Workshop on Peer-to-Peer Multicasting

IEEE CCNC 2007

A Policy Framework for Multicast Group Control

Salekul Islam and J. William Atwood

Concordia University

Department of Computer Science and Software Engineering

Montreal, Quebec, Canada

Contents

- Introduction
- Control policy for popular multicast applications
- Related work
- Proposed policy framework
- Policy specification example in XACML
- Conclusion

Introduction

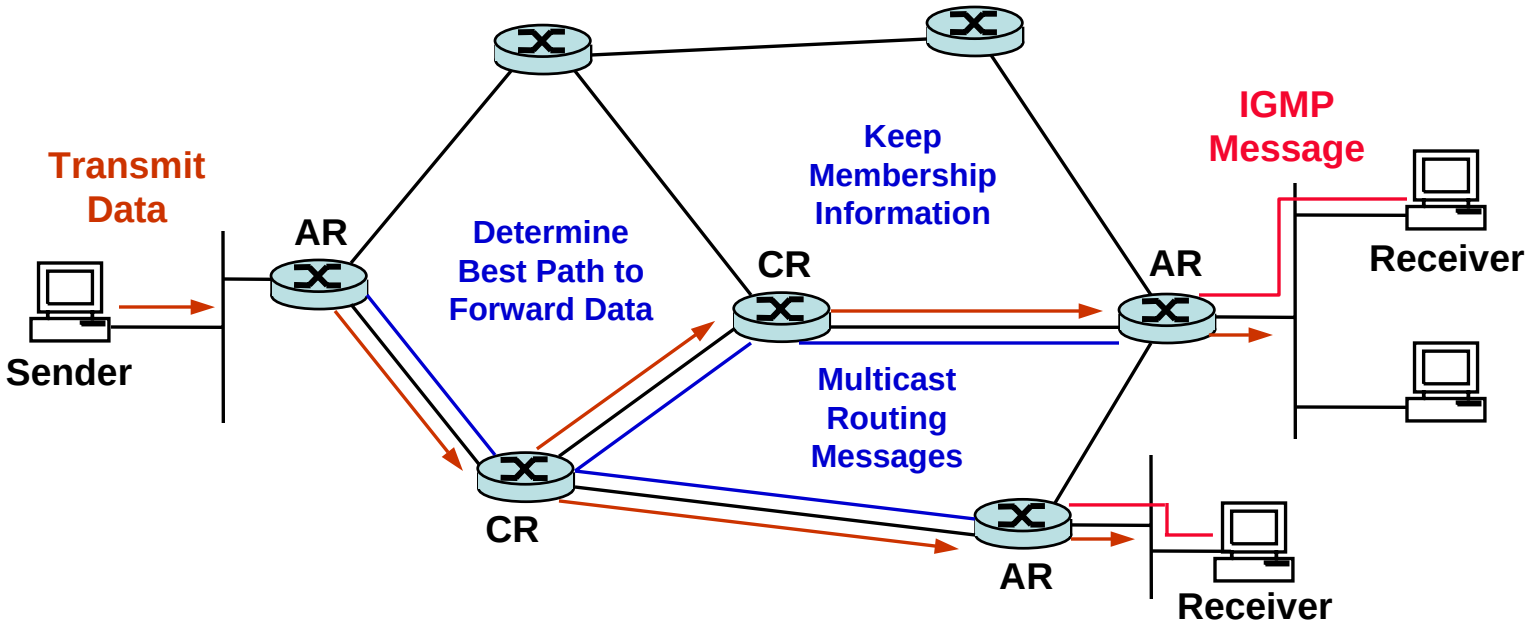

Figure 1: Present IP Multicast Architecture

Motivation

- In multicasting – anonymity of the senders and receivers
- Classical model – any one can send or receive
- Advantage of multicast – bandwidth conservation
- Network Service Providers (NSP) can generate significant revenue by deploying multicast
- The reality is
  - Multicast based applications are not in place
  - Network Service Providers (NSP) are not supporting multicast

How to break the cycle?

