ECE598NB
Privacy Enhancing Technologies

Spring 2006

Outline

- Privacy Overview
- Course Topics
- Course Structure

Privacy

- Define privacy

Privacy History

- Privacy has always existed
- Cities / large populations have made privacy easier
  - Easier to “get lost in the crowd”
- Computers make privacy harder
  - More information generated
  - More communications
  - Better methods to sift through information
- Are we trying to go against the tide?

Trade-offs

- Security and privacy are trade-offs
  - Can achieve perfect online privacy by staying offline
- Privacy enhancing technologies *change* the trade-offs

Course Topics

- First (roughly) half: anonymity
  - Anonymity underlies other privacy technologies
  - Classic designs
  - Recent implementations
  - P2P anonymity
  - Common attacks
  - Analysis techniques
  - Censorship resistance

Course Topics

- Digital Cash
- Anonymous Credentials
- Private Trust Negotiation
- Electronic Voting
- Location Privacy
- RFID Privacy
- Database Privacy
- Private Information Retrieval

Course Topics

- Private Computation / Aggregation
- Privacy in IDS
- Economics of Privacy

Course Structure

Your Responsibilities

Reading Papers

- Must read assigned papers before class
- Must email summaries of papers
- One paragraph summary of paper content
- Two or three:
  - Criticisms
  - Praises
  - Confusing points
- Email to nikita@uiuc.edu
- Do this for the two papers next lecture

Presenting Papers

- Present paper before class
  - Explain paper content (~15 minutes), lead discussion (~20 minutes)
  - Two or three times per person
  - Make sure to include discussion points, questions, points of disagreement
  - Meet with me at least one day before class to discuss paper, slides
    - Be aware of travel schedule (will be posted)

Discussion Summary

- Experiment: Course Blog
  - (not up yet)
- Summarize paper discussion in class
  - Two or three times per person
- Also encouraged:
  - Further on-blog discussion
  - Additional posts
  - External participation

Projects

- (only if taking course for 4 credits)
- Original research project
  - Anything related to privacy
  - Project suggestions will be posted
- Groups of 2-3
- Deliverables
  - Presentation for the class (~20 minutes)
  - Conference-quality report (~10-14 pages)
- Can be combined with Prof. Gunter’s class
  - Jointly advised and graded

For next class

- Read the two papers
  - “Privacy Enhancing Technologies for the Internet” and “… Part II: Five Years Later”
- Email me summaries
- Sign up to present, scribe
- http://nikita.ca/work/ece598nb