A Privacy Aware Localization Service for Healthcare Environments

Thomas Scheffler

scheffler@beuth-hochschule.de

BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN
University of Applied Sciences

IETF 96, Berlin – 19. July 2016

Table of Content

Motivation and Idea

- Privacy aware data-sharing
- Data Owner controlled privacy policies
- Sticky Policies

Policy Languages for Localization Data

- XACML
- GEOPRIV

Summary

Motivation

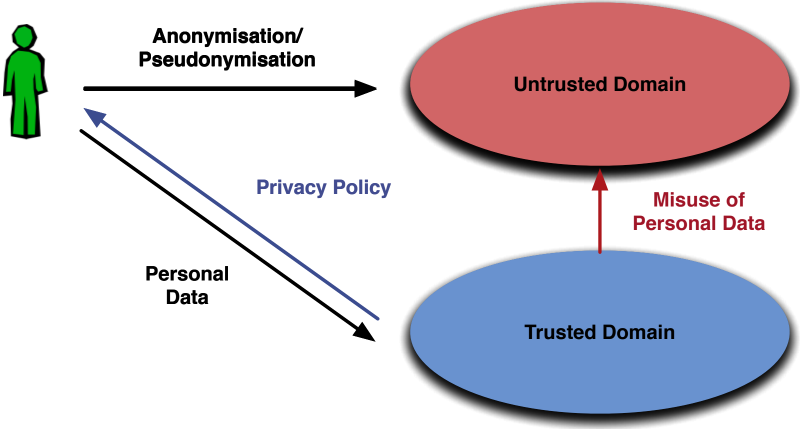
Definition (**Privacy:**)

"...the right of individuals to determine for themselves **when**, **how** and **to what extent** information about them is communicated to others."

P. Ashley and G. Karjoth, 2003

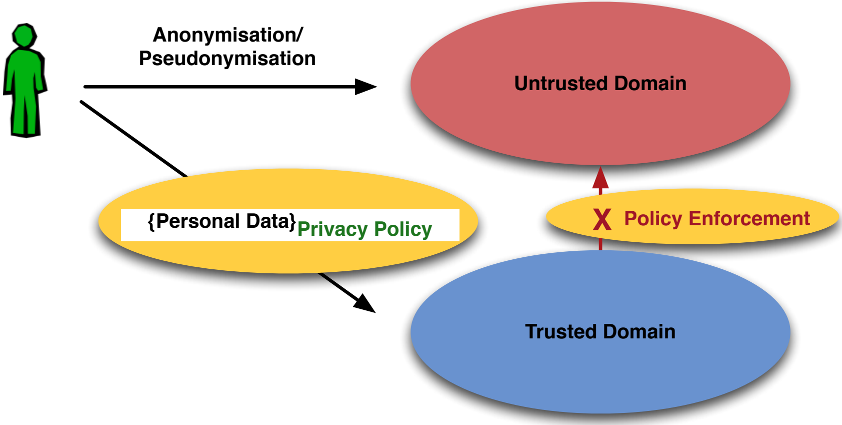
Motivation

Data sharing scenarios



Motivation

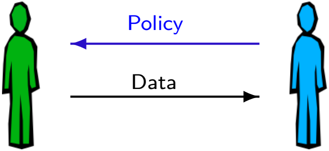
Data sharing scenarios



Controlling Data Access Policies

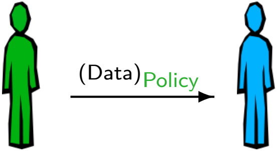
Data User controlled Policies

- The Data User specifies and publishes the access and use policy for private data.
- The Data Owner has to trust this policy and releases his/her data.



Data Owner controlled Policies

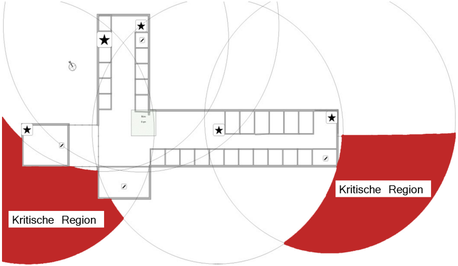
- The Data Owner specifies the access and use policy for data.
- The Data User enforces this policy.



Use case

KopAL: Assistance for Patients with Dementia

- Project at University Potsdam in 2011
- Localization of patients that have lost orientation
- Notification of nursing staff about dangerous patient movement
- Localization of lost or misplaced devices (requested by staff)



Data Privacy for Location Services

Question: How can the sensitive private location data of a patient be protected in the presence of different actors?

