Personal Privacy in Ubiquitous Computing

Marc Langheinrich
Institute for Pervasive Computing
ETH Zurich, Switzerland

Approaches to Ubicomp Privacy
Disappearing Computer Troubadour Project (10/02 - 05/03)

- Promote Absence of Protection as User Empowerment
  - „It’s maybe about letting them find their own ways of cheating”

- Make it Someone Elses Problem
  - „For [my colleague] it is more appropriate to think about [security and privacy] issues. It’s not really the case in my case”

- Insist that “Good Security” will Fix It
  - „All you need is really good firewalls”

- Conclude it is Incompatible with Ubiquitous Computing
  - „I think you can’t think of privacy... it’s impossible, because if I do it, I have troubles with finding [a] Ubicomp future”

Today’s Topics

- **Background: Ubicomp Privacy**
  - What is privacy?
  - How does ubiquitous computing affect it?

- **Privacy Infrastructure: PawS**
  - Privacy beacons, privacy proxies, and privacy-aware databases

- **Real-World Example: RFID**
  - PawS-RFID: privacy protocols for transparency
  - Shamir Tags: protection against unauthorized readouts

---

The Vision of Ubiquitous Computing

“...the most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.”

*Mark Weiser (1952 – 1999), Xerox PARC*

- **Basic Motivation of Ubiquitous Computing**
  - The computer as a *tool* for the everyday
  - Integrating computers with *intuitive* user interfaces
  - *Things* are *aware of* each other and the *environment*
So what does this mean for **personal privacy**?

What is **privacy** anyway?
What is Privacy?

- „The right to be let alone.“
  - Louis Brandeis, 1890 (Harvard Law Review)
- „The desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behavior to others.“
  - Alan Westin („Privacy And Freedom“, 1967)
    Prof. Emeritus, Columbia University

Why Privacy?

Privacy isn’t just about keeping secrets – data exchange and transparency are key issues!

- Reasons for Privacy
  - Free from Nuisance
  - Intimacy
  - Free to Decide for Oneself
- Requirement for Democracy
  - Informational Self-Determination
    - German Federal Constitutional Court, Census Decision 1983
  - „...an essential requirement for a democratic society that is built on the participatory powers of its citizens. “
So what does this mean for **personal privacy**?

**Ubicomp Privacy Implications**

- **Data Collection**
  - Scale (everywhere, anytime)
  - Manner (inconspicuous, invisible)
  - Motivation (context!)

- **Data Types**
  - Observational instead of factual data

- **Data Access**
  - “The Internet of Things”

---

How do we achieve privacy?

Privacy – Not Just a Recent Fad

- Justices Of The Peace Act (England, 1361)
  - Sentences for Eavesdropping and Peeping Toms
  - „The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail; its roof may shake; … – but the king of England cannot enter; all his forces dare not cross the threshold of the ruined tenement“
  - William Pitt the Elder (1708-1778)
  - Defined common European framework for national privacy laws
Basis: Fair Information Principles (FIP)

- Drawn up by the OECD, 1980
  - “Organisation for economic cooperation and development”
  - Voluntary guidelines for member states
  - Goal: ease transborder flow of goods (and information!)
- Five Principles (simplified)
  1. Openness
  2. Data access and control
  3. Data security
  4. Collection Limitation
  5. Data subject’s consent
- Core principles of modern privacy laws world-wide
  - Implication: Technical solutions must support FIP

FIP Challenges in Ubicomp

1. How to inform subjects about data collections?
2. How to provide access to stored data?
3. How to ensure confidentiality, integrity, and authenticity (w/o alienating user)?
4. How to minimize data collection?
5. How to obtain consent from data subjects?

Basis: Transparency Protocols
Platform for Privacy Preferences Project (P3P)

- Goal: Support automated decision-making over Web privacy policies
  - Compare policies with personal preferences
  - Log collection incidents for inspection and auditing
- Machine-readable data collection/usage policy
  - Who collects and/or processes the data?
  - What information is collected?
  - For what purpose is this data collected?

