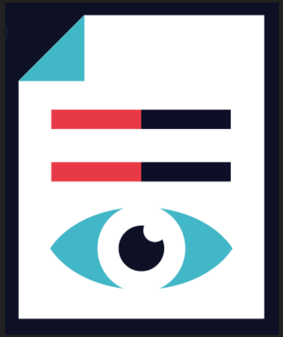
Data Privacy

UMBC CMSC 491/691, Spring 2022



Staff

- Roberto Yus
  - ryus@umbc.edu
  - https://robertoyus.com/
  - 342 ITE, office hours: MoWe 5:30-6:30pm

- TA/Grader
  - Suyash Chirme
  - suyashc1@umbc.edu

Goals

- Understand challenges to individuals’ privacy in data management
- Learn about techniques to perform data minimization
- Learn about different privacy enhancing techniques and algorithms
- Study examples of data privacy protection in contexts such as IoT and ML
- Experience what challenges researchers in the field are focusing on today

Approach

- Advanced course → You'll have to read research papers!
- For each topic:
  - Lecture → Roberto
  - Paper discussion → Led by student group
  - Invited talk → Researcher working in the field

Approach

- Grading Scheme
    - Class participation and presentation (20%)
    - Mini-critiques (25%)
    - Project (55%)
    - No midterm, no final exam

Mini-Critiques

- Individually submit a mini-critique for 7 papers that will be discussed in class.
- A mini-critique is like a peer-review at a conference
    - (i) Summary: Motivation + Problem + Approach + Result,
    - (ii) 3 Strengths
    - (iii) 3 Weaknesses
- 2 groups to lead the discussion of each paper:
    - "bad/good cop" role and argue the paper’s strengths/weakness to the rest of the class.

Group Project

- Team up! Groups of 3-4 people
- Identify an interesting question/problem in handling individuals’ data taking their privacy into account.
- Discuss the topic with the instructor
- Example topics:
    - Incorporation of a Privacy Enhancing Technique to an existing process/domain
    - Analysis of potential privacy leakage in an existing system
    - etc.
- **You need to justify that the topic is interesting, relevant to the course, of suitable difficulty**

Group Project

- At the end of the course, submit a report per project
  - Clearly articulate the concrete contribution of each member of the group at the beginning of the report
- Each group will present their project to the rest of the class in their allotted final presentation slot
- Your grade will be assigned based on the actual project and your presentation
  - You’ll grade each others' project presentations

Expectations

- Do the mini-critiques
  - On your own!
- Hand them in on time
  - No late submission allowed
- Participate in the class!
  - Ask questions, share thoughts, engage in discussions
- Don't be afraid to seek help
- Take pride in your work

Expectations (COVID-19)

- You should be fully masked during any in-person interactions, including lectures, and office hours.
    - You must wear a mask appropriately (i.e., over nose and mouth) and you must do this for every class session and for the entire duration of each class session.
- If you are sick, **stay home**.
    - If you are sick for two or more lectures, get in touch and we will work out how to accommodate any changes to the schedule.
- Participation is a critical element of this class, **but you will never be penalized for prioritizing your and others' health**

Infrastructure

- Schedule, notes
  - **Course website (www.robertoyus.com – inside of Teaching)**
- Discussion
  - **Discord**
- Grades, mini-critique and project report submission
  - **Blackboard**

Academic Integrity

All members of the UMBC community are expected to make a commitment to academic honesty in their own actions and with others. Academic misconduct could result in disciplinary action that may include suspension or dismissal. Here are examples of academic misconduct that are not tolerated at UMBC.

- **Cheating**: Knowingly using or attempting to use unauthorized material, information, or study aids in any academic exercise
- **Fabrication**: Intentional and unauthorized falsification or invention of any information or citation in an academic exercise
- **Facilitating Academic Dishonesty**: Intentionally or knowingly helping or attempting to help another commit an act of academic dishonesty
- **Plagiarism**: Knowingly representing the words or ideas of another as one's own in any academic exercise, including works of art and computer-generated information/images