Protection of the Users’ Privacy in Ubiquitous RFID-based Systems

Ivan Gudymenko

24.04.2012
Outline

- Intro
- E-ticketing
- Personal Belongings Management
- Conclusion and future work
Outline

• Intro

• E-ticketing

• Personal Belongings Management

• Conclusion and future work
Intro

- UbiComp systems based on RFID
- Privacy issues address serious concerns
- Motivation: making UbiComp privacy-respecting
- Two use cases:
  - E-ticketing
  - Personal Belongings Management
Outline

- Intro
- E-ticketing
- Personal Belongings Management
- Conclusion and future work
E-ticketing: A General Scenario

E-ticket distribution

Trip begin
ID processing unit (e.g. GPS-based)
[userID, vehicleID, in(time, coord.), out(time, coord.)]

Check-in
Reader

Trip end

Check-out

Back-end system
- distance calculation
- billing
- customer accounts mgmt.
- statistics
Privacy Concerns in E-ticketing

- Unintended customer identification
  - exposure of customer ID (direct and indirect)
  - unencrypted ID during the anti-collision session
  - physical layer identification (RFID fingerprinting)
- Information linkage
- Illegal customer profiling

Privacy Protection Goals:
1. Anonymity
2. Confidentiality
3. Unlinkability
4. Unobservability
# Privacy Concerns in E-ticketing: Countermeasures

<table>
<thead>
<tr>
<th>Threats</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Unintended customer identification:</td>
<td></td>
</tr>
<tr>
<td>(a) Exposure of customer ID:</td>
<td>Privacy-respecting authentication; ID encryption/randomization; access-control</td>
</tr>
<tr>
<td>i. personal ID exposure (direct)</td>
<td>functions [JP02]</td>
</tr>
<tr>
<td>ii. indirect identification</td>
<td>ID encryption</td>
</tr>
<tr>
<td>(b) Unencrypted ID during anti-collision</td>
<td>Randomized bit encoding [LLY08b]; bit collision masking [CR06, LLY08a] (protocol</td>
</tr>
<tr>
<td>(c) PHY-layer identification</td>
<td>dependent)</td>
</tr>
<tr>
<td>2. Information linkage</td>
<td>Shielding; switchable antennas [Gud11]</td>
</tr>
<tr>
<td>3. Illegal customer profiling</td>
<td>Anonymization (in front-end and back-end)</td>
</tr>
<tr>
<td></td>
<td>Privacy-respecting data storage (back-end); the same as in threat 1</td>
</tr>
</tbody>
</table>
Aimed at providing interoperability

Many existent solutions are still proprietary, though
Privacy-related Issues: Architecture Level – ISO EN 24014-1

Coarsely-specified, general privacy requirements:

- data minimization
- user consent acquisition
- customer confidentiality

No recommendations for further implementation
## Privacy-related Issues: Data Interfaces Level

<table>
<thead>
<tr>
<th>Privacy, security</th>
<th>Architecture</th>
<th>ISO EN 24014-1 (conceptual framework)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data interfaces</td>
<td>EN 15320 (logical level, abstract interface, security)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>EN 1545 (data elements)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISO/IEC 7816-4 (commands, security)</td>
<td></td>
</tr>
<tr>
<td>Communication interface</td>
<td>ISO 14443 (Parts 1-3 required)</td>
<td></td>
</tr>
</tbody>
</table>
Privacy-related Issues: Data Interfaces Level – EN 15320

<table>
<thead>
<tr>
<th>Privacy, security</th>
<th>Architecture</th>
<th>Data interfaces</th>
<th>Communication interface</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ISO EN 24014-1 (conceptual framework)</td>
<td>EN 15320 (logical level, abstract interface, security)</td>
<td>ISO 14443 (Parts 1-3 required)</td>
</tr>
<tr>
<td></td>
<td>EN 1545 (data elements)</td>
<td>ISO/IEC 7816-4 (commands, security)</td>
<td></td>
</tr>
</tbody>
</table>

- Specification of a generic Security Subsystem
- Access control to privacy-relevant fields further defined in EN 1545
Security Subsystem in EN 15320

[Diagram of the security subsystem showing the interaction between the Terminal, Card, Card Data Interface, Card security Management System, Data Groups (DG), and Card Profiles.]

1. Search card
2. Profile ID
3. Card commands

ISO/IEC 14443 interface

Profile 1:
Function X
{command a; command b; command c;}

Profile 2:
Function Y
{command d; command e; command f;}

Profile n:
Function Z
{command g; command h; command i;}

Card Data Interface

Card security Management System

Data Groups (DG)

Card Profiles

Card data
Privacy-related Issues: Data Interfaces Level – EN 1545

- Privacy-relevant data fields (customer number, birth date, etc.)
- Access control and encryption for protection
### Privacy-relevant Fields in EN 1545-1

