CS459/698
Privacy, Cryptography, Network and Data Security

Introduction and Administrivia

Fall 2025, Tuesday/Thursday 8:30-9:50am

Instructors

Urs Hengartner

- urs.hengartner@uwaterloo.ca
  - cs.uwaterloo.ca/~uhengart
- Instructor office hours:
  - Tuesdays 11:30am-12:30pm in DC 3526

TAs: Alim Dhanani, Anais Huang, Zhiao Wei

Other Logistics

- TA office hours posted in each assignment's release
- Lectures will take place in MC 1056 (are you here?)

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

Course Website

- The course website is at:
  - https://crysp.uwaterloo.ca/courses/data-sp/F25/index.html

  - We will use LEARN for making available assignments

  - We will use Piazza for communication, questions, and discussion

- It is your responsibility to keep up with the information on these sites

Course Outline

- Be familiar with the content in the course outline
- It is available from the course website

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

Plagiarism and Academic Offenses

We take academic offenses very seriously

- Nice explanation of plagiarism online
  - https://uwaterloo.ca/math/academic-matters/academic-integrity
- 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 Sep 30, Nov 6, and Nov 27 at 3:00pm
- Midterm
  - To take place Nov 4
- Final Exam
  - To take place TBD during exam season

For graduate students: the above scaled to 80% + 20% for a survey paper
  - Proposal due Oct 21, survey due Dec 2

Assignments

- Usually mix of theory (written) and practical (programming) exercises
- Due at 3pm on the day of the deadline
- Late submissions will be accepted up to 48 hours after the deadline (no penalty); no documentation needed
- Multiple assignments can be submitted late
  - No assistance (from TAs or instructor(s)) is available after the deadline
  - No submissions after the 48 hour window
  - All assignments must be submitted via LEARN (Dropbox)

Exams

- Midterm, in-class Nov 4
- Final Exam, during exam season TBD

- Written questions only (no programming, maybe pseudocode)

Accommodations 101

- For short-term absences before an assignment deadline, students can take advantage of the automatic 48-hour, no-penalty grace period. No further extensions will be granted.
- For short-term absences during an assignment's automatic 48-hour, no-penalty grace period, no further extensions will be granted.
- For absences lasting more than 48 hours, students should contact the instructor(s) as soon as possible and present valid justification.
- If a student misses the midterm, the midterm's weight is **shifted** to the final assessment. Missing the midterm requires valid justification (e.g., short-term absence, VIF forms).

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

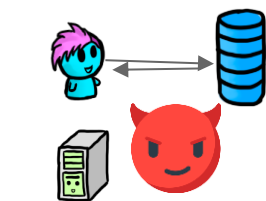- When you receive data, you get the "right" data
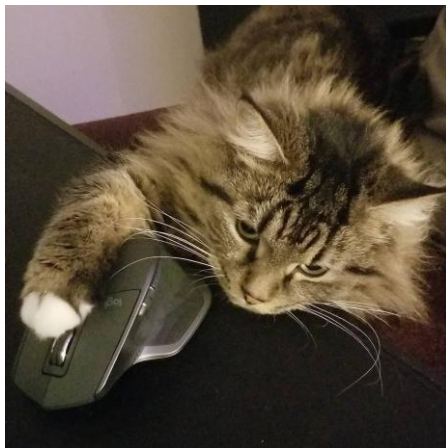
Availability