- Lack of control over multicast groups
- NSPs and Content Providers: no simple mechanism to get revenue
- To establish a revenue stream from end users:
  - Add AAA functionalities to present multicast model
  - Access Router will act as Network Access Server (NAS)
  - IGMP must carry end user authentication data

Internet Group Management Protocol with Access Control (IGMP-AC)

- Is based on IGMPv3
- Supports “source filtering”
- Supports different types of authentications
- Access control is optional
- Does not disrupt usual IGMPv3
- Adds least functionality and minimal workload
- Sends authentication data a minimal number of times

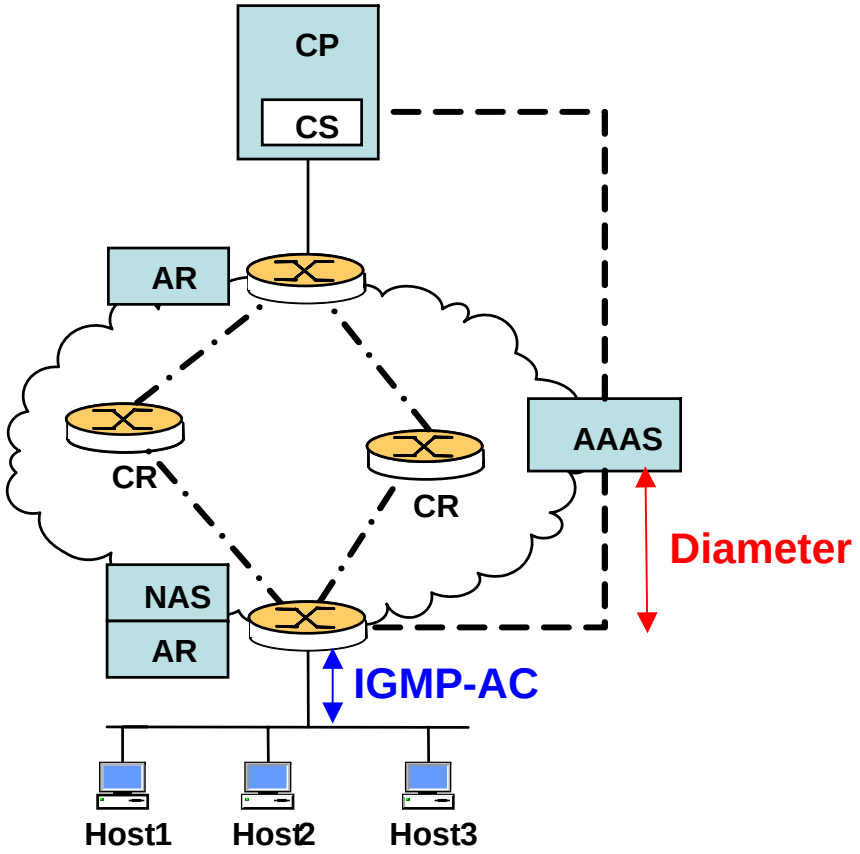

Figure 2: The IGMP-AC architecture

Multicast Group Security Policy

- Policy—a set of rules that dictates a system
- Security policy—conditions to be satisfied to access the components of a system
- Multicast group security policy—rules for elements of a group
- Two categories
  - Access control policy: deals with member authentication, join, leave, billing, etc.
  - Data policy: deals with data integrity and authentication, key management, etc.
- This paper—a policy framework for multicast access control policy

Multicast Control Policy for Different Applications

- Multicast access control policy is composed of
  - Authentication policy—straight-forward
  - Authorization and accounting policy—hard to specify
- Multicast applications are divided into
  - One-to-Many (1toM): single sender multiple receivers
  - Many-to-many (MtoM): multiple receivers and senders

One-to-Many (1toM) Applications

- Audio/video streaming
  - Internet TV
    - Authentication during joining
    - Authorized for any channel any time or subscribed to a specific program on a time slot
    - Accounting policy based on subscription
  - Distance learning
    - Class lectures are multicast
    - Only a registered student can access
    - Authorization is simple, no accounting policy
- Push media :News and weather updates, sports scores
  - Non-essential, requires low bandwidth
  - Simple authentication, no authorization and accounting policy

Many-to-Many (MtoM) Applications

- Multimedia conferencing
  - Audio, video and whiteboard
  - Participants with different roles—role based authorization
  - For corporate meeting—authentication is required, no accounting policy
- Multi-player game
  - Distributed and interactive application with chat group
  - In free subscription—no authorization and accounting
  - For paid users—relevant authorization and accounting policy

