Mobile Adventure

International Workshop on Ubiquitous Access Control (IWUAC)
July 17, 2006

**Context-Aware Access Control**
Making Access Control Decisions Based on Context Information

Sven Lachmund, Thomas Walter, Laurent Bussard, Laurent Gomez, Eddy Olk

---

Mobile Adventure

**Motivation and Objective**

Classic access control schemes
- Role based
- Identity based
- ACL
- ...

Does not adapt to changes
→ Not that applicable to ubiquitous environments

Context-aware access control schemes
- Role based
- Identity based
- ACL
- ...

Adapts to changes
→ Requires context information representing the actual context

Examples:
Temperature
Location
Office hours
Health status
...
Mobile Adventure

Outline

• Approach
• Architecture
  – Message Filters
  – Authorisation Service
  – Context information Acquisition and Trust Service (CATS)
• Interaction of components
• Summary

Mobile Adventure

Approach

• Focus on access control to services in a SOA
• Middleware component for (mobile) devices
  – Security enforcement on message level
    • Includes access control
    • Rules defined on action offered by Web Service
    • Outside the application/service
  – Context information acquisition and analysis

• Elaborated in the European research project

MOSQUITO

Mobile workers’ secure business applications in ubiquitous environments
Ambient security architecture: Policy enforcement + policy decision [+ security services]

CATS = Context information Acquisition & Trust Service
Message Filters = Security SOAP Proxy

- Goals: secure exchanges in distributed system
  - WS-Security
    - Integrity + Authentication of origin
    - Confidentiality
    - Credential attachment
  - WS-Policy
    - Define message-level policies
    - Access Control

- How:
  - Filters
  - Proxy
  - Gateway

Output pipeline

SOAP
WS

Integrity Filter
Confidentiality Filter
Authorization Filter

SOAP
WS-Security

Credentials
XML encryption
XML D-Sig

---

Mobile Adventure
Architecture – Authorization Service

Server Device
Client Device

Ambient security architecture: Policy enforcement + policy decision [+ security services]

CATS = Context information Acquisition & Trust Service
Mobile Adventure
Authorization Service

- Makes access control decision
- Decision are influenced by
  - Security policy (XACML)
  - Content of SOAP message (e.g. called service and invoked method)
  - Requestor’s attributes (role, identity, credential)
  - Context information
    - Either attached to SOAP message as credential
    - Or acquired by Authorization service using CATS
- Example (non policy language conform)
  - Rule: Entity physician proven by credential issued by hospital may access patient-data-service method getPatientData if patient status is emergency

Mobile Adventure
Architecture - CATS

Ambient security architecture: Policy enforcement + policy decision [+ security services]
CATS = Context information, Acquisition & Trust Service
Mobile Adventure
CATS – Threats and Scope

- From perspective of mobile device

CIS is hosted/operated by a Context Information Service Provider (CISP)

Mobile Adventure
CATS – Trust Evaluation

- Trust evaluation makes trusted CI out of CI

CIS is hosted/operated by a Context Information Service Provider (CISP)
Ambient security architecture: Policy enforcement + policy decision [+ security services]

CATS = Context information, Acquisition & Trust Service
Mobile Adventure
Summary

- Context-Aware Access Control
  - Dynamically adjust to changes
  - Augment access control schemes by conditions taking context information in account
- Proposed middleware
  - Applies access control on message level
  - Takes credentials as proof of requestor’s attributes
  - Provides trusted context information
- Trusted context information
  - Trust relationship to context information service provider
  - Analysis of received context information