Privacy Enhancing Service-Interfaces

Daniel Janusz

Advisors: Freytag, Polze

Key Contributions

- **Privacy aware Service Modelling:**
  Verifying privacy properties of service-oriented architectures
- **Privacy Facades:**
  Encapsulating service-interfaces for enhancing privacy
- **PP2PP:**
  Privacy protocol for exchanging personal data in distributed systems

Privacy aware Service Modelling

- Algebraic nets for modelling relational data

<table>
<thead>
<tr>
<th>(name, size, sensor-object)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Max, 1.78, (gyroscope, -0.15))</td>
</tr>
</tbody>
</table>

 verifying formulas: $A.(\text{Max}, 1.78, (\text{gyro}, -0.15)) \rightarrow C.(\text{Max})$?

- $F1, F2$: generated privacy facades

Application: Human Fall Detection

- **System architecture**

- **Lookup process of patient data**

PP2PP: Privacy Preserving 2-Phase Protocol

Privacy requirements for data exchange:
1. Querying one specific individual while not disclosing his/her identity:
   - Fuzzy Queries
2. Requestors can read the result only if they are authorized by the individual:
   - Authorized Data Exchange

State of the Art

Existing formal logics and formal languages:
- state different aspects of privacy, e.g. privacy policies
- reason about if a model satisfies a property or policy
- detect inconsistencies between different privacy policies
- no (semi-)automatic privacy enhancement

Existing data exchange protocols:
- guarantee privacy in distributed systems
- depend on computational heavy encryption or trusted 3rd parties

Publications