IETF Policy Framework

PEP: responsible for enforcement of policy

PDP: produces policy decisions

Policy Repository: location to store policy

Policy Management Tool: an interface for the network manager to update policies

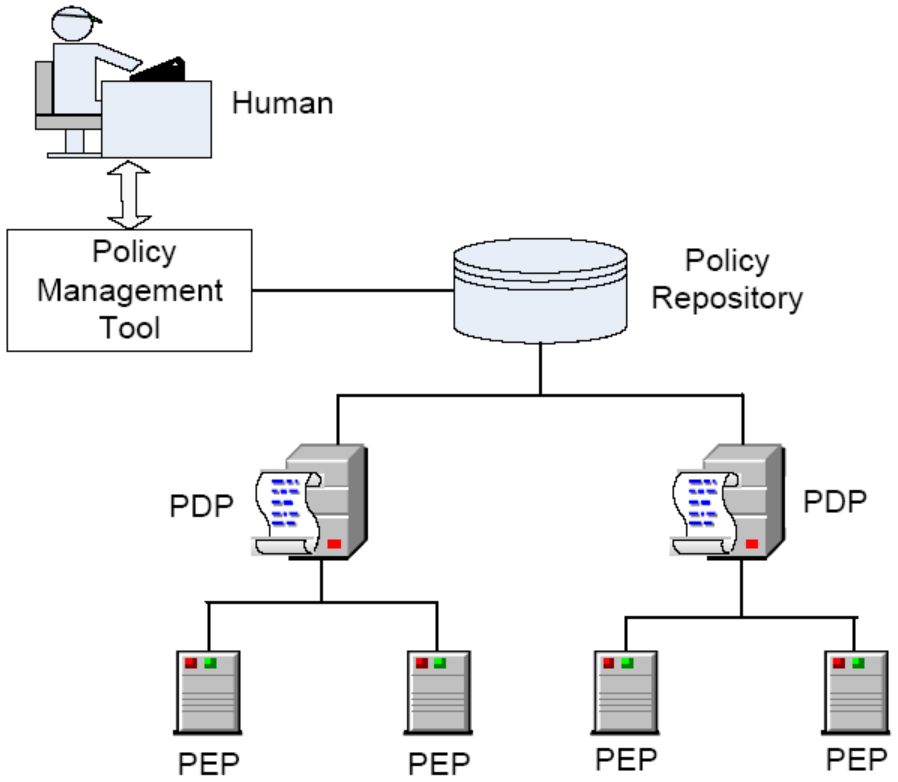

Figure 3: The IETF policy framework

Comparison Among Different Multicast Policy Frameworks

Table 1: Comparison Among Different Policy Frameworks

Method	Data Policy	Control Policy	Specification Language	Policy Protocol	Follows IETF Policy FW	Fits with MSEC FW
GSAKMP	Yes	Partially	Token based	Specified	No	Yes
XML	Yes	No	XML	Not specified	No	Yes
Antigone	Yes	Yes	Not specified	Specified	No	No
DCCM	Yes	No	Cryptographic Context Negotiation Template	Cryptographic Context Negotiation Protocol	No	No
MGMS	Yes	No	GML	Not specified	No	No

Summary of Different Methods

- None of the methods conforms with the IETF Policy Framework
- Only Antigone addresses complete access control policy
- Antigone, DCCM and MGMS are for “secure group communication”
- Only two comply with MSEC Framework
- In conclusion: a flexible, scalable, easily adaptable multicast access control policy architecture is needed.

Proposed Policy Framework: Design Requirements

- Should extend the IGMP-AC architecture
- The entities of the MSEC Framework should be present
- Will follow the IETF Policy Framework
- Will deal with multicast data policy and access control policy independently—can deploy any group key management scheme
- Should not depend on any specification language or policy protocol