- Sensitive data stored as semi-structured XML-Documents
  - Location data
  - Access Policy
- Automated enforcement of authorizations
- (Distributed) Access Control Framework
  - Requests to resources must be evaluated at time of resource access
  - Deployment of trusted infrastructure

Sticky Policies

The Policy-Store holds:

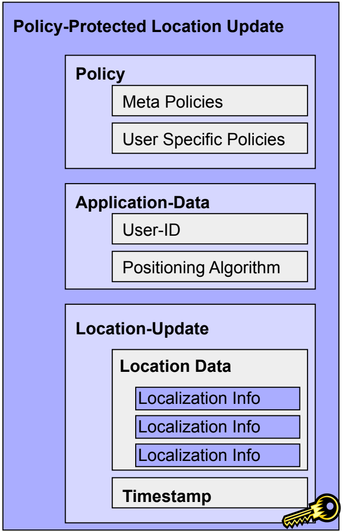
- Meta Policies
- User-generated Policies

Application data includes:

- User-ID
- Positioning Algorithm

The Location-Update contains:

- Location Data
- Timestamp



Policy-Protected Location Update

Policy
- Meta Policies
- User Specific Policies

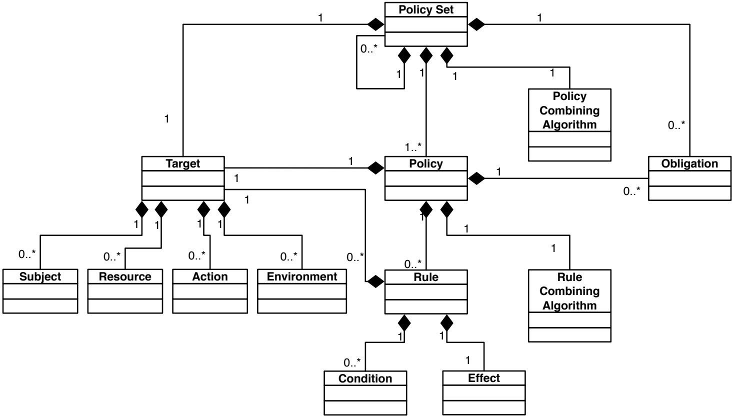
Application-Data
- User-ID
- Positioning Algorithm

Location-Update
- Location Data
  - Localization Info
  - Localization Info
  - Localization Info
- Timestamp

Policy Languages for Localization Data

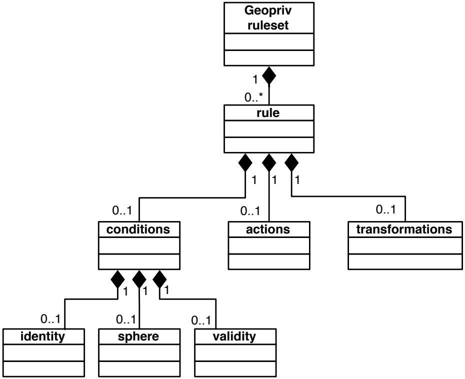
XACML - eXtensible Access Control Markup Language

- developed by OASIS, current version 3.0 (v2.0 shown here)
- Generic Policy Language, as well as Request/Response Language



GEOPRIV - Common Policy

- Developed by the Geopriv WG of the IETF, RFC 4745
- Targeted Policy Language for expression of localization policies



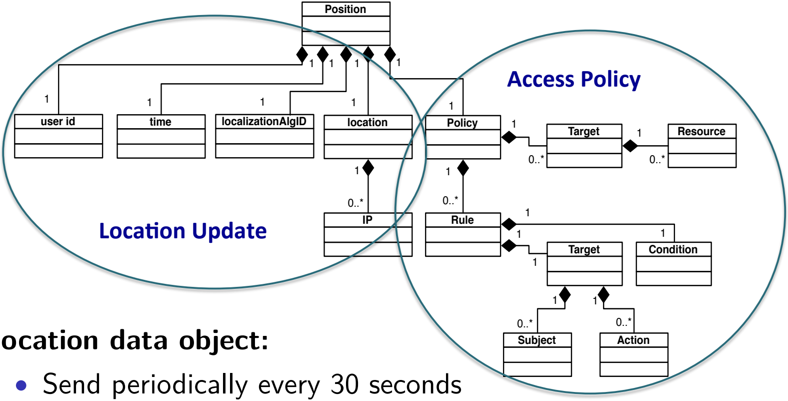
GEOPRIV - Common Policy

(Some) characteristics of Geopriv:

- Only positive authorization rules allowed
- Complete ruleset needs to be evaluated
- No ability to explicitly specify purposes for data-use in policies
- Targeted expressions for location transformation (obfuscate, reduce precision, ...)
- Policy combining is narrowly defined:
  generates the union over the matching permissions in the rule-set, returning the maximum value across the permission-set

Any implementations?

Privacy protected data exchange for Location Updates



Location data object:

- Send periodically every 30 seconds
- Server only stores a short history of values
- Every location update contains complete policy
- Location update is encrypted using XML-Encryption

Summary

Summary

- Facilitate data sharing (trusting the data user to some extend)
- Policy definition by the *Data Owner*
- Policy description using an enforceable policy language
  - Sticky policies
  - Templates
  - Conflict resolution mechanisms
- Automatic enforcement by the *Data User*
- Data & Policy are sharable (extend may be defined by Policy)

Contact

Email: scheffler@beuth-hochschule.de

WWW: http://prof.beuth-hochschule.de/scheffler/

BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN

University of Applied Sciences