Semantic Access Control

Mariemma Yagüe, Antonio Maña
Computer Science Department
University of Málaga
e-mail: yague@lcc.uma.es
Agenda

- Introduction
- SAC, *Semantic Access Control Model*
- Semantic Integration of a PMI
- Example
- Implementation
- Conclusions
- Future Work
Agenda

- Introduction
- SAC, Semantic Access Control Model
- Semantic Integration of a PMI
- Example
- Implementation
- Conclusions
- Future Work
Traditional Access Control Schemes

DAC, *Discretionary Access Control*

- Multi-user DBs
  - Reduced number of previously known users.
  - Changes are not frequent.
  - Resources under a unique entity.
- Control based on identity.
  - Rules stating what a user can do or not.
Traditional Access Control Schemes

MAC, *Mandatory Access Control*
- Military environments
  - High number of users
  - Linear and Static Hierarchical classification.
- Control based on Security Levels.
  - Rules established by a central authority.
  - Definition of Security Levels
  - Allocation of levels to resources and users
Traditional Access Control Schemes

RBAC, *Role-based Access Control*
- Business. Corporative Intranets.
  - Hierarchical structures.
  - Access Permissions depending on the user position (role) in the hierarchy.
- Control based on roles played
  - Rules establishing permissions of access to roles.
  - Allocation of roles to users.
Open and Distributed Environments

❖ Heterogeneity
  • Open Access Control Scheme

❖ Interoperability
  • Separation of the Responsibilities of Authorization and Access Control

❖ Flexibility
  • Independence of the Application Domain

❖ Scalability
  • Completely Distributed Scheme

❖ Dynamism
  • Adaptation transparently and automatically
Agenda

- Introduction
- SAC, *Semantic Access Control Model*
  - *Semantic Policy Language*
- Semantic Integration of a PMI
- Example
- Implementation
- Conclusions
- Future Work
Basis for a New AC Model

Separation of responsibilities of Authorization and Access Control is widely accepted as a Flexible and Interoperable Solution

Semantic Integration of Authorization and Access Control Applications
## SAC, Semantic Access Control

<table>
<thead>
<tr>
<th><strong>PROVIDES</strong></th>
<th><strong>AVOIDS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>❚ Schema based on the concept of attribute</td>
<td>❚ Mandatory Previous Subscription</td>
</tr>
<tr>
<td>❚ Access based on semantics</td>
<td>❚ Mandatory Identification</td>
</tr>
<tr>
<td>❚ No ambiguity in policies</td>
<td>❚ Previous Establishment of Elements for the support of access control</td>
</tr>
<tr>
<td>❚ Semantic Correction</td>
<td>- Users Hierarchy</td>
</tr>
<tr>
<td>❚ Dynamic Allocation of Policies</td>
<td>- Roles</td>
</tr>
<tr>
<td>❚ Modularization</td>
<td>- Groups</td>
</tr>
<tr>
<td>❚ Parameterization</td>
<td>- Security Classification</td>
</tr>
<tr>
<td>❚ Reuse</td>
<td>- ...</td>
</tr>
</tbody>
</table>
Mechanisms in SPL, Semantic Policy Language

To reduce the AC policies definition complexity: *Modularity, Parameterisation* and *Abstraction*.

Modularity in SPL implies:

- The separation of specification in three parts:
  - access control criteria
  - allocation of policies to resources
  - semantic information (properties about resources and context)
- The abstraction of access control components
- The ability to reuse these access control components
Mechanisms in SPL

- **Access Control Criteria Specification (Policy)**: used to describe necessary conditions to get the access; they can be composed.
- **Policy Applicability Specification (PAS)**: used to relate policies to objects dynamically when a request is received.
- **Secured Resource Representation (SRR)**: used to describe semantic information about resources.

SPL Policy and PAS can be parameterised:
- This helps defining flexible and general policies and reducing the number of different policies to manage.
- Parameters are dynamically instantiated from semantic and contextual information.

