Using XACML for access control in Social Networks

Anna Carreras, Eva Rodríguez, Jaime Delgado

Distributed Multimedia Applications Group (DMAG)
Universitat Politècnica de Catalunya (UPC)

W3C Workshop on Access Control Application Scenarios
Luxembourg, 17 November 2009
RESEARCH TOPICS

Creation, management and distribution of multimedia content in a secure and interoperable way

• Electronic commerce of multimedia services and products
• Metadata interoperability and ontologies
• Security, privacy and digital management of rights along the content life cycle
• Multimedia search
• Context handling and semantics
• Event reporting
• Privacy and rights in online social networks
• Contribution to Standardization: MPEG, JPEG, …
Contents

- Context and motivation
- Open issues on access control policy languages for Social Networks
- Our approach
  - Interoperability with content-associated policies based on XACML
  - Rights Expression Languages, Policy languages and Social Networks
  - Negotiating access control rules using XACML
  - Semantic interoperability
- Conclusions
Context and motivation

- Web 2.0 (Social Networks) → PRIVACY

- Privacy needs to be protected!

- *Our work done so far on Social Networks*

- *Issues to be solved*
Context and motivation

- Our work done so far on Social Networks:
  - Current privacy policies
  - Identification of useful elements of DRM systems
  - Implementation of privacy policies (XACML, MPEG-21 REL, ODRL)
  - Interoperability of RELs based on XACML
  - Privacy model (context-aware applications)

- Issues that need to be solved:
  - Policy languages limitations for Social Networks
  - Interoperability among different policy languages
Open issues on access control policies languages for SNs

- **Access control policies languages limitations for SNs**
  - New type of “resources” need to be protected (relationships, events)
  - High degree of expressiveness is demanded by users (preferences)
  - Policy expressions mainly depend on the access context
  - Lack of a standard format expressing SNs context

- **Lack of semantic interoperability**
  - Different services, different access control policies languages, different contexts

- **Lack of control for “third parties” applications**
  - SNs’ users also need to control them
  - Access control models could be based on symmetric level of trust and have negotiation capabilities
Interoperability with content-associated policies based on XACML

- Users don’t need to share all their data with the Service (i.e. Social Network) Provider
Demo application

- Facebook application to include protected content
- Linked to external system (outside Facebook)
- Licenses/policies specification for the content
- External system authorization

**VIDEO**

http://dmag.ac.upc.edu/downloads/xmerjd_virtualgoods09.avi
Digital Rights Management (DRM) systems enable the management of content through the complete digital value chain:

- Content creation, adaptation, aggregation
- Distribution, superdistribution, offers
- Content consumption

Rights Expression Languages (RELs) were devised to express the terms and conditions of use of content.

Policy languages exist to define which entities have access to which resources.

**SNs requirements?**
Social Networks provide:
- User (& relationships & actions) information
- Sharing of user content
- ...

SNs need languages for the definition of content & user info usage rules (and their enforcement)
- Control the usage (distribution, consumption, adaptation, negotiation, etc.) of personal data and digital content generated by the users

Candidate languages:
- Policy languages (from Access Control)
- Rights Expression Languages (from Content Mngnt. & Prot.)
Policy languages & Social Networks

- SNs can use policy languages to define which entities have access to which resources

- *Do current policy languages (e.g. XACML) support negotiation, personal data management, and can express complex content & user info usage rules?*
  - Example of content usage rule:
    
    “*Only my workmates can see the company Christmas Dinner photo album during this month*”

- The accomplishment of this rule implies knowledge about users (“workmates”)

Rights Expression Languages & SNs

- RELs express the terms and conditions of use of content through the complete digital value chain

- *Do RELs support negotiation, personal data management, and can express complex content & user info usage rules?*

- Current RELs cannot express complex content usage rules needed in SNs
  - Previous example
  - Extensions must be defined with new rights, conditions, user characteristics, …
<Policy>
  <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:SR1" Effect="Permit">
    <Target>
      <Subjects>
        <Subject>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">Alice workmates group</AttributeValue>
        </Subject>
      </Subjects>
      <Resources>
        <Resource>
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">/vc:ChristmasDinner</AttributeValue>
        </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">view</AttributeValue>
          </ActionMatch>
        </Action>
      </Actions>
      <!-- Only during January 2010 -->
    </Target>
  </Rule>
</Policy>
Architecture for REL → XACML translation
ODRL Example license
  <PolicySet>
    <Policy id="examplePolicy">
      <Title>Example Policy</Title>
      <RuleSet>
        <Rule id="SimpleRule1" Effect="Permit">
          <Target>
            <Subjects>
              <SubjectMatch />
            </Subjects>
            <Resources>
              <ResourceMatch />
            </Resources>
            <Actions>
              <ActionMatch />
            </Actions>
          </Target>
          <Condition>
            <VariableReference />
          </Condition>
        </Rule>
      </RuleSet>
    </Policy>
  </PolicySet>
</Policy>
MPEG-21 to XACML translation

```xml
  <Rule>
    <Title>Restrictions Object Title</Title>
    <Description>Restrictions Object Title</Description>
    <VariableDefinition>
      <VariableReference Variables="000000001" />
    </VariableDefinition>
    <RuleDefinition>
      <Term>
        <VariableReference Variables="000000001" />
      </Term>
      <Operator>And</Operator>
    </RuleDefinition>
    <Condition>
      <VariableReference Variables="000000001" />
    </Condition>
    <Effect>Permit</Effect>
  </Rule>
</Policy>
```
Negotiating access control using RELs

- RELs can be used to express offers
  - MPEG-21 REL, ODRL, ...
- Users propose to others the usage of their content according to the rights and conditions that they negotiate
- MPEG-21 REL example:
Negotiating access control using XACML

<Policy>
  <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:OF1" Effect="Permit">
    <Target>
      <Resources> <Resource>
        <Rule RuleId="urn:oasis:names:tc:xacml:2.0:example:VW1" Effect="Permit">
          <Target>
            <Resources> <Resource>
              ...<AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">/vc:video</AttributeValue>
              ...</Resource> </Resources>
            <Actions> <Action>
              <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue Data="http://www.w3.org/2001/XMLSchema#string">view</AttributeValue>
                ...
              </Action> </Actions>
            </Target>
          </Resource>
        </Target>
      </Rule>
    </Target>
  </Rule>
</Policy>
Semantic Interoperability

- Current existing ontologies
  - Social Networks → Friend Of A Friend (FOAF)
  - Contextual Information → Delivery Context Ontology
  - DRM → Media Value Chain Ontology
  - ...

Not enough to express all possible privacy requirements for SNs!

A lot of work needs to be done!
Conclusions

- Issues on access control policies for Social Networks have been analysed, including:
  - Access control policy languages limitations for SNs
  - Lack of semantic interoperability

- Possible approaches:
  - Use of Rights Expression Languages concepts to improve Policy languages for Social Networks
  - Interoperability with content-associated policies based on XACML
  - Negotiating access control rules using XACML
  - Extending ontologies to achieve semantic interoperability

- An extension to current Policy languages (XACML) to support SNs requirements may be needed
Using XACML for access control in Social Networks

Anna Carreras, Eva Rodríguez, Jaime Delgado

Distributed Multimedia Applications Group (DMAG)
Universitat Politècnica de Catalunya (UPC)

W3C Workshop on Access Control Application Scenarios
Luxembourg, 17 November 2009