# CS475/577 Data Privacy

## Course Overview

Asst. Prof. Sinem Sav

# Content

1. Introduction to Privacy I
2. Introduction to Privacy II
3. Privacy-Enhancing Technologies (PETs)
4. Crypto-Based Solutions
5. Machine Learning Security and Privacy - I
6. Machine Learning Security and Privacy - II
7. Midterm Presentations
8. Privacy of Healthcare and Genomic Data
9. Privacy in E-cash, Blockchains
10. Privacy in E-cash, Blockchains
11. Privacy in E-voting
12. Location Privacy

# Course logistics

- MOODLE
  - Announcements
  - Submissions
  - Material (slides) + supplementary materials (e.g., papers)

# Contact information

- Instructor: Sinem Sav
  - Please email me in an understandable format -> sinem.sav@cs.bilkent.edu.tr
- TA: TBD soon
  - Please ask your questions to our TA regarding announcements, Moodle problems, deadlines, submissions, quizzes

# Grading

- Final exam 30%
- Quizzes 10% -> 5 quizzes in total
- Midterm presentations 10%
- Final Presentations 25%
- Final Report 25%

# Course Agenda

| Content | Date | Deliverables |
|---|---|---|
| Introduction to Privacy I | January 30, February 1 | |
| Introduction to Privacy II | February 6, February 8 | QUIZ1<br>Group formation |
| Privacy-Enhancing Technologies (PETs) | February 13, February 15 | Project description deadline |
| Crypto-Based Solutions | February 20, February 22 | QUIZ2 |
| Machine Learning Security and Privacy - I | February 27, February 29 | |
| Machine Learning Security and Privacy - II | February 29, March 5 | QUIZ3 |
| Midterm Presentations | March 12, March 14 | Midterm Presentations |
| Privacy of Healthcare and Genomic Data | March 19, March 21 | QUIZ4 |
| Privacy in E-cash, Blockchains | March 26, March 28 | |
| Privacy in E-cash, Blockchains | April 2, April 4 | QUIZ5 |
| No Lecture | April 9, April 11 | |
| Privacy in E-voting | April 16, April 18 | |
| No Lecture | April 23, April 25 | |
| Location Privacy | April 30, May 2 | |
| Final Presentations<br>Final Presentations | May 7, May 9<br>May 14, May 16 | Final reports, Final Presentations |

# Quizzes

- Recaps the previous weeks
- 5-10 minutes, at the end of the lecture
- 1-2 questions

# Projects

- Carried out by 4-5 students (depending on the number of students)
- Tutoring by me and the TA
- If you take this course for credit, be proactive on your choice of project!
- You can propose your own subject and we will discuss its appropriateness; it can be related to your ongoing research -> please email me ASAP
- I will also provide potential project topics (refer to Moodle)
- Ideally, a successful project can *lead to* a publication
- Novelty and effort on the project are important
- Deliverables include final report, midterm presentation, and final presentation

# Project content

- Project can either be (i) research or (ii) implementation based:

# Project content

(i) Research:

- Focus on a particular topic
- Do a literature survey
    - NDSS, ACM CCS, IEEE S&P, Usenix Security, PETS ->relevant conference proceedings are a good start!
- Analyze the existing work and criticize (determine weaknesses and potential improvements)
- Make suggestions, propose your improvements, come up with a systematic solutions including pseudocodes, system figures etc.
- Examples:
    - Privacy in social networks
    - Privacy-enhanced access control, authentication, and identity management
    - Privacy-preserving, secure systems (e.g., distributed machine learning, federated learning)
    - De-anonymization
    - …

# Project content

(ii) Implementation:

- Focus on a particular application or dataset
- Decide on the architecture and system model
- Determine the privacy requirements
- Implement PETs/attacks/defenses for your application or dataset
- Examples:
    - Linkage attacks
    - CryptDB for genomic data
    - Inference/reconstruction attacks on machine learning models
    - Defenses for machine learning systems
    - Applications of PETs
    - Attacks/defenses for healthcare systems/genomic data
    - ….

# Code of conduct

- **Academic Integrity Policy:** All students in this course are expected to adhere to University standards of academic integrity. Cheating, plagiarism, misrepresentation, and other forms of academic dishonesty will not be tolerated. Ignorance will not be accepted as an excuse. If you are not sure whether something you plan to submit would be considered either cheating or plagiarism, it is your responsibility to ask for clarification.
- Responsible disclosure of security vulnerabilities
  - inform us of vulnerabilities
  - do not try to hack/test without permission