Requirements for policy-management in distributed systems

Policy workshop
Sun Microsystems
21 Feb 2003
Types of policy

• Authorization
  – Is this request properly authorized?
• Cryptographic security
  – Does this request have the required security attributes?
• Privacy
  – Is the requested disclosure properly authorized?
• Trust
  – Is this key acceptable for this purpose?
• Others
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:and">
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
    <ResourceAttributeDesignator AttributeId="wssqop:key-management-algorithm" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">Ds#rsa-sha1</AttributeValue>
  </Apply>
</Apply>

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:integer-greater-than-or-equal">
  <ResourceAttributeDesignator AttributeId="wssqop:key-size" DataType="http://www.w3.org/2001/XMLSchema#integer"/>
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#integer">1024</AttributeValue>
</Apply>
</Apply>
Alternative view

• Policy instances contain data:-
  – Requirements
  – Capabilities
  – Preferences
  – Properties
  – Features

• “This service supports English” ≡ “Is this request in English?”
Application points

- Receive: Cryptographic security policy
- Process: Authorization policy
- Forward: Privacy policy
Questions a service-consumer may ask

Does my request satisfy the provider’s requirements?
How can I form a request that satisfies the provider’s requirements?
How can I find out what the provider’s requirements are?
Are the provider’s requirements compatible with my requirements?
How can I form a request that satisfies both the provider’s requirements and my requirements?
Solving policy

- policy
  - translates to execution instructions
  - conforms with message
  - produces
## XAMPL

<table>
<thead>
<tr>
<th>WSPF</th>
<th>XACML</th>
<th>BPEL4WS</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;All&gt;</td>
<td>&lt;Apply and&gt;</td>
<td>&lt;sequence&gt;</td>
</tr>
<tr>
<td>&lt;OneOrMore&gt;</td>
<td>&lt;Apply or&gt;</td>
<td>&lt;switch&gt;</td>
</tr>
</tbody>
</table>
Combining consumer and provider policies

(policy1) -> (combine) -> (renormalize) -> (policy3)

(provider policy) -> (combine) -> (policy3)

(consumer policy) -> (policy2)
Combining policies

• All component policies MUST be satisfied
  <and>
  <policy1/>
  <policy2/>
  </and>

• Any one component policy MUST be satisfied
  <or>
  <policy1/>
  <policy2/>
  </or>
Renormalization

• Sample rules
  – Collapse identical adjacent operators
  – Reorder a sequence
  – Combine identical set operators
  – Combine identical inequality operators
XAMPL

<and>
<and>
...
</and>
<and>
...
</and>
</and>

<superset a>
b
c
</superset>
<superset a>
c
d
</superset>

<greater-than a>
b
</greater-than>
<greater-than a>
c
</greater-than>
<greater-than a>
max{b,c}
</greater-than>
Policy for responses

service consumer

PRP

PDP

PEP

service provider

decision request

decision

decision

policy

service response
Policy distribution

- **WSDL**
  - Provider policy
  - `<wsdl:operation>` element
- **SOAP**
  - Consumer policy
  - `<wsse:security>` header element
- **LDAP**
  - Attribute of target entry
- **HTTP**
  - ?
## Requirements and capabilities

<table>
<thead>
<tr>
<th></th>
<th>Form of message prevents processing</th>
<th>Form of message permits processing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider returns Fault</td>
<td>REQUIRE</td>
<td>REJECT</td>
</tr>
<tr>
<td>Provider processes message</td>
<td>SUPPORT</td>
<td>SUPPORT</td>
</tr>
</tbody>
</table>
REJECT

<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:not">
  <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:anyURI-superset">
    <ResourceAttributeDesignator AttributeId="wssqop:encryption-scope"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
    <AttributeValue
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      //record/patient/patient-number
    </AttributeValue>
  </Apply>
</Apply>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:anyURI-superset">
  <ResourceAttributeDesignator AttributeId="wssqop:encryption-scope"
    DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
</Apply>
Preferences

• Some alternatives may be preferable to others
  – E.g. lower processing cost

• List options in order of preference?
Miscellaneous

• Sequential application of requirements
  – E.g. sign then encrypt the data plus signature
• Attributes identified by name or location
• Policy specifies behaviour in event of unavailable attributes
• Mechanisms for locating and retrieving policies
Summary

- Publish provider-policy for request
- Transfer consumer-policy for response
- Combine provider and consumer policies
- Translate to execution instructions
- Express capabilities as well as requirements
- Express preferences
- Identify result of an execution step
- Use single formal logic system
  - Aids combining, renormalization and analysis