Policies can be composed importing components of other policies without ambiguity.
- modular composition of policies based on the XPath standard.
Metadata in SPL

 Metadata applied at different levels:

- Semantic and contextual validation of access control policies.
- Dynamic policy allocation and instantiation.
- Creation of policies
  - For the specification and acquisition of certification rules
- Management of policies
  - Any change in the authorization rules or the context is detected and the consequences are revealed.
SAC, Semantic Access Control

- Attribute Certificate Based Approach.
- Supported by XML related technologies for metadata.
- Modular Language.
- Policy Composition.
- Parameterised Policies.
- Content-aware access control (content introspection).
- Means for the semantic integration of an external PMI.
  - Authorization becomes interoperable.
Agenda

- Introduction
- SAC, *Semantic Access Control Model*
- *Semantic Integration of a PMI*
- Example
- Implementation
- Conclusions
- Future Work
Semantic Integration of a PMI

PUBLIC KEY INFRASTRUCTURE

Authorization
Role, status,... social-economic attributes

Authorization

PMI: Source of Authorization (SOA)
Certificates a set of semantically related attributes

PKI: Certification Authority (CA)
Certificates only identity

Solution: Attribute Certificates
Semantic Integration of a PMI

SOAD Model (*Source of Authorization Description*)

- Describes the semantics of the certificates issued by the SOA.
- Describes relationships among the certificates
  - and between attributes certified by this SOA and others sources of authorization.
- Helps to the specification of access criteria.
- Enables the semantic validation.
Agenda

- Introduction
- SAC, *Semantic Access Control Model*
- *Semantic Integration of a PMI*
- *Example*
- Implementation
- Conclusions
- Future Work
Example: ACS DL

- Various Special Interest Groups (SIGs)
- ACS members can be members of the different SIGs, not mandatory.
- ACS publishes journals and newsletters, directly or through the SIGs.
- Newsletters can be accessed by the ACS members and also by people subscribed to them (ACS members or not).
- Journals can be accessed by users subscribed to them independently they are members of the ACS or not.
- If the journal is published by an Special Interest Group, all the members of that group can access that journal.
- An special subscription type called Portal grants access to every publication in the digital library.
Role structure must be predefined

A role for each journal

SIG1 members can play j2 and j3 roles

A role for portal

A role for ACS

A role for each newsletter

Role Hierarchy for the ACS Digital Library
<xml version="1.0" encoding="UTF-8">
  <Policy xmlns="http://www.lcc.uma.es/SAC Policy.xsd">
    <Parameter>PublicationName</Parameter>
    <Parameter>PublicationSOA</Parameter>
    <AccessRules>
      <AccessRule>
        <AttributeSet AttributeSetDescription="Suscripción a una publicación" AttributeSetName="Suscripcion">
          <Attribute Equivalence="Enabled">
            <AttributeName>Subscription</AttributeName>
            <AttributeValue>*PublicationName</AttributeValue>
            <SOA_ID>*PublicationSOA</SOA_ID>
          </Attribute>
        </AttributeSet>
      </AccessRule>
    </AccessRules>
  </Policy>
</xml>
<xml version="1.0" encoding="UTF-8"?>
<spl:PAS xmlns:spl="http://www.lcc.uma.es/SAC"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.lcc.uma.es/SAC pas.xsd">
    <spl:Policy>Journal.xml</spl:Policy>
    <spl:Object>
        <spl:ObjectLocation>http://www.acs.org/</spl:ObjectLocation>
        <spl:Conditions>
            <spl:Condition>
                <spl:PropertyName>PublicationType</spl:PropertyName>
                <spl:PropertyValue>Journal</spl:PropertyValue>
            </spl:Condition>
        </spl:Conditions>
    </spl:Object>
</spl:PAS>
Description of TOSEC journals

