CS489/689
Privacy, Cryptography, Network and Data Security

Winter 2023, Tuesday/Thursday 8:30-9:50am

Instructors

Bailey Kacsmar and Thomas Humphries

- {bkacsmar, thomas.humphries}@uwaterloo.ca
  - cs.uwaterloo.ca/~bkacsmar/ and cs.uwaterloo.ca/~t3humphr/
- Instructor office hours:
  - Tuesdays 10:30-11:30am in DC2130, or by appointment
  - Link for online office hours (on request) will be made available via LEARN
- TA's: Abdulrahman Diaa, Lucas Feneaux, Vecna

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

Logistics

- TA office hours posted to LEARN
- You will need an account in the student.cs environment
  - If you need to reset your passwords at https://www.student.cs.uwaterloo.ca/password/
  - If you don’t have a student.cs account for some reason, ask cscfhelp@uwaterloo.ca for help
- Lectures will occur in MC4058

Course Website

- The course website is at:
  - https://crysp.uwaterloo.ca/courses/data-sp/W23/
- We will use LEARN
  - will be updated regularly, syllabus, calendar, lecture notes, additional materials, assignments, and policies.
  - It is your responsibility to keep up with the information on both LEARN and the course site.
- Questions can be posted to LEARN discussion forum. Do not post solutions.
- Some communication may be sent to your uwaterloo email

Course Syllabus

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

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 (like for previous offerings of this course, maybe written by yourself)
  - 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

- 10% participation in flipped classroom (short exercises/assignments, etc.)
- 60% three homework assignments (20% can be midterm)
  - Due Feb 2nd, Mar 2nd, and Mar 23rd at 4:00pm
- 0 or 20% midterm exam (can replace worst assignment)
- 30% final exam

For graduate students: the above scaled to 80% + 20% for project/survey paper (February 21 topic write up due)

Regular Assignments

- Due 4pm on the day of the deadline
- Late submissions will be accepted up to 72 hours after the deadline (without penalty) and no documentation needed
- Note:
  - No assistance (from TAs or Instructors) is available after the deadline
  - No submissions after the 72 hour window
  - All assignments must be submitted via LEARN

Midterm and Final Assessments

- Midterm, in-class March 9th
  - Weighted 20% if better than worst assignment (replaces that grade)
  - Otherwise, no weight
- Final exam to be scheduled by registrar office
- Written questions only (no programming)

Lectures

- Include interactive portions, including programming
- Please bring a laptop to class
  - If you do not have a laptop/it will not hold a charge, email me after this lecture
- Participation in interactive classroom is 10% of your grade, and includes submitting material.
- Some activities will be portions of the main assignments.
- Research shows including interaction and engaging with the material in class helps with learning and grade outcomes

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 the express consent of the owner
- You will comply with all applicable laws and uWaterloo policies

Security and Privacy?

What is security?

Confidentiality

Integrity

Availability

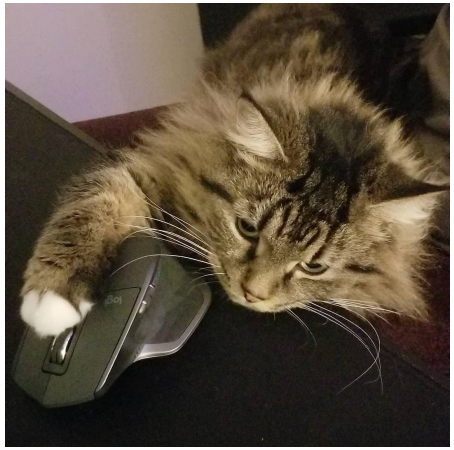
Not all inclusive, but it is a start.

