Privacy in Computing

Jun Li

lijun@cs.uoregon.edu

Learning Objectives

- Concepts of privacy
- Privacy principles and policies

Introduction

- Privacy exists before there was computers or even written language
  - But computers provide functions affecting privacy in new ways
- Privacy is a human right, but depends on the situation and affected parties
  - Cultural, historical, personal, contextual
- We focus on privacy's implications on computing and information technology
  - **Information privacy**

Information Privacy

Three aspects:

- Sensitive data
- Affected parties
- Controlled disclosure

Sensitive Data

Examples:

- Identity
- Finance info
- Legal matters
- Medical info
- Voting, opinions
- Preferences
- biometrics
- Diaries
- Privileged communications
- Performance
- Activities
- etc.

Overall, the sensitivity is at the discretion of the subject.

Controlled Disclosure

- Privacy is the right to control who knows certain aspects about you
- Key point is *you* decide
- No complete control, however
  - Once you give your private information to someone else, your control is diminished

Affected Subject

- Individuals, groups, companies, organizations, and governments all have data they consider sensitive
- Privacy has a cost
  - It conflicts with availability

Computer-Related Privacy Problems

Rezgui et al. list eight dimensions of privacy (specifically the web)

- Information collection (explicit consent)
- Information usage (specified purpose)
- Information retention (time window)
- Information disclosure (only to the authorized)
- Information security
- Access control
- Monitoring (logs)
- Policy changes (cannot become less restrictive)

Privacy Principles and Policies

- Fair information policies
- US Privacy Laws
- Controls on US government web sites
- Controls on commercial web sites
- Non-US privacy principles
- Anonymity, multiple identities
- Government and privacy
- Identity theft

Fair Information Policies

The Willis Ware committee report, 1973, Rand

- Collection limitation
  - Lawful and fair
- Data quality
  - Relevant, accurate, complete, up-to-date
- Purpose specification
  - Destroyed if no longer necessary
- Use limitation
  - Unless authorized
- Security safeguards
- Openness
  - Can query the collection, storage, and use of data
- Individual participation
  - Data subject can challenge
- Accountability
  - Data controller accountable

Four Ways to Protect Stored Data

- Reduce exposure
  - Limit the amount, asking for only what is necessary, random samples instead of complete surveys
- Reduce data sensitivity
  - Add subtle errors?
- Anonymize the data
- Encrypt the data

U.S. Privacy Laws

- 1974 Privacy Act: US government data
- Fair Credit Reporting Act: Consumer credit
- Health Insurance Portability and Accountability Act (HIPPA): healthcare info
- Gramm-Leach-Bliley Act (GLBA): finance
- Children's Online Privacy Protection Act (COPPA): children's web access
- Federal Educational Rights and Privacy Act: student records
- E-Government Act 2002: privacy policies of federal agency web sites

Identity Protection

- Anonymity
- Multiple identities – linked or not
- Pseudonymity