

CS459/659

Privacy, Cryptography, Network and Data Security

Introduction and Administrative

Fall 2026, Tuesday/Thursday 8:30-9:50am

Instructors



Urs Hengartner

- urs.hengartner@uwaterloo.ca
 - cs.uwaterloo.ca/~uhengart
- Instructor office hours:
 - Tuesdays 11:00am-12:00pm in DC 3526 or in or in [course Teams channel](#)

TAs: Alim Dhanani, Lucas Fenaux, Anais Huang

Other Logistics

- TA office hours posted in each assignment's release
- Lectures will take place in MC 2054

What is this course? Learning Outcomes

- Evaluate the use of cryptography to protect data assets in storage, transit, and use
- Analyze security and privacy threats to data assets, including the privacy level of various data release mechanisms, privacy-utility trade-offs, and statistical inference attacks to infer sensitive information
- 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
- Understand data-driven attacks on machine learning systems

Course Website

- The course website is at:
 - <https://crisp.uwaterloo.ca/courses/data-sp/F26/index.html>
 - We will use LEARN for making available and submitting 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

- Possible penalties

- All severe cases of suspected academic misconduct will be reported to the Math Assistant Dean of Students

- Use of AI

- Use of AI tools is permitted, but discouraged
- All use (including careful spelling/grammar correction) must be disclosed
- Disclosure includes the prompt used to generate the output
- You are responsible for the answers you submit
- We will grade typical mistakes by AI very harshly
- See course outline for details

Grading Scheme

- 45% three homework assignments (15% each)
 - Due Oct 8, Nov 12, and Dec 8 at 3:00pm
- Midterm (25%)
 - To take place Oct 29
- Final Exam (30%)
 - To take place TBD during exam season

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

- Proposal due Oct 22, survey due Dec 8

Assignments

- 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)
 - Short-term absences will not extend the late policy

Exams

- Midterm, in-class **Oct 29**
- 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, VOC 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 of the owner**
- You will comply with all applicable laws and policies and uWaterloo policies

Security and Privacy?

What is security?



Confidentiality



Integrity



Availability

Not all inclusive, but it is a start.

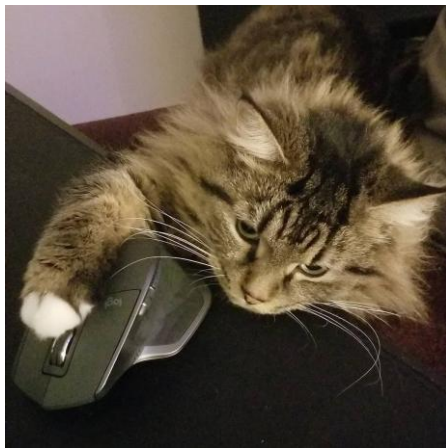
Confidentiality

- Access to systems or data is limited to authorized parties



Integrity

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

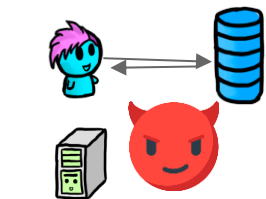


Availability

- The system or data is there when you want it



What is privacy?