<table>
<thead>
<tr>
<th>Privacy-relevant field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>birth date</td>
<td>-</td>
</tr>
<tr>
<td>birth name</td>
<td>-</td>
</tr>
<tr>
<td>birth place</td>
<td>-</td>
</tr>
<tr>
<td>customer number</td>
<td>customer reference number</td>
</tr>
<tr>
<td>device ID</td>
<td>can be linked to a particular customer</td>
</tr>
<tr>
<td>e-mail address</td>
<td>-</td>
</tr>
<tr>
<td>telephone number</td>
<td>-</td>
</tr>
<tr>
<td>postal address</td>
<td>-</td>
</tr>
<tr>
<td>location ID</td>
<td>-</td>
</tr>
<tr>
<td>customer profile ID</td>
<td>e.g. student, military, resident, etc.</td>
</tr>
<tr>
<td>user data</td>
<td>additional information about a customer</td>
</tr>
</tbody>
</table>
Privacy-related Issues: Data Interfaces Level – ISO 7816-4

- Secure messaging mechanisms
- Can be used for protecting privacy-critical data

<table>
<thead>
<tr>
<th>Privacy, security</th>
<th>Architecture</th>
<th>ISO EN 24014-1 (conceptual framework)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data interfaces</td>
<td>EN 15320 (logical level, abstract interface, security)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>EN 1545 (data elements)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ISO/IEC 7816-4 (commands, security)</td>
</tr>
<tr>
<td></td>
<td>Communication interface</td>
<td>ISO 14443 (Parts 1-3 required)</td>
</tr>
</tbody>
</table>
Privacy-related Issues: Communication Interface

- Solely functionality-oriented
- No security or privacy mechanisms considered
Privacy-related Issues: Summary

<table>
<thead>
<tr>
<th>Standard</th>
<th>Security</th>
<th>Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO EN 24014-1</td>
<td>- definition of security policy;</td>
<td>coarsely specified privacy requirements, targeted at compliance with</td>
</tr>
<tr>
<td></td>
<td>- security management (by the Security Manager entity).</td>
<td>the regulation</td>
</tr>
<tr>
<td>EN 15320</td>
<td>- Security Subsystem (SSS);</td>
<td>- privacy-relevant data groups;</td>
</tr>
<tr>
<td></td>
<td>- security-related operations are defined in profiles.</td>
<td>- protection through access control (AC) and encryption.</td>
</tr>
<tr>
<td>EN 1545</td>
<td>security-relevant fields</td>
<td>privacy-relevant fields</td>
</tr>
<tr>
<td>ISO/IEC 7816-4</td>
<td>- secure messaging;</td>
<td>security mechanisms can be applied to privacy-critical data</td>
</tr>
<tr>
<td></td>
<td>- security architecture with AC</td>
<td></td>
</tr>
<tr>
<td>ISO 14443 (1-3)</td>
<td>not considered</td>
<td>not considered</td>
</tr>
</tbody>
</table>

Legend: **AL** – Architecture level  
**DIL** – Data interfaces level  
**CIL** – Communication interface level
Privacy-related Issues: Summary (2)

- Security mechanisms are considered in the first place
- Customer privacy more as a by-product
- Privacy issues are not explicitly addressed across the stack
- Proprietary solutions act in a similar way (ITSO, CALYPSO, MIFARE)

⇒ Develop an approach explicitly addressing privacy in a cross-layer fashion and across system components
Outline

• Intro

• E-ticketing

• Personal Belongings Management

• Conclusion and future work
A General Scenario

- **Home**
  - RFID infrastructure
  - Personal tracking device

- **Travel**
  - Personal tracking device only

- **Office**
  - RFID infrastructure
  - Personal tracking device
Key Differences to E-ticketing

- The requirement to track items from a certain distance
- No validation step is required
- Anonymization is easier
- Only a few readers (e.g. a portable one, at work and at home)
- Compliance to the Standards Stack not required (weaker interoperability?)

➡ Develop a privacy-respecting solution for personal belongings management
Outline

- Intro
- E-ticketing
- Personal Belongings Management
- Conclusion and future work
Conclusion

- Two use cases for the PhD dissertation have been discussed
- Focus on user privacy
- No decent cross-layer, cross-component solution with respect to privacy has been developed so far
Future Work

- Further research on partial solutions developed so far
- Identify what can be done for a decent cross-layer, cross-component solution
- Focus on the issues representing a particular interest for a research community and industry
## Time Plan: Near Future

<table>
<thead>
<tr>
<th>Month</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2012</td>
<td>• Finish State-of-the-Art:</td>
</tr>
<tr>
<td></td>
<td>- proprietary solutions</td>
</tr>
<tr>
<td></td>
<td>- focus papers</td>
</tr>
<tr>
<td></td>
<td>• Privacy-preserving protocol evaluation</td>
</tr>
<tr>
<td>June 2012</td>
<td>• Specific tasks determination</td>
</tr>
<tr>
<td></td>
<td>• Core concept development</td>
</tr>
<tr>
<td>July/August 2012</td>
<td>• Requirements paper for doctoral symposium</td>
</tr>
</tbody>
</table>
References


Thank you very much for your attention!

Questions?
Comments?
Suggestions?
Back-up Slides
Logical Interfaces in EN 15320: States Transitional Diagram