Cranor, Langheinrich, Marchiori, Reagle: The Platform for Privacy Preferences 1.0 Specification. W3C Recommendation, April 2002
PawS – A Privacy Awareness System

1. Privacy Beacons

- **Announce (Unobtrusive) Data Collections**
  - “Protocol Beacons” integrated into communications protocol
  - “Stand-alone Beacons” for video, audio, sensory data
  - Detected by mobile “Privacy Assistant” (e.g., wristwatch)

- **Describes Current/Potential Data Collection**
  - Format: machine-readable privacy policy ("P3P++")
  - Extending it for Ubicomp-specific elements (e.g., sensor data)
2. Privacy Proxies

- **Service Proxy** Solicitates Consent (if Needed)
  - User proxy compares user preferences with privacy policy of service provider

- **Central Access Point for Data Management**
  - Supports updating and deleting data and contracts

![Diagram](image1.png)

3. Privacy-Aware Database

- **All Data is Stored Together With Privacy (P3P) Policy**
  - Data and policy (Metadata) form logical unit

- **Each Data Access Needs Usage Policy**
  - Database compares allowed/announced and proposed usage
  - Data with non-matching allowed usage is held back
  - Each data access (who, why) is recorded (auditing)

![Diagram](image2.png)
Privacy is compatible with Ubiquitous Computing – technical solutions can support FIP in Ubicomp

Today’s Topics

- **Background: Ubicomp Privacy**
  - What is privacy?
  - How does ubiquitous computing affect it?

- **Privacy Infrastructure: PawS**
  - Privacy beacons, privacy proxies, and privacy-aware databases

- **Real-World Example: RFID**
  - PawS-RFID: privacy protocols for transparency
  - Shamir Tags: protection against unauthorized readouts
Today’s RFID Systems

All tags respond, please!

DB

ID 8.95.6.086
ID 2.1.741.850
ID 9.834.12.30
ID 9.834.12.31
ID 9.834.59.01
ID 8.75.03.914
ID 1.82.221.3
ID 8.95.6.086
ID 2.1.741.850
ID 9.834.12.30
ID 9.834.12.31

RFID-PawS

- Goal: Fair Information Principles for RFID
- PawS and RFID
  - Privacy beacon: RFID-reader
  - Privacy assistant: „watchdog-tag“
  - Privacy proxies & privacy database
- Requirements
  - RFID-standard compatibility
  - Low bandwidth

Example: Openness in RFID-PawS

- **Init Round Command in ISO 18000 Part 6**
  - Defines start of reading cycle (Aloha-based anti-collision)
  - Defines anti-collision protocol parameters
- **New: 130 Bits „Privacy-Header“ Extension**

### Openness using the ReaderPolicyID

<table>
<thead>
<tr>
<th>Protocol extension</th>
<th>Init round all</th>
<th>SUID flag</th>
<th>Round size</th>
<th>CRC-5</th>
<th>CRC-16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 bit</td>
<td>6 bits</td>
<td>1 bit</td>
<td>3 bits</td>
<td>5 bits</td>
<td></td>
</tr>
</tbody>
</table>

- **CRC-5**
  - 96 bits
- **CRC-16**
  - 16 bits

- **Collection type**
  - 2 bits
- **Purpose**
  - 2 bits

- **Header**
  - 8 bits
- **Data Collector**
  - 28 bits
- **Policy**
  - 24 bits
- **Reader**
  - 36 bits

**5F.4A886EC.8EC947.24A68E4F6**

- Each Read Request can be Associated with Data Collector
  - Data collector, reader, and privacy policy identifiable (auditing)
  - Format follows EPC standard (facilitates implementation)
Today’s RFID Systems (with RFID-PawS)

Example Store, Smart Shelf 4: Local Identification, Inventory, All

Privacy Policy

Data Access & Control

Openness

User Consent

Collection Limitation

Privacy Policy

Data Access & Control

Openness

User Consent

Collection Limitation

Tomorrow’s RFID-Systems?

Example Store, Smart Shelf 4: Local Identification, Inventory, All
But what about unauthorized RFID readers?

Solution: Disabling RFID Tags

- „Dead Tags Tell No Tales“
  - Permanently deactivate tag at checkout
- Hard Kill
  - Cut tag antenna or „fry“ circuit
- Soft Kill
  - Needs password to prevent unauthorized killing

- Both Approaches Require Consumer Action
  - Also voids any post-sales benefits (returns, services, …)
Alternative: Securing RFID-Tags Against Unauthorized Readouts

- **General Principle: Lock/Unlock ID With Password**
  - Tag only replies if correct password/secret is sent

- **Requires RFID-Owner to Know Secret**
  - Password must be transferred at checkout (where to?)

- **Requires Owner to Know Which Secret to Use**
  - Chicken And Egg Problem: If you don’t know what tag it is, how do you know what password to use?

Deactivation and Password Management...

