Contextual Privacy Management in Extended RBAC Model

Nabil Ajam,
Nora Cuppens, Frédéric Cuppens
24 september 2009

Plan

- **Introduction**
- Motivation to use RBAC models
- Privacy requirements as OrBAC contexts
- Use case
- Conclusion

Background

- **Enhanced services extensively use sensitive information**
- **New services threaten user's privacy**
  - More and more acceptance of such services: community service, location service...
- **International organisations tend to institute privacy principles**
  - Common acceptance of the OECD requirements (1980)

Privacy definition

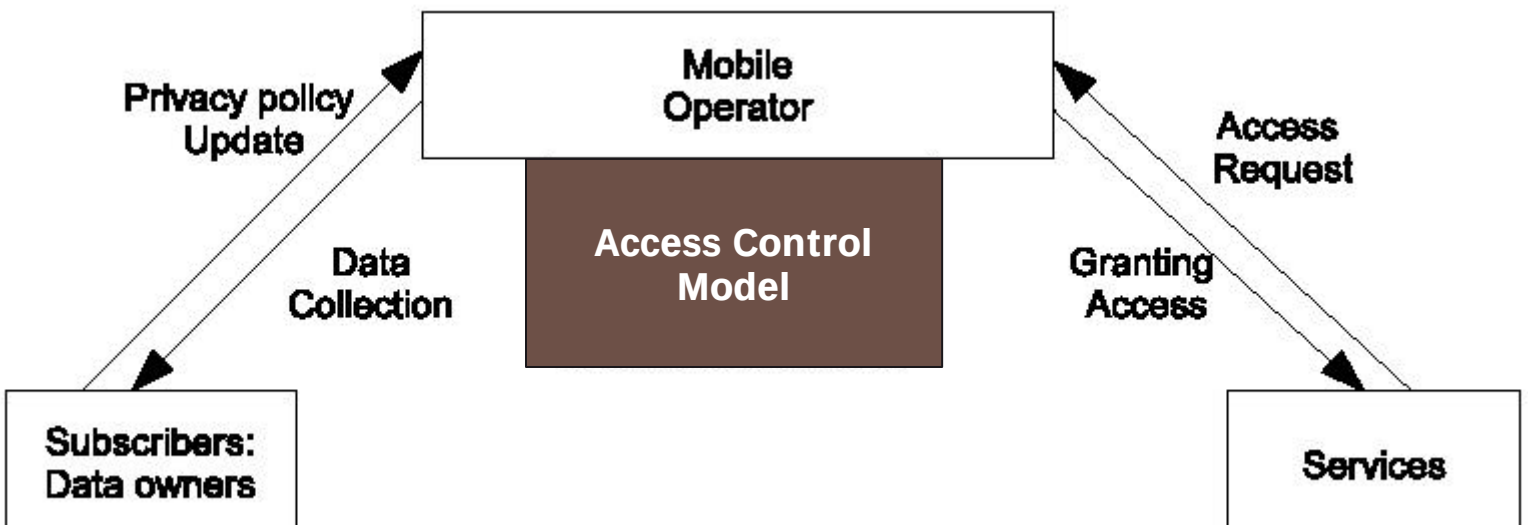
- **Sensitive data**
  - Any data that can be used to identify directly or indirectly a physical person
- **Privacy is**
  - The demands from individuals, groups and institutions to determine by themselves when, how and to what extent information about them is to be communicated to others
- **Data owner**
  - The subject, who the sensitive data is referred to

Context of work: Three actors for LBS

- **Operator is the organization that collects, stores and discloses private information about subscribers**
- **Assumption: Subscribers trust the operator organisation**

- **Subscribers can define the privacy policy**
  - Authorized service providers
  - Different object accuracies
  - Purpose as user-declared context
    - A set of access objectives declared by the data owner
  - Provisional obligation
  - Consent requirement before delivering data

Motivation



- Location services are able to track subscribers continuously
- Idea: Define one model for access control and privacy control

Plan

- Introduction
- **Motivation to use RBAC models**
- Privacy requirements as OrBAC contexts
- Use case
- Conclusion

Related works

- **P-RBAC (Purpose-based RBAC)**
  - A dedicated langage to express privacy conditions
  - Definition of obligations

- **Purpose-Based Access Control and PuRBAC (Purpose-Aware RBAC)**
  - Intended purposes
  - Access purposes
  - Three types of conditions: Constraints, pre-obligations, post-obligations

Motivation

- **Common acceptance of RBAC model to express security policy**
  - Reuse existing model
  - One model for access and privacy control
- **Extension of RBAC model**
  - Support of dynamic and environment parameters through contexts
  - Possibility to integrate the majority of privacy requirements
  - Example: OrBAC model
- **Integrate privacy for NGN services**

OrBAC model

- **Two abstraction levels**
  - Concrete: subject, action, object
  - Abstract: role, activity, view
- **Policy specification based on the abstract entities: permission, prohibition, obligation, dispensation**
  - Permission(org, role, activity, view, context)
- **Five context types:**
  - Spatial
  - Temporal
  - Provisional
  - User-declared
  - Prerequisite

Plan

- Introduction
- Motivation to use RBAC models
- **Privacy requirements as OrBAC contexts**
- Use case
- Conclusion

Privacy requirements

- **OECD guidelines (initially concern transborder flow), which are adopted by western countries**
  - Collection limitation (owner consent)
  - Data quality (need to know)
  - Purpose specification
  - Use limitation (owner consent)
  - Security safeguards
  - Openess
  - Individual participation
  - Accountability

Privacy requirements : Consent

- **Data owner can require his consent before delivering his location by the operator**

- **Consent is needed either :**
  - Before data collection
  - After data collection

