Personal Security and Privacy in Ubiquitous Computing

Marc Langheinrich
Institute for Pervasive Computing
ETH Zurich, Switzerland
Approaches to Security & Privacy in Ubicomp
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

- What is Privacy and Why Should We Want It?
- How do Future Smart Environments Challenge Existing Solutions?
- How Less Security Can (Sometimes) Increase Privacy
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
- Things are aware of each other and the environment
- Integrating computers with intuitive user interfaces
Energy-Efficient Heating

- Sensors Inside and Outside
- Takes Weather Forecast into Account
- „Conspires“ with Car of Owner & E-Agenda to know Time of Arrival
Instead of „World inside the Computer“…

Not like this!
World inside Computer would be Virtual Reality
„Computer in the World“
Is Technology a Good Predictor?

- Past Predictions...
Societal Trends (Ubicomp Drivers)

- **Higher Efficiency**
  - Lean production (Overproduction, Out-of-Stock)
  - Targeted Sales (1-1 Marketing)

- **More Convenience**
  - Finding your way (e.g., travel assistants)
  - Lower TCO (“total cost of ownership”) w/ pay-per-use

- **Increased Safety**
  - Homeland security (terrorism, drug trafficking, etc.)
  - Road safety & health (e.g., black box for cars)
So what does this mean for personal privacy?
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?

- Reasons for Privacy
  - Free from Nuisance
  - Intimacy
  - Free to Decide for Oneself

- By Another Name...
  - Data Protection
  - Informational Self-Determination

Privacy isn’t just about keeping secrets – data exchange and transparency are key issues!
“But I’ve Got Nothing to Hide!”
Do you?

- Arson Near Youth House Niederwangen
  - At scene of crime: Migros-tools
  - Court ordered disclosure of all 133 consumers who bought items on their supermarket loyalty card (8/2004)
  - (Arsonist not yet found)
- “Give me six lines written by the most honorable of men, and I will find an excuse in them to hang him”

Armand Jean du Plessis, 1585-1642 (a.k.a. Cardinal de Richelieu)
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)

- First Data Protection Law in the World in Hesse
  - 1970
The 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 most modern privacy laws**
  - Implication: Technical solutions must support FIP
1. Challenge: Openness

- No Hidden Data Collection!
  - Legal requirement in many countries
- Established Means: Privacy Policies
  - Who, what, why, how long, etc. ...
- How to Publish Policies in Smart Environments?
  - Is a poster enough? A paragraph of fine print?
- Too Many Transactions?
  - Countless announcements an annoyance
2. Challenge: Access & Control

- **Identifiable Data Must be Accessible**
  - Users can review, change, sometimes delete

- **Collectors Must be Accountable**
  - Privacy-aware storage technology

- **When Does Sensor Data Become Identifiable?**
  - Even anonymized data can identify people (AOL case)

- **Who to Ask? How to Verify? How to Display?**
  - Who was reading me when? Is this really my trace?
3. Challenge: Data Security

- **Traditional Approach: Centralistic Authentication**
  - Powerful centralized system with known user list
  - Plan for worst case scenario (powerful attacker)

- **Numerous, Spontaneous Interactions**
  - How do I know who I communicate with, who to trust?
  - How much extra time does “being secure” take?

- **Complex Real-World Situations**
  - Access to my medical data in case of emergency?

- **Context-Dependent Security?**
  - Based on battery power, data type, location, situation
4. Challenge: Data Minimization

- Only collect as much information as needed
  - No in-advance data collection for future uses
- Best: use anonymous/pseudonymous data
  - No consent, security, access needed
- How much data is needed for becoming “smart”?
  - No useless data in smart environments (context!)
- Sometimes one cannot hide!
  - Sensor data (biometrics) hard to anonymize
5. Challenge: Consent

- Participation Requires Explicit Consent
  - Usually a signature or pressing a button

- True Consent Requires True Choice
  - More than „take it or leave it“, needs alternatives

- How to Ask “On The Fly”?
  - The mobile phone as a background agent (legal issues?)