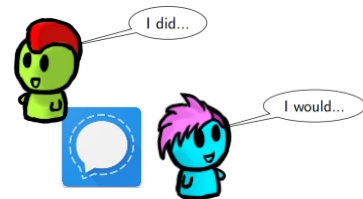
Technical
Privacy



Conceptual
Privacy

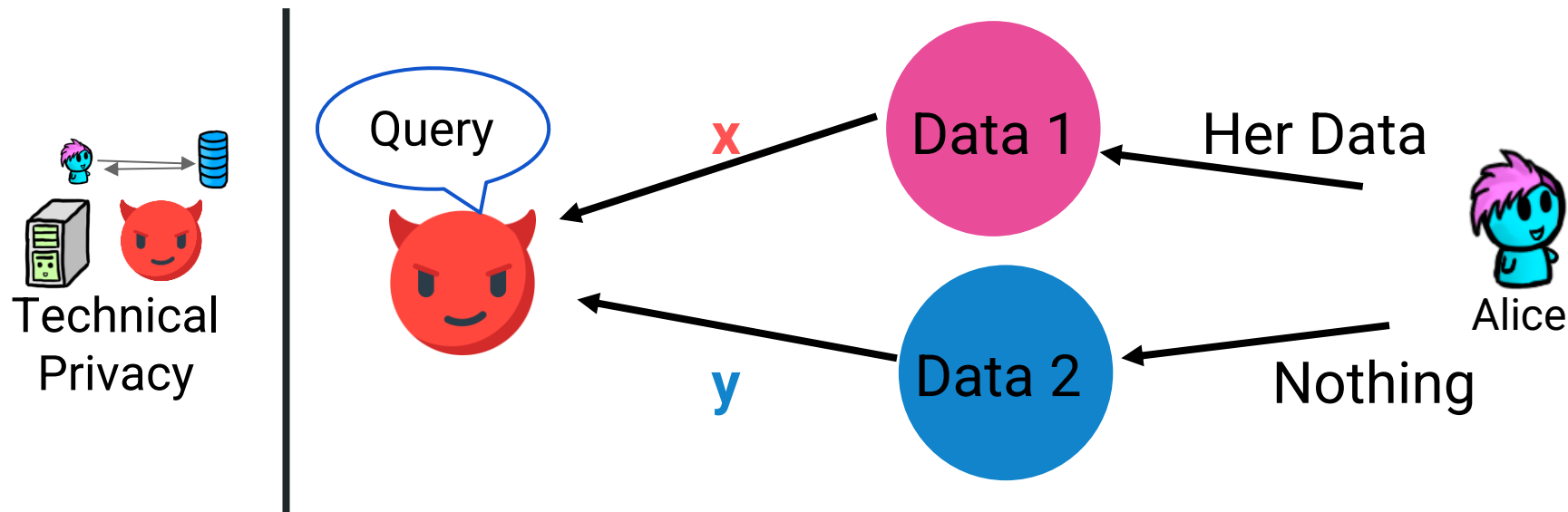


Legal
Privacy



Usable
Privacy

Technical Privacy



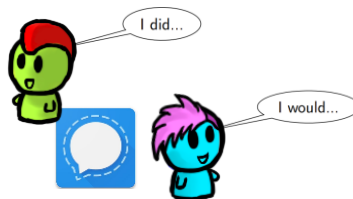
Define, **what** is being protected, from **who**, and under what **conditions** this protection will hold.