- **User preference is stored within the « consent preference » view by the operator**

Privacy requirements : Consent

- **Consent object attributes are :**
  - Requestor
  - Target
  - Data-owner
  - NeedConsent

- **User consent is triggered when**

$$Hold(org, s, \alpha, o, Consent\_context) \leftarrow Use(org, cp, Consent\_preference)$$
$$\wedge Requestor(cp, s) \wedge Target(cp, o) \wedge Data\_owner(cp, do) \wedge NeedConsent(cp$$
$$\wedge Consent\_response(Org, do, s)$$

Privacy requirements: Accuracy

- **Users can define several accuracies for the same sensitive data**
- **Sensitive data are modelled by an object hierarchy based on the accuracy**
- **Object derivation: compute objects based on the accurate root object**

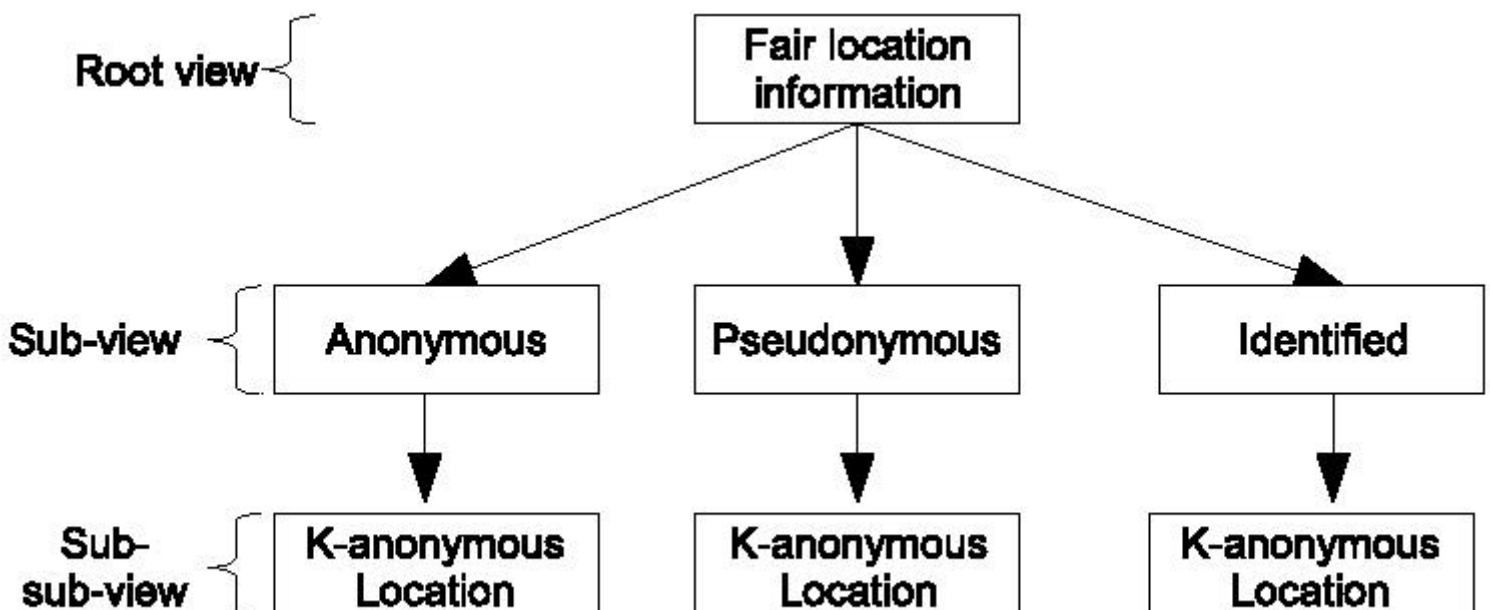
- **Two accuracy levels**
  - Anonymity level
  - Cloaked sensitive data (position)
    - K-anonymity algorithm

Privacy requirements: Accuracy

- **Anonymity is considered part of the object accuracy**
  - K-anonymity algorithm

- **Anonymity level depends on requestors**
  - Each data owner can define several objects

Privacy requirements: Accuracy



Privacy requirements : purpose definition

- **Purpose as user-declared context**

- **Definition of purpose context:**
  - Recipient: who takes advantage of the declared purpose
    - Service providers

  - Data owner defines purposes

Provisional obligation

- **Enforce usage control after delivering locations**
- **Obligation**
  - Activate condition: when obligation is needed
  - Violation condition
- **Obligation is triggered by a provisional context activation**

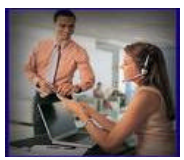
$$Hold(operator, s, \alpha, o, Notification) \leftarrow Use(operator, l, log) \wedge Log\_actor(l, s) \wedge Log\_action(l, \alpha) \wedge Log\_target(l, o) \wedge Log\_context(l, Notification)$$

Plan

- Introduction
- Motivation to use RBAC models
- Privacy requirements as OrBAC contexts
- **Use case**
- Conclusion

Location based service

User: Data owner



Requestor: service provid

Cellular network:
Location data

Role: fleet_management_

Purpose: Optimise_route
Consent: Yes
Accuracy: Anonymous data
Obligation: User notification

Plan

- Introduction
- Motivation to use RBAC models
- Privacy requirements as OrBAC contexts
- Use case
- **Conclusion**

Conclusion

- **Contribution**
  - Several privacy requirements
    - Accuracy
    - Consent
    - Purpose
  - Modelling privacy requirements
    - Consent context
    - Provisional context
    - User-declared context
- **Future works**
  - Model other privacy principles
    - Remedies, retention, user participation
  - Policy administration
  - Privacy policy deployment

Thanks