<?xml version="1.0" encoding="UTF-8"?>
<SRR ...xsi:schemaLocation="http://www.lcc.uma.es/SAC SRR.xsd" >
  <Property>
    <PropertyName>PublicationName</PropertyName>
    <PropertyValue>TOSEC</PropertyValue>
  </Property>
  <Property>
    <PropertyName>PublicationSOA</PropertyName>
    <PropertyValue>SIGSEC</PropertyValue>
  </Property>
  <Property>
    <PropertyName>PublicationType</PropertyName>
    <PropertyValue>Journal</PropertyValue>
  </Property>
  <Resource>http://www.acs.org/Journals/TOSEC/</Resource>
</SRR>
<?xml version="1.0" encoding="UTF-8"?>
<Policy ... xsi:schemaLocation="http://www.lcc.uma.es/SAC Policy.xsd">
  <AccessRules>
    <AccessRule>
      <AttributeSet AttributeSetDescription="Suscripción a una publicación" AttributeSetName="Suscripción">  
        <Attribute Equivalence="Enabled">  
          <AttributeName>Subscription</AttributeName>  
          <AttributeValue>TOSEC</AttributeValue>  
          <SOA_ID>SIGSEC</SOA_ID>  
        </Attribute>  
      </AttributeSet>
    </AccessRule>
  </AccessRules>
</Policy>
Semantics of the Attributes

<SOAD ... xsi:noNamespaceSchemaLocation="SOAD.xsd"
ValidFrom="2002-01-01T00:00:01" ValidUntil="2004-01-01T00:00:01">
  <SOA_ID>SIGSEC</SOA_ID>
  <ACDeclarations>
    <SOAAttribute>
      <AttributeName>SIGMember</AttributeName>
      <AttributeValue>SIGSEC</AttributeValue>
    </SOAAttribute>
    <SOAAttribute>
      <AttributeName>Subscription</AttributeName>
      <AttributeValue>SIGSECNewsLetter</AttributeValue>
    </SOAAttribute>
    <SOAAttribute>
      <AttributeName>Subscription</AttributeName>
      <AttributeValue>TOSEC</AttributeValue>
    </SOAAttribute>
  </ACDeclarations>
</SOAD>
Semantics of the Attributes

To be a member of the SIG on Security, SIGSEC, implies the subscription to the SIGSEC newsletters and to the TOSEC journal.
Example Conclusions

- RBAC model presents problems to adapt to changes.
  - Administrative overload.
- No every problem is easily modelled using RBAC.
- The SAC model enables to express in a more natural and simple way complex access control situations.
  - Simple, generic, reusable, dynamically instantiated specifications.
- The semantic integration of external authorization entities provides additional advantages to SAC.
Agenda

- Introduction
- SAC, Semantic Access Control Model
- Semantic Integration of a PMI
- Example
- Implementation
  - Management Mechanisms in SAC
  - Integration Mechanism of the PMI
- Conclusions
- Future Work
Administration

One of the main objectives of the SAC model is the ease of administration.

- Validation of the semantic and contextual correction.
- Reuse of components.
- Ease of implementation.
- Administrator Supporting tools.
  - Integrated environment with smart and visual edition, syntactic and semantic validation, control of changes, ...
- Authorization Management.
  - SOADs Client
Environment Window of the Policy Assistant

Policy Summary

Pas & SRR

SPL POLÍCIES

Results Information
Semantic Integration of PMI

ائه SOADs Management at the server and client side
- Publication / Localization
- History
- Caducity
- Edition on the Server and the Client side.
Semantic Integration of a PMI

SOADs Management System

SOADs Client
Agenda

- Introduction
- SAC, *Semantic Access Control Model*
- Semantic Integration of a PMI
- Example
- Implementation
- *Conclusions*
- Future Work
Conclusions

- Semantic Integration of Applications
  - of Authorization and Access Control.
- Access Control Model based on semantics of the contents and the application context.
- High level of Interoperability, Scalability, Flexibility, Adaptability, Applicability.
- Semantic Soundness.
- Ease of Administration.
- Avoids the registration phase.
Agenda

- Introduction
- SAC, *Semantic Access Control Model*
- Semantic Integration of a PMI
- Example
- Implementation
- Conclusions
- *Future Work*
Future Work

Delegation
- To maintain the control over the delegation process.
  - Establish semantics of the delegation.

DRM
- Extension of SPL to express rights over digital contents.
- Inclusion of new DRM functions in the XSCD infrastructure.

Application of SAC to new environments.
Thank you for your attention ;-) 

**Semantic Access Control**

Presented by: Mariemma Yagüe  
Computer Science Department  
University of Málaga  
e-mail: yague@lcc.uma.es