CS459/698
Privacy, Cryptography, Network and Data Security

Introduction and Administrivia

Fall 2024, Tuesday/Thursday 02:30pm-03:50pm

Instructors

Abdelkarim Kati

- akati@uwaterloo.ca

- Office hours: (Starting next week)
  - Instructor: Wednesdays 11:00am - Noon in DC-2127.
  - TA's: Mondays 10:30 - 11:30am in DC-2127.

TA's: Sina Kamali, Anais Huang, Zahra Manochehri.

What is this course? Learning Outcomes

- Evaluate the use of cryptography to protect data assets in storage, transit, and in 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 Logistics

- LEARN: course info, assignments, grades, etc.
  - Important course announcements will be made on LEARN (Please keep up with the information there).
- Piazza: Q&A, general discussions.
  - Use a private question for questions not of general interest.
  - Use email only as a last resort, and then it must be from your uwaterloo.ca email address for privacy reasons.
- Course website: syllabus, slides, public materials
  - https://crysp.uwaterloo.ca/courses/data-sp/F24/index.html
  - It is your responsibility to keep up with the information on both LEARN and the course site
- Lectures will take place in E2-1736 (are you here?)

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.

Grading Scheme

- 60% three homework assignments (20% each)
  - Due October 3rd , October 31st, and November 28th at 4:00PM.
- Midterm 1
  - To take place October 29th
- Midterm 2
  - To take place December 03rd

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

  - Proposal due November 17th, survey due December 10th

Regular Assignments

- Due 4pm 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 are released and must be submitted via LEARN (Dropbox)

Midterms

- Midterm 1, in-class October 29th
- Midterm 2, in class December 03rd

- Written questions only (no programming)

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

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 information security?

Confidentiality

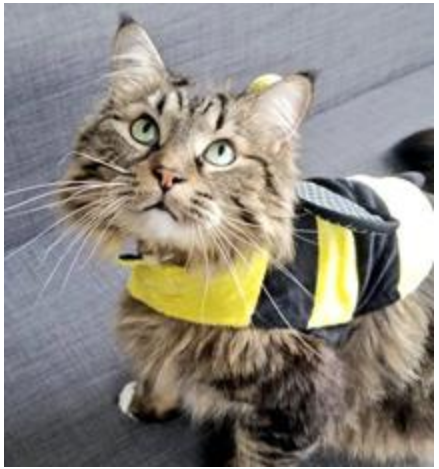
Integrity

Availability

Not all inclusive, but it is a start.

Confidentiality

- Data being stored is safe from unauthorized access & use



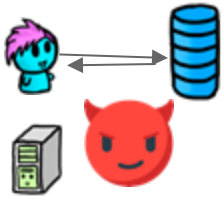
Integrity

- Data is reliable and accurate. i.e., you get the “right” data

Availability

- The system or data is available for use when it is needed

What is privacy?