Confidentiality

- Access to systems or data is limited to authorized parties

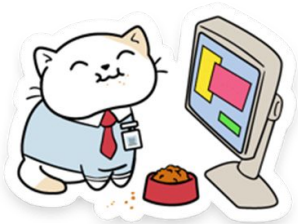
Integrity

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

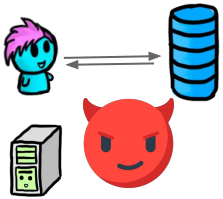


Availability

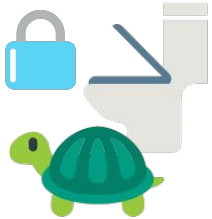
- The system or data is there when you want it



What is privacy?



Technical Privacy

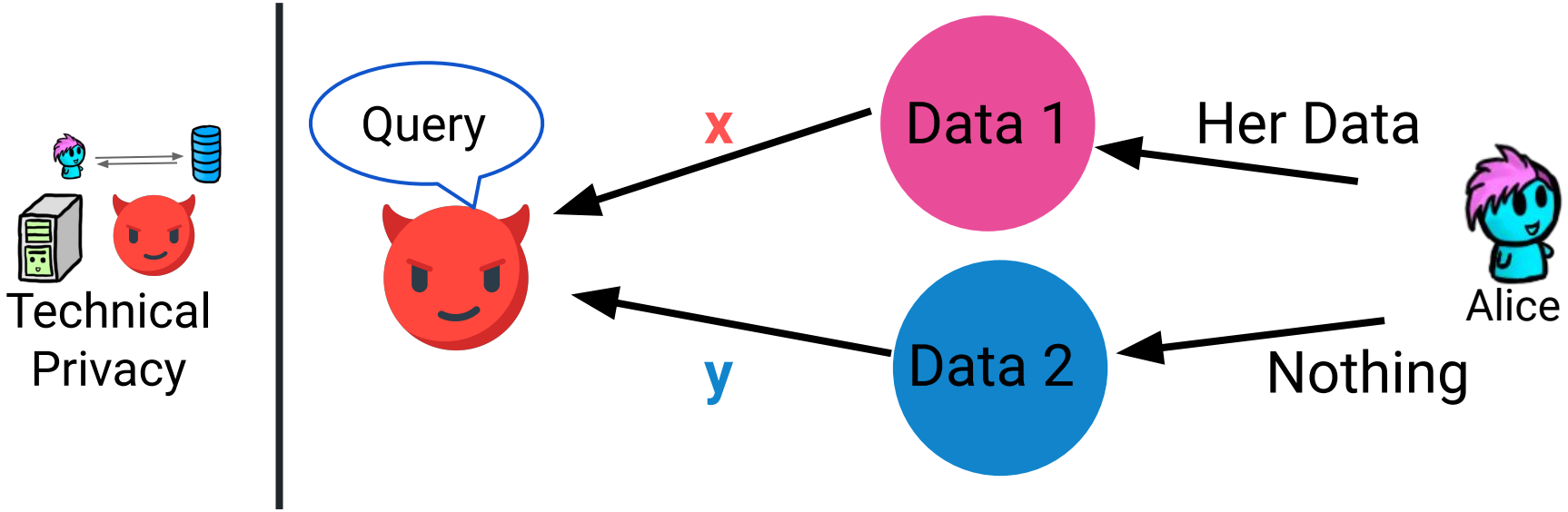


Conceptual Privacy

Legal Privacy

Usable Privacy

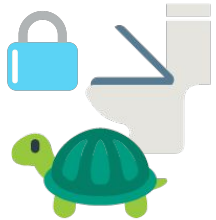