Does Your Solution Work Here?
Alternative: Shamir Tags
An Example for Zero-Management Privacy Protection

- **Default: Tags Take Long Time To Read**
  - Complicates Tracking & Unauthorized Identification
  - Bitwise release, short range (e.g., one random bit/sec)
  - Intermediate results meaningless, since encrypted
  - Decryption requires all bits being read
- **But: Known Tags Can be Directly Identified**
  - Allows owner to use tags without apparent restrictions
  - Initial partial release of bits enough for instant identification from a limited set of known tags

---

Secret Shares (Shamir 1979)

Polynomial of degree $n$ can be described using at least $n+1$ points

$$p(x) = s + a_1 x + a_2 x^2$$
Secret Shares (Shamir 1979)

\[ p(x) = s + a_1 x + a_2 x^2 \]

- 96-bit EPC Code
- 106-bit Shamir Share
- 318-bit Shamir Tag

\[ 11100001101010001010111010101101010100\ldots1010101110101 \]

\[ 011010111\ldots101 \]

\[ 111000011101010001010111010101101010100\ldots1010101110101 \]
### Personal Privacy in Ubiquitous Computing

#### March 11, 2008

**Marc Langheinrich**

**ETH Zurich**

---

**110110111…1101 Secret**

**111000011…110101**

**101101101…110111**

**Shares**

**hi**

**96‐bit EPC Code**

**106‐bit Shamir Share**

**1011010011…101101**

**318‐bit Shamir Tag**

**318‐bit Shamir Tag**

**106‐bit Reply**

**Initial Reply**

**16‐bit Reply**

**Bit Disclosure Over Time**

**Instant identification of known items**

**Unknown tags will eventually be identified**

---

### Preventing Tracking

- **Subsequent readouts receive only substring of bits**
  - Insufficient data to track tag repeatedly
  - E.g., tag population of 10⁹ over 3 million tag have 5 bits in common
# of Overlapping Bits Between 2 Readouts

<table>
<thead>
<tr>
<th>x</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
</tr>
<tr>
<td>1</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>99.79%</td>
</tr>
<tr>
<td>2</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>99.05%</td>
<td>99.05%</td>
<td>97.35%</td>
<td>88.35%</td>
<td>64.42%</td>
<td>76.73%</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>98.17%</td>
<td>98.17%</td>
<td>98.24%</td>
<td>43.10%</td>
<td>20.59%</td>
<td>7.10%</td>
<td>1.85%</td>
<td>0.32%</td>
<td>0.03%</td>
<td>0.00%</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>42.07%</td>
<td>4.06%</td>
<td>1.86%</td>
<td>0.18%</td>
<td>0.01%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5.00%</td>
<td>0.12%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0.35%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.02%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.00%</td>
<td></td>
</tr>
</tbody>
</table>

E.g., a 0.12% chance that the same 5 bit positions are read from \(\geq 2\) tags

More Privacy Through Less Security?

- **Shamir Tags Require No Consumer Effort**
  - Delay upon first use, but **no passwords** to manage!
  - Not useful for „important“ items (passports, e-money)
  - Does not alleviate user concerns (tags remain active)

- **Building Block for Comprehensive Solution**
  - Strong crypto for passports, drug-authenticity, ...
  - Clipping/killing for concerned consumers
  - Unconcerned consumers get basic protection „for free“
  - Combined with Paw5-like background infrastructure
Today’s Topics

- **Background: Ubicomp Privacy**
  - What is privacy?
  - How does ubiquitous computing affect it?
- **Privacy Infrastructure: PawS**
  - Privacy beacons, privacy proxies, and privacy-aware databases
- **Real-World Example: RFID**
  - PawS-RFID: privacy protocols for transparency
  - Shamir Tags: protection against unauthorized readouts

Where to Go From Here? (Current Activities)

- **Further Application of Shamir Tags**
  - Highly distributed version (Hitachi mu-chips)
  - As location-based access control
- **The Role of Mobile Phones as Interaction Devices**
  - Open-source 1d bar code recognition toolkit
  - As a universal information appliance & control device
  - Security and privacy issues in mobile phone use
- **Understanding Implicit Interactions**
  - Within context of augmented toy environments
Where to Go From Here? (Current Activities)

- Further Application of Shamir Tags
  - Langheinrich: *Secure Localized Storage Based on Super-Distributed RFID-Tag Infrastructures*. Journal of Location Based Services. Accepted for publication, 2008

- The Role of Mobile Phones as Interaction Devices

- Understanding Implicit Interactions

Summing Up!
Take Home Message(s)

- Privacy is more than just „good security“
  - It’s about sharing and control
- Smart environments pose new challenges
  - Novel data types, increased # of incidents, hidden collection
- Security and privacy must be usable to be useful!
  - Almost never primary goals, get easily „in the way“
- Goal: privacy mechanisms that „just work“
  - Paws: transparency and control for smart environments
  - Shamir Tags: protection from unauthorized readouts