- The system or data is there when you want it

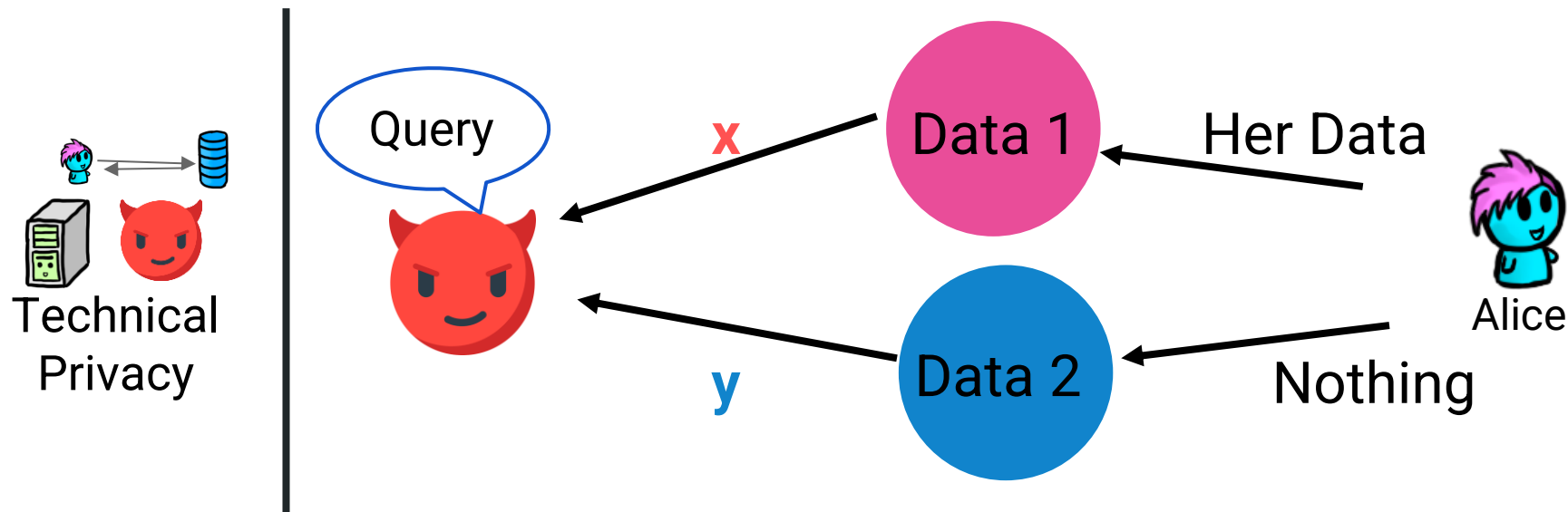# What is privacy?