Technical Privacy



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'…

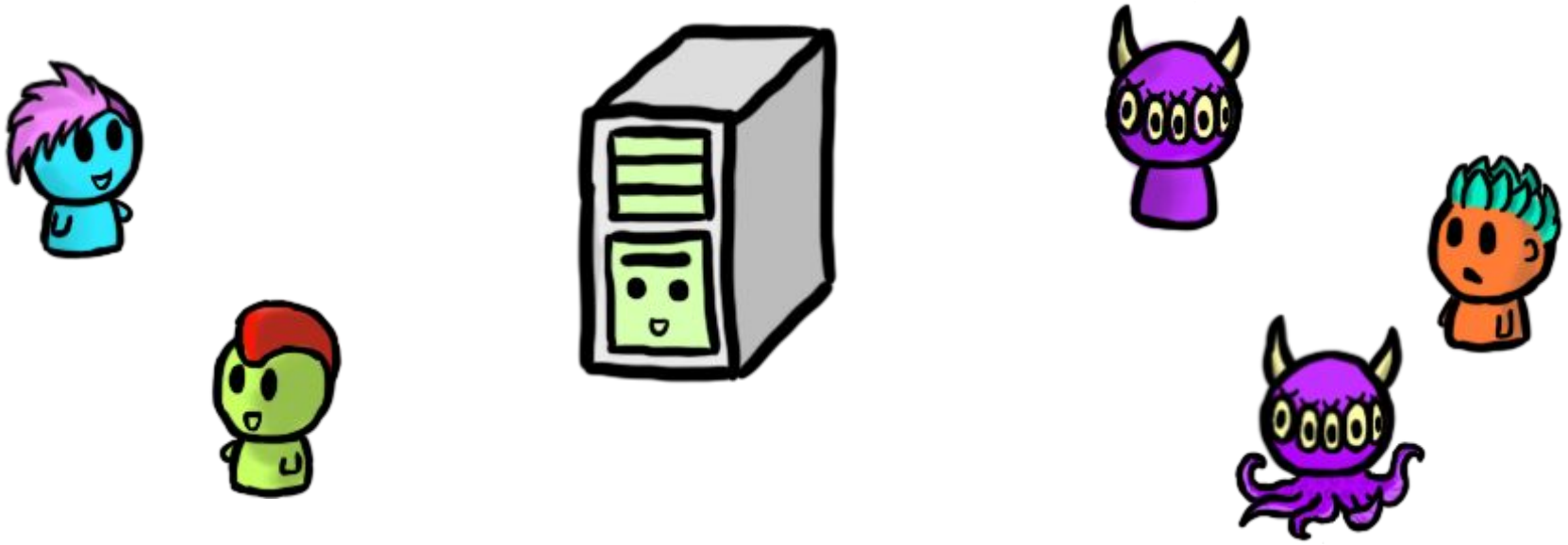
under what conditions

Think-pair-share

How do we distinguish between security and privacy?

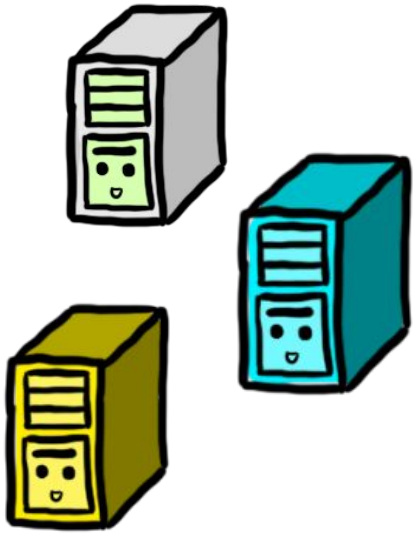
1. Take a minute to think about the prompt
2. Discuss in groups of 2 or 3
3. Nominate one member of the group to share a key point with the class discussion
4. Each student submits to Learn dropbox write up of response and names of members of group.

