Using Subject- and Object-specific Attributes for Access Control in Web-based Knowledge Management Systems

Gerald Stermsek, Mark Strembeck, Gustaf Neumann
Vienna University of Economics and BA
{firstname.lastname}@wu-wien.ac.at
Presentation Overview

- Web-based Knowledge Management
- Basic Approach
- Resource Description Framework
- High-level Architecture
- Example
- Summary
Web-based Knowledge Management

- Gathering, organizing and disseminating information
- Advantages of Web-based IS: e.g. interoperability, extensibility, possible integration with web service, Web-based user interface
- Well established standards: e.g. XML, RDF, HTTP
- Semantic Web and RDF
- Sensitive information requires security management
Basic Approach

- Traditional Access Control: <subject, operation, object>
- ID-based systems vs. attribute-based systems
  - Use RDF to add additional attributes to entities
  - Enforce access control based on attributes
  - Attribute assignment may be distributed
  - Local access control decisions
- Example Scenarios:
  - AC directly based on subject- and object attributes
  - Assignment of permissions and/or roles based on subject attributes
RDF example

```xml
<?xml version="1.0"?>
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:attributes="http://nm.wu-wien.ac.at/rdf/attributes#">...
  <rdf:Description rdf:about="http://nm.wu-wien.ac.at/rdf/entities#PublicKey25097">
    <rdf:type rdf:resource="http://nm.wu-wien.ac.at/rdf/attributes#Subject"/>
    <attributes:nationality>Austrian</attributes:nationality>
    <attributes:birthyear>1977-07-07</attributes:birthyear>
    <attributes:project>Project X</attributes:project>
  </rdf:Description>
  ...
</rdf:RDF>
```
High-level Architecture

Policy Management Tool

Policy Decision Point (Access Control Monitor)
  - provide policy rules
  - ask for access decision

Attribute Validator
  - validation request
  - validation result

RDF Parser
  - uses

Policy Enforcement Point (e.g. a Web Server)
  - issue access request

Client
Architecture with KMS
Summary

- Knowledge management in web-context
- Well established standards
- Sensitive information needs access control
- Distributed systems: “ID only” vs. attributes
- Use attributes to render access control decisions
- Approach based on subject- and object-specific attributes
- Attributes are defined via RDF statements