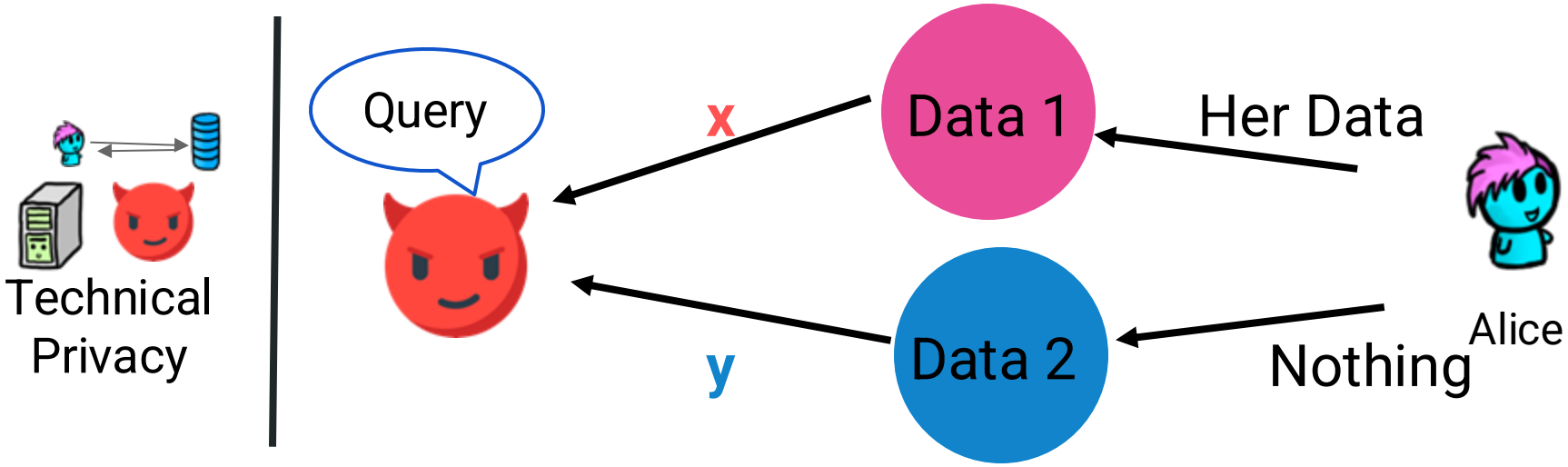
Technical Privacy

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'…

Wh

…'use and disclosure'…

can do

wh

…'right to be forgotten'…

under what conditions

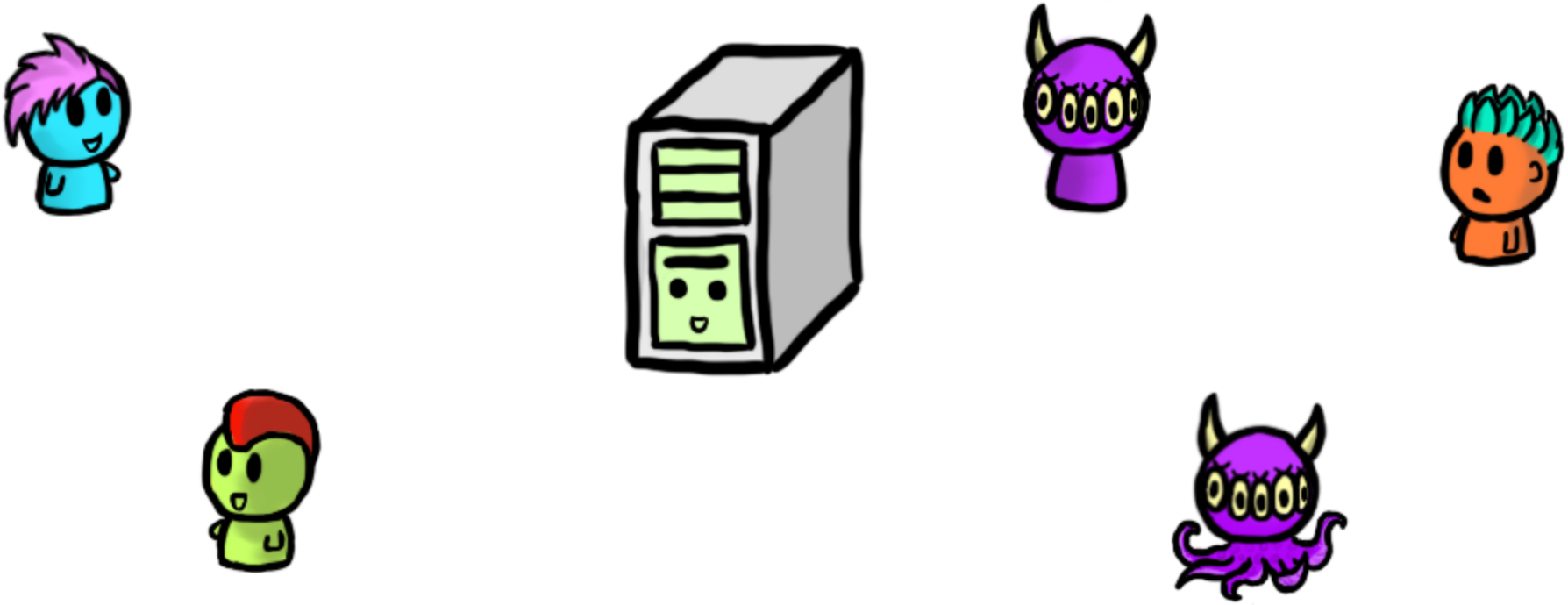
Information Leakage

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



Framing Security and Privacy Principles

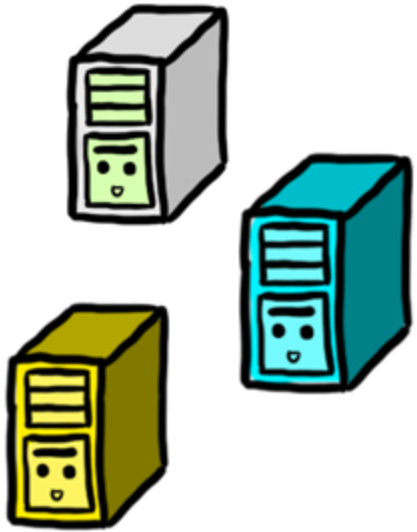
What are the protections?

Who are the adversaries?

Attacks vs defenses

