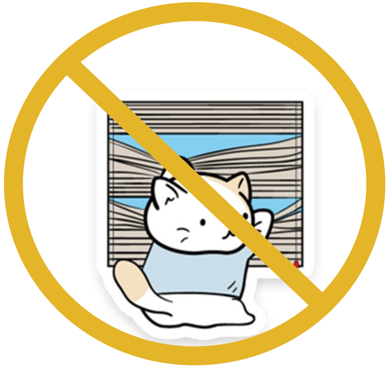
Integrity

Availability

Not all inclusive, but it is a start.

Confidentiality

- Access to systems or data is limited to authorized parties



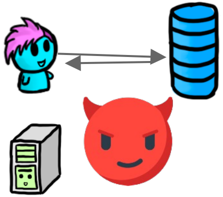
Integrity

- When you receive data, you get the “right” data

Availability

- The system or data is there when you want it

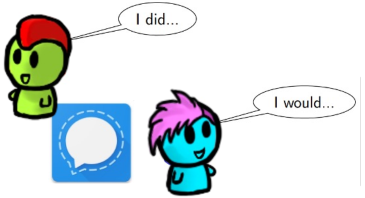
What is privacy?



Technical Privacy

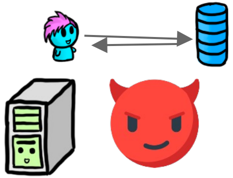
Conceptual Privacy

Legal Privacy

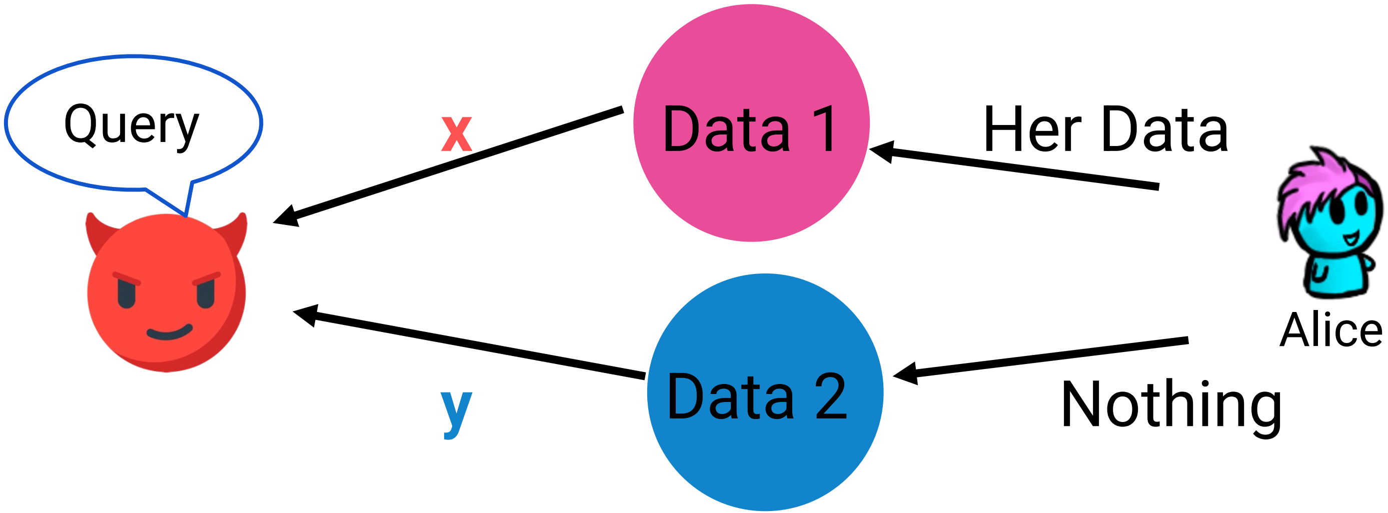


Usable Privacy

Technical Privacy



Technical Privacy

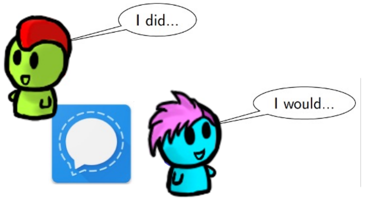


Define, **what** is being protected, from **who**, and under what **conditions** this protection will hold.

