Privacy-Aware Service Integration

Pierre Parrend, Stéphane Frénot
pierre.parrend@insa-lyon.fr
Lab. CITI, 21, Avenue J. Capelle
69621 Vileurbanne Cedex, France

Sebastian Höhn
sebastian.hoehn@iig.uni-freiburg.de
Dept. of Telematics
University Freiburg (Germany)
Context

- Pervasive Systems
  - Personnalized Services Everywhere
  - Useful when combined together
- Data handling in Pervasive Systems
A Framework for Privacy Aware Service Integration

- A vision of Pervasive Services
- Secure Architecture for Pervasive Service Provisioning
- Privacy Model
- System Requirements
A Vision of Pervasive Services

- Use Case I: Intelligent supermarket
A Vision of Pervasive Services

- Use Case II: On-board Desktop
A Vision of Pervasive Services

• Use Case III: Smart Home
A Vision of Pervasive Services

- Architectural Overview
A Vision of Pervasive Services

- Requirements for Privacy Aware Pervasive Services
  - No external Data Misuse – Secure Architecture
  - No internal Data Misuse – Privacy-friendly Services
Summary

- A vision of Pervasive Services
- Secure Architecture for Pervasive Service Provisioning
- Privacy Model
- System Requirements
Secure Architecture for pervasive Service Provisioning

- Architectural Overview

Sign Bundles with JarSigner

Bundle Privacy Metadata

Bundle Signature

Unsecure Com. Channel

Service Privacy Metadata

Services Repository

Secure Com. Channel

Local Logs

Local Policies

Certificate Database

Service Box

Signer's Public Key Certificate

Terminal 1

Terminal 2

Signer's Private Key
Secure Architecture for pervasive Service Provisionning

- Discovery Protocol for Bundles
Secure Architecture for pervasive Service Provisioning

- Discovery Protocol for Services
Secure Architecture for pervasive Service Provisioning

• Security Analysis
  – Bundle Deployment
    • Bundle Digital Signature
    • Integrity, Authentication of the Publisher
    • No confidentiality
    • Client Side Control
  – Service Use
    • Secure Communication Channel, as SSH
    • Integrity, Authentication and Confidentiality must be checked at the server side AND at the client side
Summary

- A vision of Pervasive Services
- Secure Architecture for Pervasive Service Provisioning
- Privacy Model
- System Requirements
Privacy Model

• Formal Foundations
  – Missing Semantics:
    Attributes and associations to individuals
    The context in which they are processed and evaluated
  – Requirements (for practical applicability)
    Handling of non-static spreading of information
    Distributed modeling
    Information gathering through data-mining
Privacy Model

• Formal Foundations
  – Users Id – the users
  – Actions Act$_i$ – the services
  – Attributes A – the data that is gathered about a user by a service
  – Production Rules: to identify data mining risks
    • $R_p \subseteq \text{Set}(A_{\text{available}}) \times \text{Set}(A_{\text{deduced}})$
Privacy Model

Building blocks for implementation
- Services and actions
- Users
- Data Attributes
- Administrative Domains

Definition of Privacy-Aware Partial Policy
- Well-defined set of actions
- Data attributes
- Administrative Domains and their trust-level
Summary

- A vision of Pervasive Services
- Secure Architecture for Pervasive Service Provisioning
- Privacy Model
- System Requirements
System Requirements

• Remote Service Implementation
  – Openness and Transparency
    Users can observe the fulfilment of privacy policies
    Technically unaware people can rely on others
    like Open-Source approach
  – Enforcement rather difficult (according to Hilty, 2005)
    Enforceable obligations
    Observable obligation
    Other obligations
  – Human actions are required
    Service certification – before release
    Service audit – during runtime, and in case of court trial
System Requirements

- User Platform
  - 3 steps-control: validation during installation, monitoring, and logging
  - Sandboxing: Java Permissions, Virtual OSGi for multi-provider support
System Requirements

- Isolation between Bundles for Privacy policy enforcement
  - Services are bound to a privacy profile
    - which bundles are allowed to access it
    - which bundles it is allowed to access
    - specific rights (see services/use service)
  - Through OSGi Services only (no package-level access)
  - All Services provided by a given bundle must share the same privacy profile
  - OSGi Service Permission not sufficient
    - Do not take the privacy meta-data into account
System Requirements

- Isolation between Bundles for Privacy policy enforcement
  - OSGi Context must be modified to allow access to authorized services only: definition of 'RestrictedContext', which contains a policy driven filter that can not be modified by the bundles (better performance)
  - OR
  - Service Conditionnal Permissions must be extended to take the privacy model into account (slight extension of the current specification)
Conclusions

• Contribution
  – Framework for privacy aware service integration
  – Privacy meta-data part of the bundle/service meta-data
    • Privacy aware service integration can be performed as other types of service integration
  – System requirements

• To be done
  – Integration of the model with the use cases
Questions?