Technical
Privacy

Conceptual
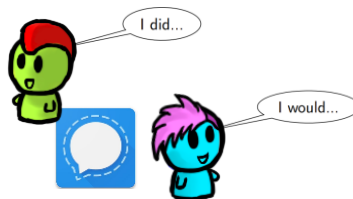Privacy

Legal
Privacy

Usable
Privacy

Technical Privacy

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

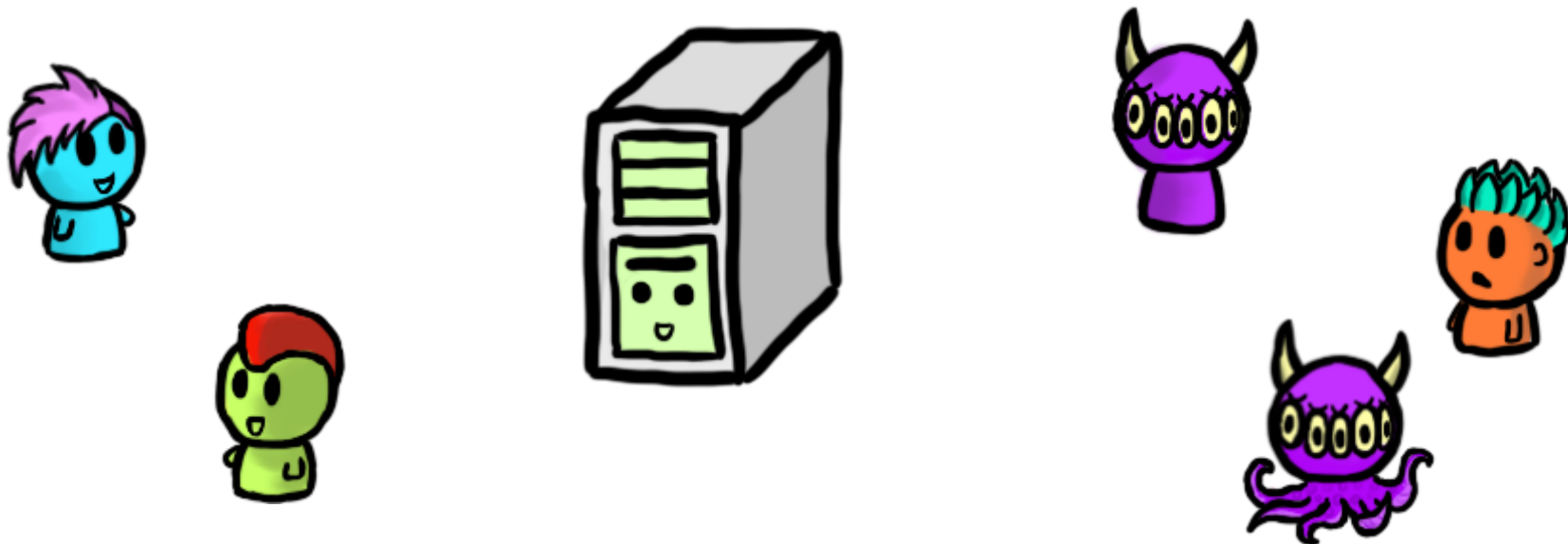…'use and disclosure'…
can do what

…'right to be forgotten'…

under what conditions

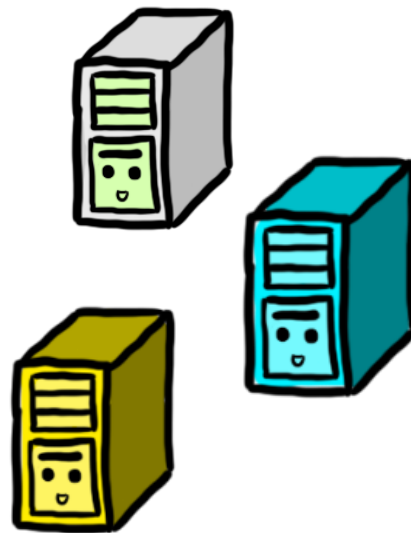# Think-pair-share

"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
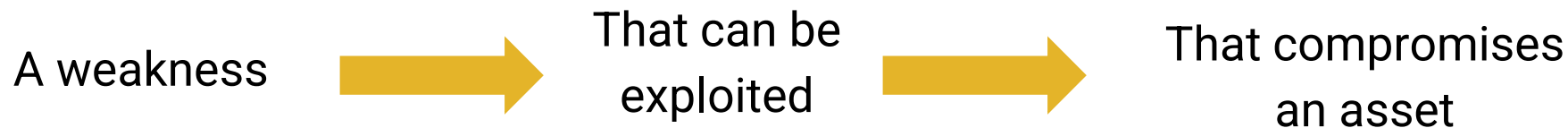- **Data**

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

A loss or harm that might compromise an asset
- 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

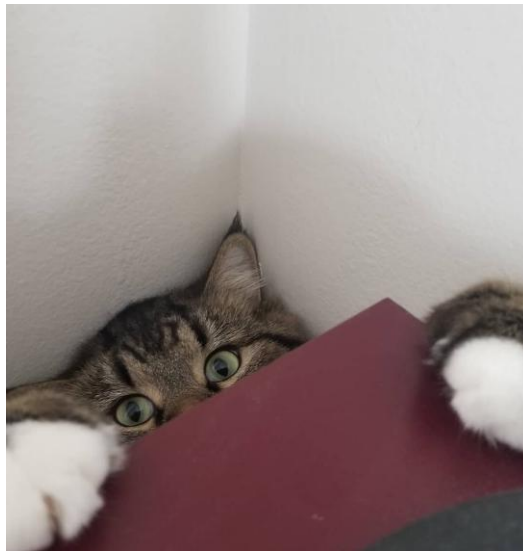
"Security" Tape

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

How secure should we make it?

Weakest Link, Principle of Easiest Penetration

Risk Management - When is "good enough"?

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?