Privacy and Risk

- Financial
- Professional
- Societal
- Safety
- Right to privacy

Conceptual Privacy



Usable Privacy

Laws, Legal and Regulated Privacy

Legal
Privacy

…'partners'…

…'third-parties'…

…'affiliates'…

Who

…'use and disclosure'…

can do what

…'right to be forgotten'…

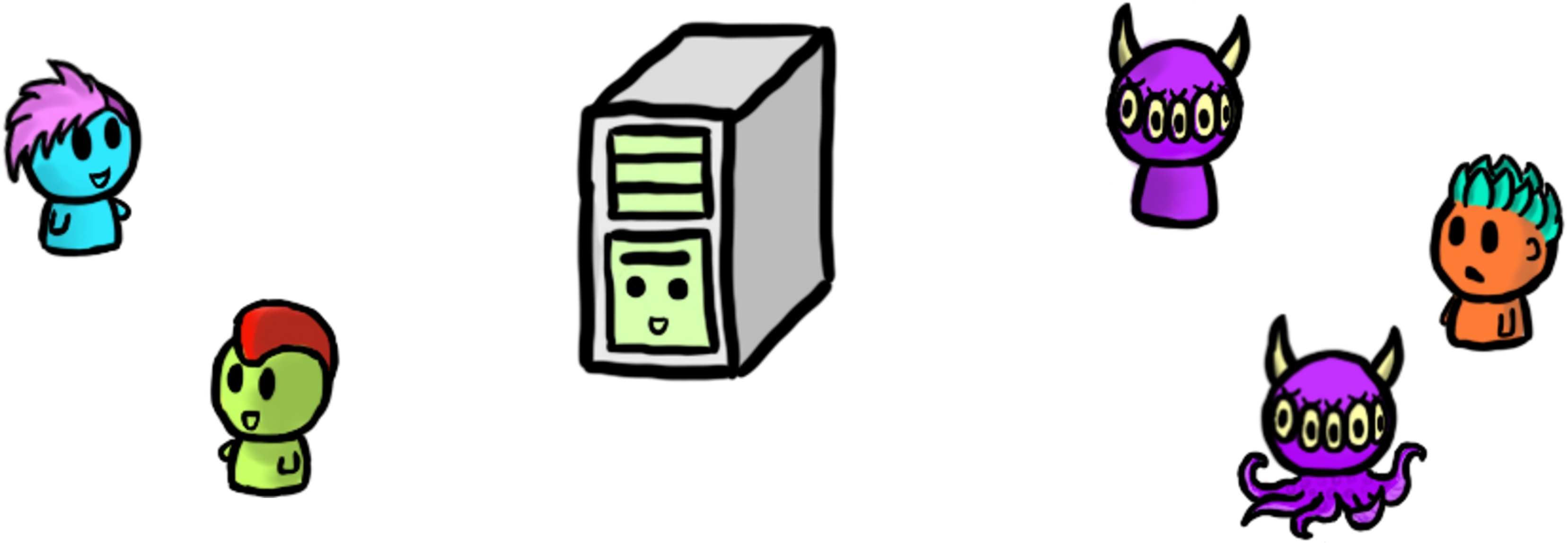
under what conditions

Think-pair-share

“How do we distinguish between security and privacy?”

