

An Introduction to XACML

Nurmamat. Helil

nur@is.pku.edu.cn

11th March 2005

Outline

- 1 Introduction to XACML
- 2 XACML Processing Environment
 - XACML Processing Environment
 - An Example: Access Control Rule
 - Example Deployment
 - Conflict Resolution
- 3 Related Work

Introduction to XACML

- The eXtensible Access Control Markup Language is an OASIS Standard
- XACML is a general purpose authorization policy language
- Follows the PEP/PDP model
- Essentially a tree of boolean combinations of predicates
- Provides powerful mechanisms like combining and retrieval
 - Supports distributed, decentralized policy

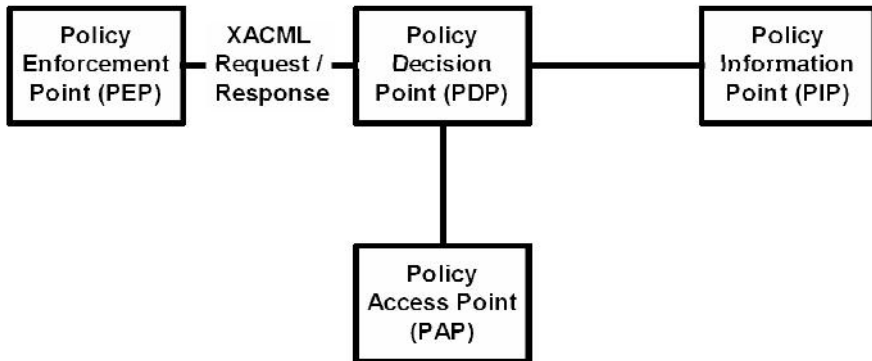
Standardization Motivation

- Access to resources must be constrained.
- The security policy of an enterprise is complex, and enforced at many points.
- Implemented by configuration at every point policy changes are expensive and unreliable.
- Consolidated policy view impossible.

What XACML Provides

- Policy language
- Request and Response language
- Semantics for processing policies and determining applicability to requests
- Standard data-types, functions, and combining algorithms
- Extensibility and flexibility

XACML Protocol



XACML Protocol

- 1 The Policy Administration Point (PAP) creates security policies and stores these policies in the appropriate repository.

XACML Protocol

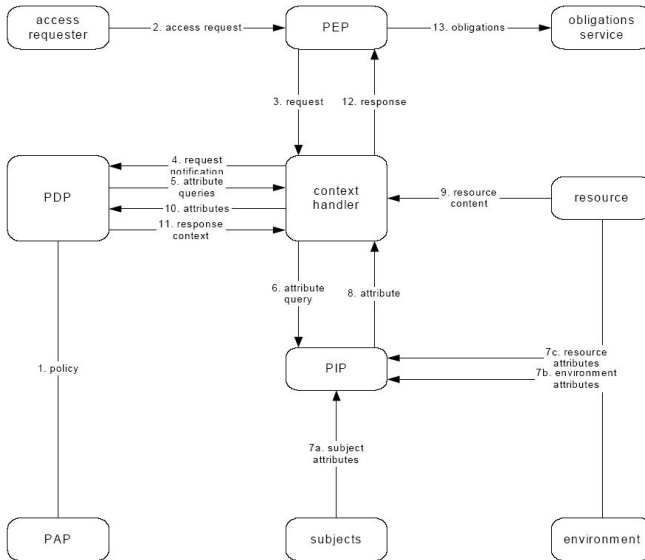
- 1 The Policy Administration Point (PAP) creates security policies and stores these policies in the appropriate repository.
- 2 The Policy Enforcement Point (PEP) performs access control by making decision requests and enforcing authorization decisions.

XACML Protocol

- 1 The Policy Administration Point (PAP) creates security policies and stores these policies in the appropriate repository.
- 2 The Policy Enforcement Point (PEP) performs access control by making decision requests and enforcing authorization decisions.
- 3 Policy Information Point (PIP) serves as the source of attribute values, or the data required for policy evaluation.

XACML Protocol

- 1 The Policy Administration Point (PAP) creates security policies and stores these policies in the appropriate repository.
- 2 The Policy Enforcement Point (PEP) performs access control by making decision requests and enforcing authorization decisions.
- 3 Policy Information Point (PIP) serves as the source of attribute values, or the data required for policy evaluation.
- 4 The Policy Decision Point (PDP) evaluates the applicable policy and renders an authorization decision.



