On Privacy Evidence for UbiComp Environments
Broadening the Notion of Control to Improve User Acceptance

Rafael Accorsi and Matthias Bernauer
University of Freiburg, Germany

UbiPriv'07, Innsbruck

UbiComp and user acceptance
- UbiComp status quo: huge potential, tiny user acceptance
  - Projects stagnate or are called off.

Two reasons:
- Bad usability:
  - Frustration.
- Lacking privacy:
  - Fear of surveillance.
  - Loss of control over personal data.

Æ Lack of control leads to user scepticism, rejection…

Control: What privacy-enhancing technologies can offer?

<table>
<thead>
<tr>
<th>Paradigm</th>
<th>Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>Information hiding (k-)anonymity</td>
</tr>
<tr>
<td></td>
<td>Pseudonymy, partial identities, (federated) identity management, zero-knowledge identity proofs.</td>
</tr>
<tr>
<td>Usage control</td>
<td>Unilateral privacy statement Privacy certification/seals, declarative privacy policies</td>
</tr>
<tr>
<td></td>
<td>Bilateral negotiation on terms of usage Provisional and obligational (sticky) policies</td>
</tr>
</tbody>
</table>

• "Control" = a priori regulation of privacy preferences.
• Regulation is necessary for acceptance but not sufficient.

Control encompasses supervision
- Thesis: Control = regulation + supervision.
- Complete control mechanisms => better user acceptance.

• Supervision: does UbiComp act in compliance with privacy policies?
  - No prevention of privacy violations, but their detection.
  - Sanctions are due in case of violations.

• Approach: privacy evidence.
  - Reports generated by automated system audits.

Privacy evidence architecture

Automated audit: "Model-checking" rationale
- Privacy properties expressed by rules $P_{expr} = \{\pi_1, \ldots, \pi_k\}$.
- No formal system model but:
  - Complete and finite state-space (BBox).
  - Selection of "relevant" events (log view).
- Audit based on falsification.
  - Each (negated) rule is checked against the log view.
  - If violation, audit gives counter-example.
Expression of privacy properties

- Privacy properties based on data collection and access.
  - Conditions: **provision** and **obligations**.

- Examples of rules:
  - **Deny** rule:
    \[ r_1 = \text{(deny, RFID-Reader.*, *, *)} \]
    Prohibit the collection of any RFID information.

  - **Allow** rule:
    \[ r_2 = \text{(allow, *, Transaction.Value, read, if (Transaction.Date > 01-01-2007 \&\& purpose == statistic) \&\& (notify A within 7 days))} \]
    Allow any subject to read the value of transactions with the provisions that...

- Discretionary access control policies expressing safety properties.

Falsification of privacy properties

- Transformation function \( \gamma' \):
  - Takes a policy and returns the family of violations \( \gamma' \).

- Falsification strategy:
  - **Deny** rule:
    \[ r_1 = \text{(deny, RFID-Reader.*, *, *)} \]
    Falsification of the conditions.

- **Allow** rule:
  - Change rule’s polarity
  \[ v_1 = \text{(allow, RFID-Reader.*, *, *)} \]
  - Negate rule’s conditions
  \[ v_2 = \text{(allow, *, Transaction.Value, read, if (Transaction.Date <= 01-01-2007 \&\& purpose != statistic) \&\& (notify A after 7 days))} \]

- Other falsification strategies are allowed.

Compliance audits

- Can violation \( v \) be pinpointed in \( L \) ? \( v \not\in L \).
  - Pattern matching of entries and violations head ("anchor").
  - Provisions: evaluate access/collection request.
  - Obligations: check existence and evaluate temporal modality.

- Example: check violation \( v_1 = \text{(allow, RFID-Reader.*, *, *)} \)

- Privacy evidence: log view and audit.
  - Semaphore notation indicates audit result.
  - Different navigation levels.

Conclusion and outlook

- **Contribution**: realisation of supervision.
  - Privacy evidence based on audit trails and secure logging.

- Current assumptions:
  1. Every event is collected in the BBox.
  2. Users are "identified" during the interaction.
  3. The collection and processing capabilities are static.

- Ongoing work focuses on relaxing these assumptions.

- **Related research fields**:
  - Provable enforcement.
  - Compliance.
  - Usability.

- **Privacy forensics**: "evidence as an evidence".
  - http://www.telematik.uni-freiburg.de/PrivacyForensics