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”?

Principle of Easiest Penetration

“A system is only as strong as its weakest link”

Principle of Adequate Protection

Cost vs Damage

"Don't spend $$$ to protect a system that can only cost $ in damage"

Some Defenses for Data - This Course

At rest

Cryptography

In transit

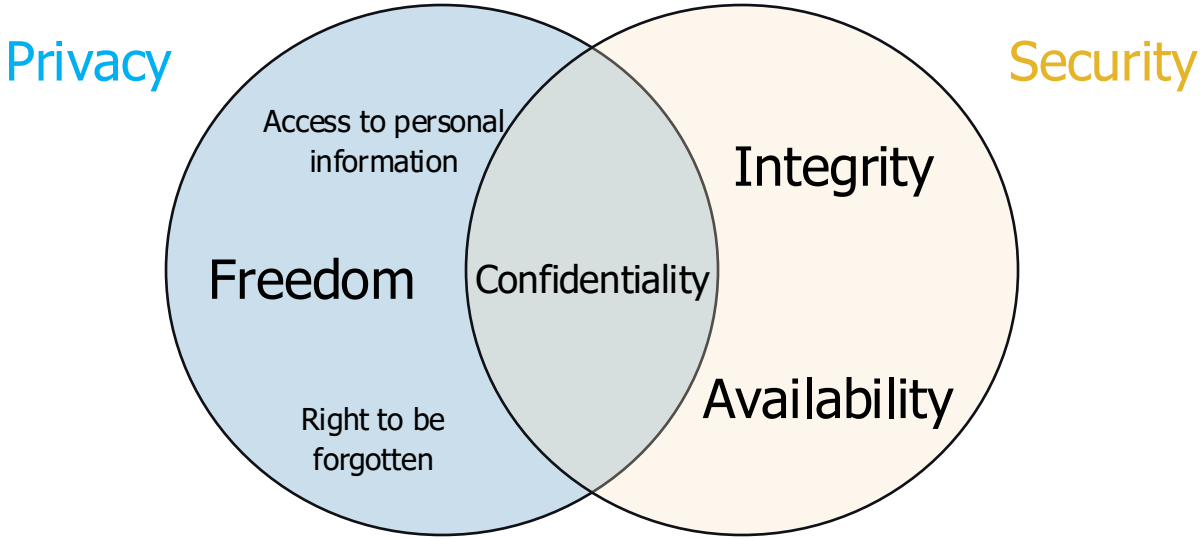
Network security

During computation

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



Recap

- 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