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

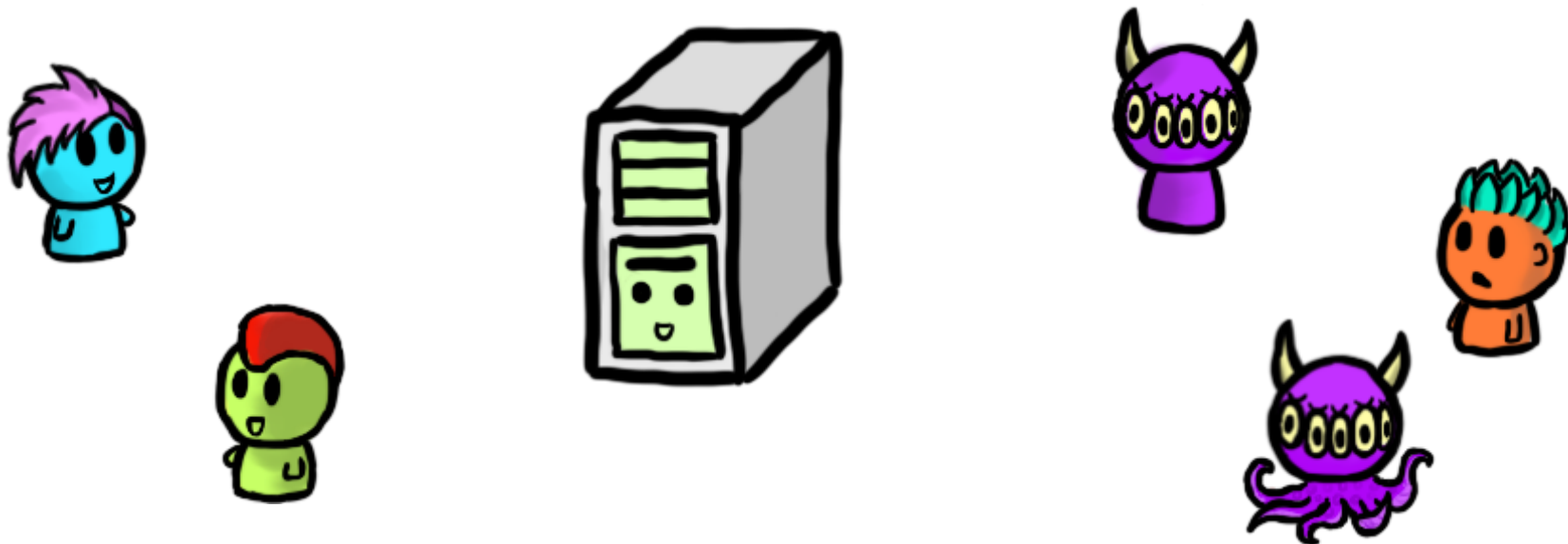
...‘right to be forgotten’...
under what conditions

Think-pair-share

“How do we distinguish between security and privacy?”

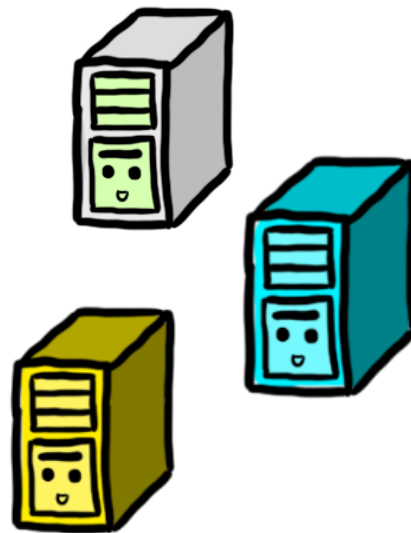
- 1. Take a minute to think about the prompt**
- 2. Discuss in groups of 2 or 3**
- 3. Nominate one member of the group to share a key point with the class**

Framing Security and Privacy Principles



Data Security and Privacy: Assets

- Hardware
- Software
- **Data**



Data and Abstraction



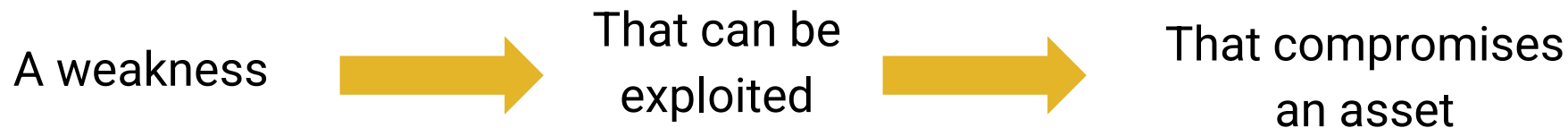
A company
wants to analyze
data



But the data has
privacy implications
for the data subjects

Researchers
develop technical
solutions

Data Security and Privacy: Vulnerabilities



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

Risk Management? When is “good enough”?

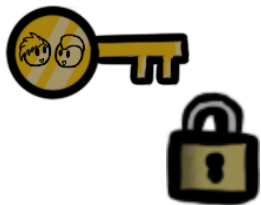


Weakest Link, Principle of Easiest Penetration

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?