- Consenting to What?
  - Do I understand the implications?
  - Do I have options?
Ubicomp Challenges to Security & Privacy

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?
Public Concern over Unauthorized RFID Access
Unauthorized RFID Access – Implications

Passport:
Name: John Doe
Nationality: USA
Visa for: Israel

Wig:
Modell #2342
Material: Polyester

Tiger Tanga:
Manufacturer: Woolworth
Washed: 736

Viagra:
Manufacturer: Pfitzer
Extra Large Package

Wallet:
Contents: 370 Euro
Disability Card: #2845
Securing RFID Access

- 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 Out
  - 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

011010111…1101

Secret \( s \)

111000011…101101

106-bit Shamir Share

101101101…110111

318-bit Shamir Tag

11100001110100010101110101101010100…1010101110101

Shamir Tag

\[ p(x) = s + a_1 x + a_2 x^2 \]
96-bit EPC-Code: 011010111…1101

106-bit Shamir Share:
- 111000011…101101
- 101101101…110111
- 101010011…101101 Shares

318-bit Shamir Tag: 111000011101010001010111010101101010100…1010101110101

16-bit Reply: 1 0 1 1 10 1 1

Bit Disclosure Over Time:
- 1 0 1 1 010 1 1
- 1 0 1 1 010 0 1 1
- 1 1 0 1 1 010 0 1 1
- 01 1 0 1 1 010 0 1 1
- 01 1 0 0 1 1 010 0 1 1

Unknown tags will eventually be identified.

Instant Identification of Known Items:
16-bit Reply: 1 0 1 1 10 1 1

Time +1 bit

Initial Reply: 1 0 1 1 10 1 1

19.11.2007 Personal Security and Privacy in Ubiquitous Computing
Preventing Tracking

- Subsequent readouts receive only substring of bits
  - Insufficient data to track tag repeatedly
  - E.g., tag population of $10^9$ over 3 million tag have 5 bits in common
# of Overlapping Bits Between 2 Readouts

<table>
<thead>
<tr>
<th>x</th>
<th>&gt;=1</th>
<th>&gt;=2</th>
<th>&gt;=3</th>
<th>&gt;=4</th>
<th>&gt;=5</th>
<th>&gt;=6</th>
<th>&gt;=7</th>
<th>&gt;=8</th>
<th>&gt;=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>
</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>99.79%</td>
</tr>
<tr>
<td>2</td>
<td>100.00%</td>
<td>100.00%</td>
<td>100.00%</td>
<td>99.95%</td>
<td>99.58%</td>
<td>97.35%</td>
<td>88.35%</td>
<td>64.42%</td>
<td>26.72%</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>98.17%</td>
<td>89.17%</td>
<td>69.24%</td>
<td>43.10%</td>
<td>20.59%</td>
<td>7.30%</td>
<td>1.85%</td>
<td>0.32%</td>
<td>0.03%</td>
<td>0.00%</td>
</tr>
<tr>
<td>4</td>
<td>42.07%</td>
<td>9.56%</td>
<td>1.36%</td>
<td>0.13%</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>
</tr>
<tr>
<td>5</td>
<td>5.09%</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>
</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>
</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>
</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>
</tr>
</tbody>
</table>

E.g., a 0.12% chance that the same 5 bit positions are read from >=2 tags

Original "RFID-Man" Artwork (c) 2006 Ari Juels, RSA Laboratories
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“
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, implicit interactions
- Security and privacy must be **usable** to be useful!
  - Almost never primary goals, get easily „in the way“
- Goal: security/privacy mechanisms that „just work“
  - Shamir Tags: protection from unauthorized readouts
SPMU’o8: Security & Privacy Issues in Mobile Phone Use

- Secure payment/ticketing and authentication systems
- Usability issues in mobile phone security/privacy
- Public perception, legal, and social issues
- Digital rights management on mobile phones
- Options for using mobile phones in law enforcement

Organized by:
- Rene Mayrhofer (Lancaster University, UK)
- Marc Langheinrich (ETH Zurich, Switzerland)
- Alexander De Luca (LMU Munich, Germany)

Workshop call soon on: www.pervasive2008.org
Take Home Message(s) & Thank You!

- Privacy is **more** than just „good security“
  - It’s about sharing and control
- **Smart environments pose new challenges**
  - Novel data types, increased # of incidents, implicit interactions
- **Security and privacy must be usable to be useful!**
  - Almost never primary goals, get easily „in the way“

- **Goal: security/privacy mechanisms that „just work“**
  - E.g., **Shamir Tags**: protection from unauthorized readouts