XACML Protocol

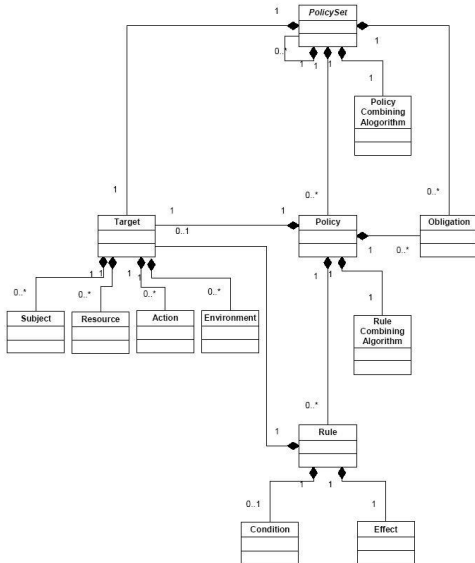
- XACML Request
 - Subject:
 - Resource:
 - Action:
- XACML Response
 - Permit
 - Permit with Obligations
 - Deny
 - NotApplicable
 - Indeterminate

XACML Protocol

Environment:The set of attributes that are relevant to an authorization decision and are independent of a particular subject, resource or action

Rule Combining Algorithm:The procedure for combining decisions from multiple rules

Obligation:An operation specified in a policy or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision



An Example: Access Control Rule

- Permit "John" to "Open" the "Door".
 - Entity: "John"
 - Action: "Open"
 - Resource: "Door"

An Example: Access Control Rule

```
<Rule RuleId="" Effect="Permit"> <Description>Permit John to Open the Door</Description>
  <Target>
    <Subjects><Subject>
      <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">John</AttributeValue>
        <SubjectAttributeDesignator
          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </SubjectMatch>
      </Subject></Subjects>
    <Resources><Resource>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">door</AttributeValue>
        <ResourceAttributeDesignator
          AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
        </ResourceMatch>
      </Resource></Resources>
    <Actions><Action>
      <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">open</AttributeValue>
        <ActionAttributeDesignator
          AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
          DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action></Actions>
    </Target>
  </Rule>
```

An Example: Access Control Rule

```
<ActionMatch  
  MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">  
  <AttributeValue  
    DataType="http://www.w3.org/2001/XMLSchema#string">open</AttributeValue>  
  <ActionAttributeDesignator  
    AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"  
    DataType="http://www.w3.org/2001/XMLSchema#string"/>  
</ActionMatch>
```

Example Deployment

- Internet Website for Customers
- Extranet Website for Partners
- Intranet Website for Employees
- Web Services based Applications
- Any Enterprise Application
- As a component of the Grid

conflict Resolution Policy

1 Deny-overrides

conflict Resolution Policy

- 1 Deny-overrides
- 2 Permit-overrides

conflict Resolution Policy

- 1 Deny-overrides
- 2 Permit-overrides
- 3 First applicable

conflict Resolution Policy

- 1 Deny-overrides
- 2 Permit-overrides
- 3 First applicable
- 4 Only-one-applicable

Related Work

Irini Fundulaki and Maarten Marx, "**Specifying Access Control Policies for XML Documents with XPath**," June 2004.

-How XPath can be used to specify the semantics of an access control policy for XML documents.

-XPath has great advantages: it is standard technology, widely used and it has clear and easy syntax and semantics.

Related Work

Ernesto Damiani, Sabrina De Capitani di Vimercati, Cristiano Fugazza, et al. **"Extending Policy Languages to the Semantic Web,"** 2003

how XACML can be extended to specify access control requirements about subjects and resources in terms of the rich ontology based metadata describing them.

- resource domain ontology,
- subject domain ontology,

Related Work

Elisa Bertino and Anna C. Squicciarini, **"A Flexible Access Control Model for Web Services,"** 2004

- Access request that can be accepted, either totally or partially, is said to be compliant.
- This work mainly focuses on the negotiation issue,

Related Work

Andreas Matheus, **"How to declare access control policies for XML structured information objects using OASISeXtensible Access Control Markup Language (XACML),"** 2005

-How access control restrictions can be declared using XACML and XPath. fine grained access control policies, multiple policies can be applicable.

-This paper also focuses on specifying the ground of policy inconsistencies and how to solve them.

Thank You