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.

  → Lack of control leads to user scepticism, rejection…

Control: What privacy-enhancing technologies can offer?

	Paradigm	Principles
Access control	Information hiding	(k-)anonymity
		Pseudonyms, partial identities, (federated) identity management, zero-knowledge identity proofs
Usage control	Unilateral privacy statement	Privacy certification/seals, declarative privacy policies
	Bilateral negotiation on terms of usage	Provisional and obligational (sticky) policies

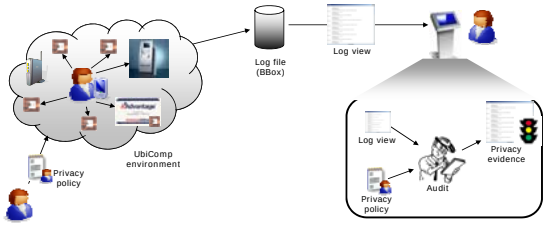
- "Control" = a priori *regulation* of privacy preferences.
- Regulation is necessary for acceptance **but not sufficient.**

Control encompasses supervision

- Thesis: Control = regulation + ***supervision***.
- Complete control mechanisms ⇝ better user acceptance.

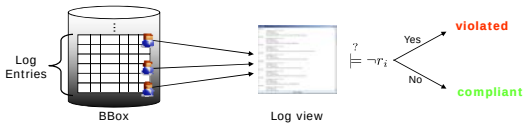
- Supervision: does UbiComp act in compliance with privacy policies?
  - No prevention of privacy violations, but their detection.
  - Sanctions are due in case of violations.
- Approach: *privacy evidence*.
  - Reports generated by automated system audits.

Privacy evidence architecture



Automated audit: "Model-checking" rationale

- Privacy properties expressed by rules $P_{User} = \{r_1, \ldots, r_n\}$.
- 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: provisions and obligations.
- Examples of rules:

```
r1 = (deny, RFID-Reader.*, *, *)
```

Prohibit the **collection** of any RFID information.

```
r2 = (allow, *, Transaction.Value, read,
  if (Transaction.Date > 01-01-2007
      && purpose != statistic)
 and (notify A within 7 days))
```

Allow any subject to **read** the value of transactions with the proviso that…

→ Discretionary access control policies expressing safety properties.

Falsification of privacy properties

- Transformation function ν:
  - Takes a policy and returns the family of violations V.
- Falsification strategy:

```
r1 = (deny, RFID-Reader.*, *, *)
```

Change rule's polarity

```
v1 = (allow, RFID-Reader.*, *, *)
```

```
r2 = (allow, *, Transaction.Value, read,
  if (Transaction.Date > 01-01-2007
      && purpose == statistic)
 and (notify A within 7 days))
```

Negate rule's conditions

```
v2 = (allow, *, Transaction.Value, read,
  if (Transaction.Date <= 01-01-2007
      || purpose != statistic)
  or (notify A after 7 days))
```

- Other falsification strategies are allowed.

Compliance audits

- Can violation v_i be *pinpointed* in L? $L \rhd v_i$.
  - Pattern matching of entries and violations head ("anchor").
  - Provisions: evaluate access/collection request.
  - Obligations: check existence and evaluate temporal modality.
- Example: check violation `v1 = (allow, RFID-Reader.*, *, *)`

```
42, Scanner, COL_159, RFID_Reader.5, Profile.PassNr, 9543329, Identity_Check, deny
45, Scanner, COL_172, BarCode_Scanner.2, Transaction.BP-Nr, 1787732, BP_Check, allow
69, Scanner, COL_198, RFID-Reader.7, shelf, 1734, CRM, recommend, RFID_Tag, allow
73, Terminal, COL_211, Terminal.1, corridor, 1445, CRM, recommend, Transaction, deny
```

Log view (excerpt)

Counterexample

- 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 focusses on relaxing these assumptions.
- Related research fields:
  - Provable enforcement.
  - Compliance.
  - Usability.
- Privacy forensics: "evidence as an evidence".
  http://www.telematik.uni-freiburg.de/PrivacyForensics