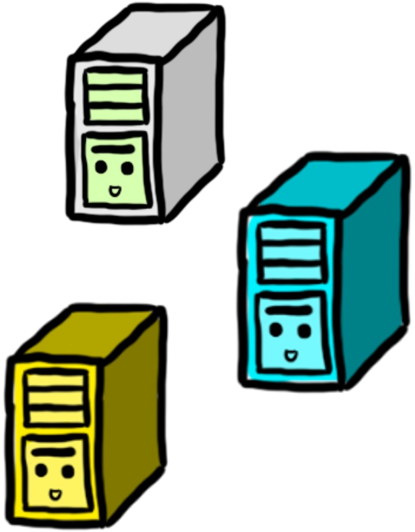
1. Take a minute to think about the prompt
2. Discuss in groups of 2 or 3
3. Nominate one member of the group to share a key point with the class

Framing Security and Privacy Principles

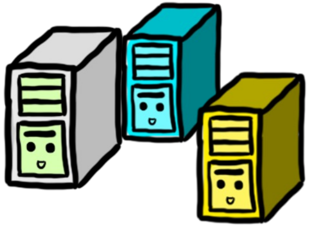


Data Security and Privacy: Assets

- Hardware
- Software
- **Data**



Data and Abstraction



A company wants to analyze data

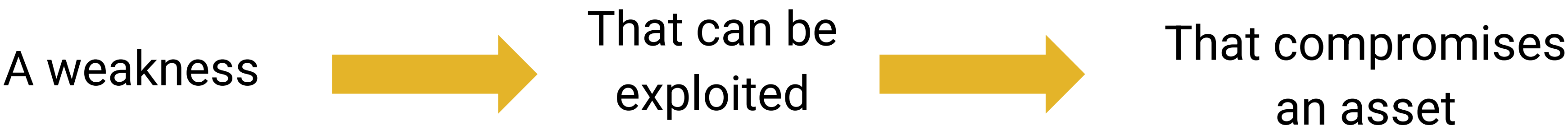
→

But the data has privacy implications for the data subjects

→

Researchers develop technical solutions

Data Security and Privacy: Vulnerabilities



A weakness

That can be exploited

That compromises an asset

Data Security and Privacy: Threats

- Loss or harm
- Interception
- Interruption
- Modification
- Fabrication

These **threats** are part of a **threat model**. Recall the **what** is being protected, from **who**, and under what **conditions**

Data Security and Privacy: Attack

Exploit a vulnerability

Execute a threat

Data Security and Privacy: Control and Defense

“Security” Tape

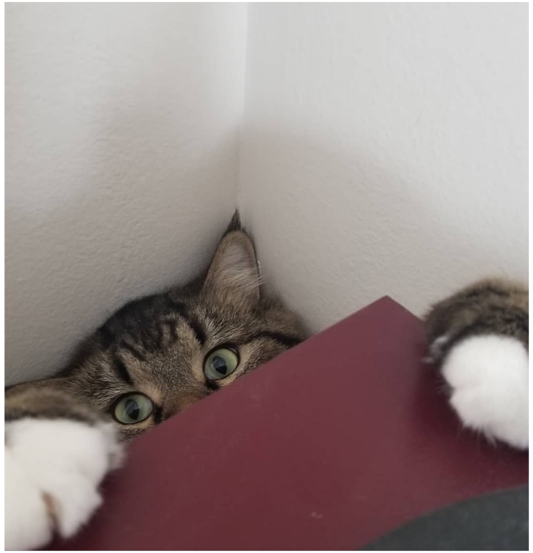
Remove or reduce a vulnerability

Control to prevent attacks and defend against threats

Dealing with Attacks

- Prevent it
- Deter it
- Deflect it
- Detect it
- Recover from it

Risk Management? When is “good enough”?

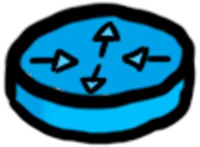


Easiest Target, Principle of Easiest Penetration

Principle of Adequate Protection

Some Defenses for Data - This Course

Cryptography



Network security

Data collection and usage practices

Recap

- This course is about data security and privacy
  - You will learn to evaluate the use of crypto to meet data security and privacy goals
  - You will learn to evaluate network security
- By the end of this course you will be able to present the advantages and disadvantages of the covered data security and privacy techniques
- You will learn how an attacker approaches a system
- You will learn defenses (cryptography, network security, and data protection techniques)

Questions?
Day one mini office hours