Privacy in Wireless Sensor Networks

Marc Langheinrich

ETH Zurich, Switzerland

http://www.inf.ethz.ch/~langhein/

RESEARCH GROUP FOR

Distributed Systems

ETH

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

What's Up?

- **Privacy Primer**
  - Privacy issues
  - Fair information practices

- **Privacy in Wireless Sensor Networks**
  - Anonymous identification
  - Privacy threats

- **Privacy Tools**
  - Anonymity & transparency

Privacy Issues

- **Secure Communications**
  - Gets my information safely across
- **Secure Storage**
  - Locks my information safely away
- **Usage?**   *Transparency*
  - What do they do with my data
- **Recipients?**
  - Who gets my data?
- **Retention?**
  - How long do they keep my data?

Fair Information Practices

- US Dept. HEW '73, OECD '81, EU '95, …
- Basis for Most Privacy Legislature Today
  - Notice and awareness
  - Choice and consent
  - Access and participation
  - Integrity and security
  - Enforcement and redress
  - Limitation of collection and use

Privacy in Sensor Networks?

- **Military Applications**
  - Detection of enemy tanks, soldiers
  - Protecting landmines
- **Environmental Applications**
  - Detecting & monitoring forest fires, oil spills
  - Monitoring animals in the wild
- **Building Automation**
  - Regulating energy consumption
  - Finding people in an emergency
- **Health Care? Floating Cars? CCTV Network?**

Privacy Boundaries

- When is Our Privacy Being Violated?
- Border Crossings of Personal Data:
  - Natural (physical limitations)
  - Social (group confidentiality)
  - Spatial / Temporal (adolescence vs. midlife)
  - Transitory (fleeting moments)
- Example: Smart Hotel
  - Detects human presence (heat, motion)
  - Services: call diversion, doctor on call, ...

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Anonymous Identification

- **Identity Through Presence**
  - Someone in your office late at night

- **Identity Through Routine, Traits**
  - Someone who always uses the elevator
  - Someone who uses a cane, wears knitwear

- **Identity Through Co-location**
  - Someone who carries your laptop
  - Someone who drives your car

Anonymity Tools

- **Location-Mix-Network (Beresford et al)**
  - Mix zones (unobserved) vs. application zones (using location service)
  - Middleware assigns new pseudonyms when user passes through Mix zones
- **Hierarchical k-Anonymity (Gruteser et al)**
  - Hierarchical areas with controller nodes
  - If k or more subjects, return exact location
  - If less then k subjects, aggregate location

Transparency Tools

- **P3P: Platform for Privacy Preferences Project**
  - Privacy policies in machine-readable format
  - Who? Why? What? How long?
  - Allows automated decisions (based on user prefs)
  - W3C recommendation since 2001
  - Partial implementations in IE6, Mozilla
- **Transparent Sensor-Networks?**
  - Sensors announce their presence & purpose
  - Querying sensors requires usage policy
  - Personal device keeps track of collected data

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Summary

- **Privacy Not Just Secrecy**
  - Basis for personal autonomy, democracy
  - Comprehensive privacy needs more than security

- **Sensor Networks & People**
  - Even w/o identification privacy violations possible

- **Who Should Worry About it?**
  - Legislators?
  - Community?
 - Programmers?

Technology Affects Privacy

- **What Kind Of Infrastructure?**
  - Code is Law (Lessig)
  - Example: Spam-Email
- **What Kind Of Privacy?**
  - How manipulative do we want to get?
  - Spotty data against personal testimony
- **What Kind Of Security?**
  - 9-11 2001, 3-11 2004 attacks
  - But also: speeding, smoking, fatty diets, …

Interesting Reads

- David Brin: The Transparent Society. Perseus Publishing, 1999

- Lawrence Lessig: Code and Other Laws of Cyberspace. Basic Books, 2000

- Simson Garfinkel: Database Nation – The Death of Privacy in the 21st Century. O'Reilly, 2001
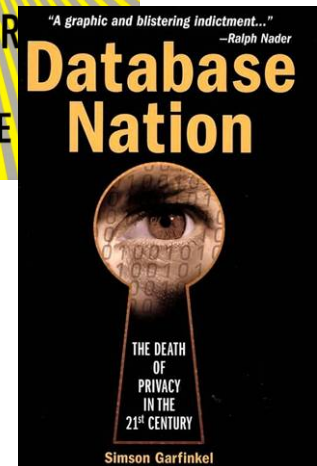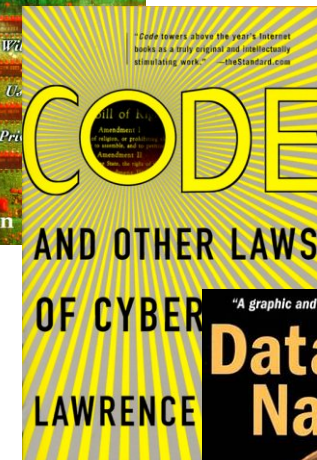
More Books

- **Security for Ubiquitous Computing,** by Frank Stajano

- **Privacy & Human Rights 2003,** EPIC

- **Technology and Privacy: The New Landscape,** by Philip E. Agre and Marc Rotenberg

- **Information Privacy Law** by Daniel Solove and Marc Rotenberg

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich