

Data Security & Privacy

CSE 6392 – 010

Instructor: Nan Zhang

About Me

Office: 306 Nedderman Hall

Office Hours: TR 3:20pm – 4:20pm

Email: *nzhang@cse.uta.edu*

Today's Lecture

- Course Information
- Course Policies

Security and Privacy

- Security
- Privacy
 - Not about hiding everything
 - Control what stays inside and what leaks to the outside

Data Security & Privacy

- Data Security Breaches & Privacy Violations (2005 – now)
 - Bank of America, J. P. Morgan, LexisNexis, Fidelity, Ameriprise
 - IRS, Air Force, State of RI
 - Boeing, Ford, Honeywell, GM
 - FedEx, UPS
 - Universities: Stanford, CMU, Cornell, Duke, Purdue, UCSD, Utah, Iowa, Georgia, CUNY, Colorado, Ohio State, Hawaii, etc
 - AA, NWA, etc
 - AOL
 - Blue Cross and Blue Shield, several hospitals

References: <http://www.privacyrights.org>, http://www.wrf.com/publication_newsletters.cfm?publication_ID=12248

Benefits of Data Applications

- Convenience
- Reduced Cost and Prices
 - Focused Advertisement: Amazon – Personalized Recommendation List
 - MBNA – Credit Card with Targeted Customers
- Homeland Security

Major Problem

- Conflicted Objectives
 - Provide efficient access to (or analysis of) large amounts of data
 - Restrict data access/analysis for security and privacy reasons
- Enforce security & protect privacy without impeding data applications.

Possible Solutions

- Privacy Laws and Policies
 - Code of Fair Information Practices
 - HIPAA
 - Privacy Directive
 - California Database Breach Notification Act
- Access Control 4417749 == Ms. Thelma Arnold, 62, GA
- Encryption/Decryption
- Perturbation

What's in it for YOU?

- Next Frontier?
 - Heightened level of privacy concerns
 - Online Data Collection
 - Information Availability
 - Advanced Data Analytical Techniques
 - Fundamental Problem with Great Impact
- Synergy

Today's Lecture

- Course Information
- **Course Policies**

Covered Topics

- Basic Tools
 - Applied Cryptography & Secure Multiparty Computation
 - Information Theory, Game Theory
- S&P in Databases
 - Multi-level Databases
 - Statistical Databases
 - Data Sharing and Integration
 - Anonymity
- S&P in Data Mining
 - Inference Control in OLAP
 - Privacy-Preserving Data Mining

Project

- Topic
 - You can name it. I can help.
 - All kinds of topics related to data security/privacy
 - Paper review topic: review a data-security related paper published in the last three years (2003-2006) on:
 - SIGMOD, VLDB, PODS, ICDE, KDD, TKDE, TODS, VLDBJ, S&P, CCS, CRYPTO
 - Please remember to reserve the paper.
- Three Components
 - Proposal
 - Presentation
 - Report

Proposal

- 0.8: What you will definitely accomplish
- 1.0: What you expect to accomplish
- 1.2: What you will, or hope to, accomplish if you have time.

Presentation

- Tell us what you learn from the project
 - 30 minutes
 - 10 slides
 - Not necessarily comprehensive, understanding is the key.

Report

- At least 6 pages long
- Comprehensive
- For paper review topic:
 - Summarization of results
 - Contribution to the literature
 - Critical evaluation: any mistake? Assumptions reasonable?
 - Suggestions for future extensions/improvements

Grading

- Homework and Class Participation: 25%
- Presentation: 35%
- Project: 40%

Questions