Framing Security and Privacy Principles

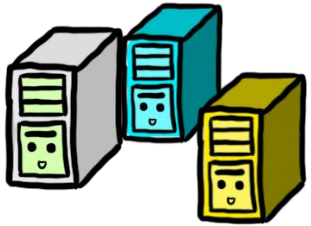


Data Security and Privacy: Assets

- Hardware
- Software
- **Data**



Data and Abstraction

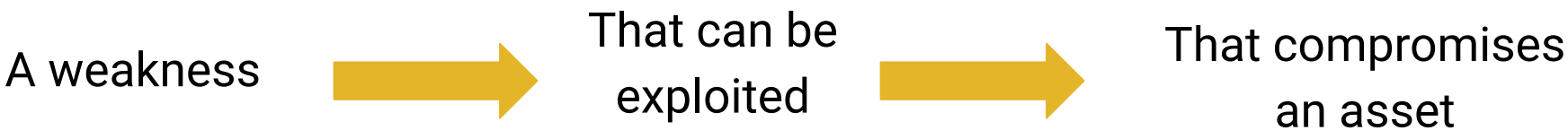


A company wants to analyze data

But the data has privacy implications for the data subjects

Researchers develop technical solutions

Data Security and Privacy: Vulnerabilities



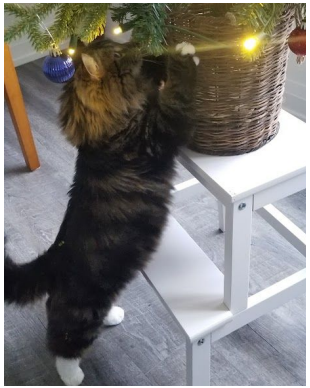
Data Security and Privacy: Threats

- 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**

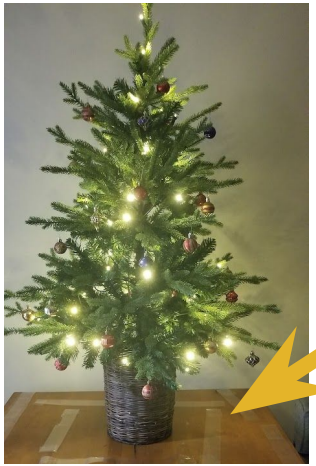
Data Security and Privacy: Attack

Exploit a vulnerability



Execute a threat

Data Security and Privacy: Control and Defense

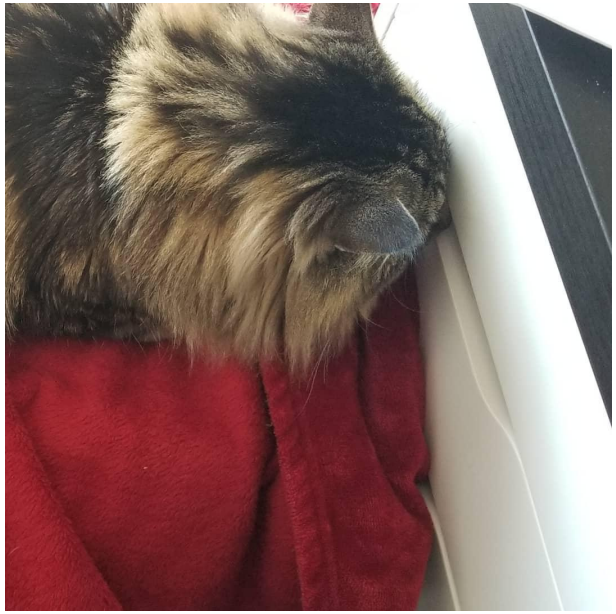


“Security” Tape

Remove or reduce a vulnerability

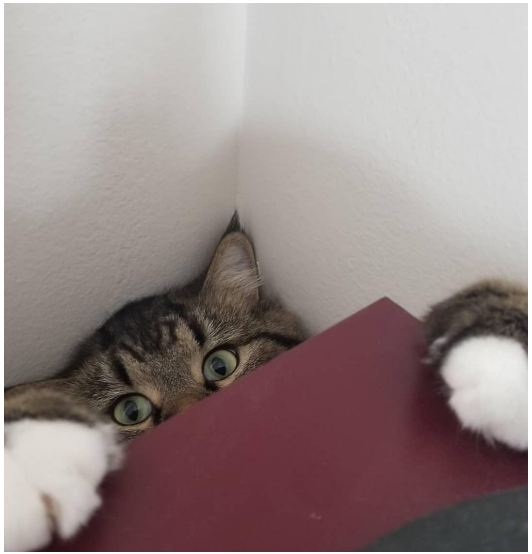
Control to prevent attacks and defend against threats

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

Scenario 1:

What are the abilities of the attacker/adversary

What is available to them

What measures can be taken to thwart them?

Costs?