eXtensible Access Control Language (XACML)

Fatih Turkmen
fturkmen(at)disi.unitn.it
fturkmen(at)mit.edu

Visiting PhD Student, CSAIL, MIT
DISI, University of Trento
Outline

• eXtensible Access Control Markup Language (XACML)
  • Syntax
  • Architecture
• Industry Practices
• Weaknesses
• Available Implementations
• XACML & AIR
• References
XACML

• XML based access control language

• Simple Syntax, Strong Expressivity, Machine Processable

• OASIS standard

• Widely adopted both in industry and academia

• Many implementations (both open source and proprietary)
XACML (Cont.)

PolicySet

Rule

Target

Policy

Target
Rule/s
Obligation

Obligation/s

Subject/s
Resource/s
Action/s
Redrawn from “Anne Anderson, Sun Microsystems Laboratories, XML Community of Practice, 21 June 2006”
<Policy PolicyId="Policy0" RuleCombiningAlgId="Permit-Overrides">
  <Description>Sales Report Policy</Description>
  <Target/>
  <Rule RuleId="Report_Access" Effect="Permit">
    <Target>
      <Subjects>
        <Subject>Manager</Subject>
      </Subjects>
      <Resources>
        <Resource>Sales Report</Resource>
      </Resources>
      <Actions>
        <Action>Modify</Action>
      </Actions>
    </Target>
    <Condition>
      <SubjectAttributeDesignator AttributeId="Division" /> Sales Department
    </Condition>
  </Rule>
  <Rule RuleId="FinalRule" Effect="Deny"/>
</Policy>
Policy Enforcement Point (PEP): Responsible for making access control decision requests to PDP and the enforcement of the given decisions.

Policy Decision Point (PDP): Makes access decisions by evaluating the given request against matched policies.

Context Handler: Responsible for conversions between XACML canonical format and native formats

Policy Information Point (PIP): Source of content values for XACML attributes.

Policy Administration Point (PAP): Creates and manages the policy and policy sets.
XACML Runtime

1. policy
2. service invocation
3. request
4. request notification
5. attribute query
6. attribute query
7a. subject attributes
7b. Resource attributes
7c. Environment attributes
8. attributes
9. resource
10. attributes
11. response context
12. response
Industry Practices

• Adaptation to Business Requirements via Profiles (e.g. RBAC Profile, Web Services Profile, Privacy Profile)

• SAML supported authorization services

• Together with an Identity Management System (e.g. LDAP, OpenID)
Industry Practices (Cont.)

- Integration of XACML to products
Industry Practices (Cont.)

• FedoraCommons
  • General purpose repository system

• Health-care Systems
  • National Swedish Health Care
    (Axiomatics startup)

• Geospatial XACML
  • Protecting access to distributed geographic information
XACML Weaknesses

• Verbose syntax (XML)
  • Can easily get complex.
  • Scalability Issues

• Very basic structure
  • Needs profiles and schemas

• Some Issues listed for v3.0:
  • More general conclusions (yes, no ...)
  • Really generic architecture (so much to be done)
XACML Weaknesses (Cont.)

- Delegation problem
  - Administrative delegation is available

- Informal Syntax, difficult to analyze
  - Verification of Properties (e.g. SoD, Permissions)
  - Compatibility among different policies

- Enforcement is difficult
Available Implementations

- XEngine
- Permis
- XACML Enterprise
- XACMLLight
- Sun XACML
  (Many implementations based on it: GlobusXACML, Axiomatics)
- HerASAF
- Some out-of-date or proprietary ones
  (XACML.Net, Parthenon, AXESCON XACML 2.0 Engine)
AIR vs XACML

• AIR is logic-based, XACML is not (informal)
  → AIR (Phyton) can be serialized to XML??

• XACML is dedicated for access control, AIR seems more generic
AIR vs XACML (Cont.)

• Obligations can not be addressed in AIR?
  • The requirements to be met after the decision.

• No architectural (enforcement) model provided with AIR
## AIR vs XACML (Cont.)

<table>
<thead>
<tr>
<th>Constructs</th>
<th>XACML</th>
<th>AIR</th>
</tr>
</thead>
<tbody>
<tr>
<td>PolicySet, Policy, {Subject, Resource, Action, Environment}, Rule, Condition, Obligation</td>
<td>Policy, Pattern (Variable), Assertion, Rule, MatchedGraph</td>
<td></td>
</tr>
<tr>
<td>Usage</td>
<td>Suitable for offline/online control</td>
<td>More suitable for offline control (analysis)</td>
</tr>
<tr>
<td>Evaluation Mechanism</td>
<td>Request against Policy (Request - Response)</td>
<td>Forward Chaining (based on Policy and the generated data) Reasoning</td>
</tr>
<tr>
<td>Complexity</td>
<td>Low (both advantage and disadvantage)</td>
<td>High (both advantage and disadvantage)</td>
</tr>
<tr>
<td>Extensibility</td>
<td>Yes</td>
<td>??????</td>
</tr>
<tr>
<td>Conflict Resolution</td>
<td>Flexible Combining Algorithms</td>
<td>Left to the reasoner</td>
</tr>
</tbody>
</table>
References

• http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
• http://www.oasis-open.org/committees/download.php/27298/xacmlRefs-V1-84-1.htm
• http://www.cse.msu.edu/~feichen/xengine.html
• http://sec.cs.kent.ac.uk/permis/downloads/download.shtml
• http://code.google.com/p/enterprise-java-xacml/downloads/list
• http://sourceforge.net/project/showfiles.php?group_id=224175
• http://sourceforge.net/cvs/?group_id=73884
• http://www.herasaf.org/development.html
• http://www.fedora-commons.org/about/
Shoot with Questions !!!