Proposed Policy Framework

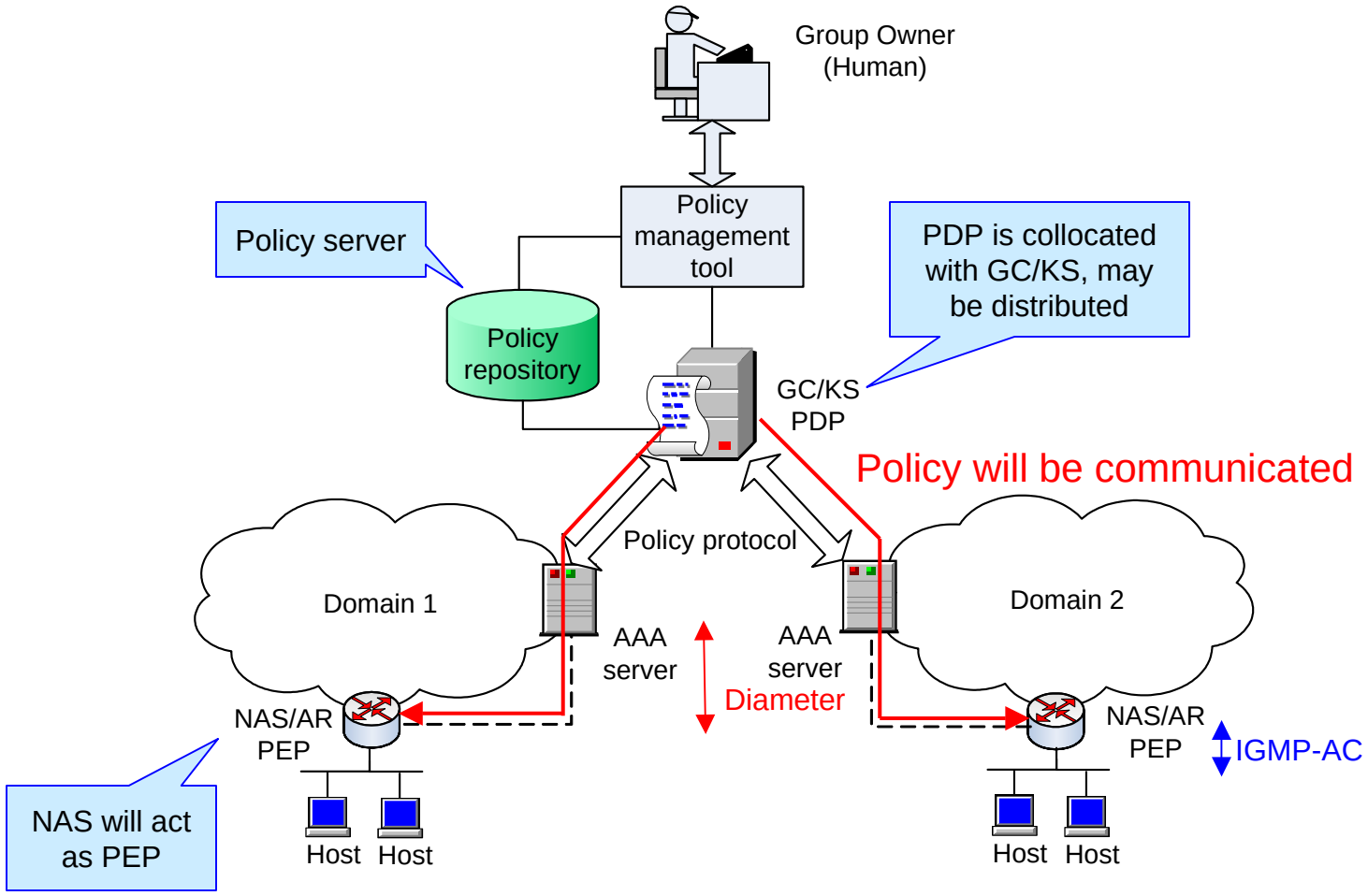

Figure 4: Proposed policy framework

Policy Specification and Protocol

- eXtensible Access Control Markup Language (XACML) for policy specification
- Security Assertion Markup Language (SAML) for the communication between a PEP and a PDP
- Any other language/protocol can be used
- XACML:
  - XML-based for access control
  - Query-response language
- OASIS standard specifies transportation of XACML query/response inside SAML

Policy Specification in XACML

- XACML with SAML is used widely for access control
- Flexible to express different needs of access control policy
- Extensible to support new requirements
- The developers can reuse their existing code to support policy language
- Sun Microsystems, Inc. has already implemented XACML using Java

Com…t of XACML Policy


```
<Policy >
  <Rule>
    <Target>
      <Subject
        .....
      </Subje
      <Resour
        .....
      </Resour
      <Actions>
        .....
      </Actio
    </Target>
    <Condition
      .....
    </Condition>
  </Rule>
</Policy>
```

The most elementary unit of …

Composition of Subjects, Resources, and Actions to whi…

Actors with specific attributes. May have more than one Subjects.

Data, service or a system component. May have more than one Resources.

An operation on a Resource. May have more than one Actions.

An expression either true or false.

XACML Architecture

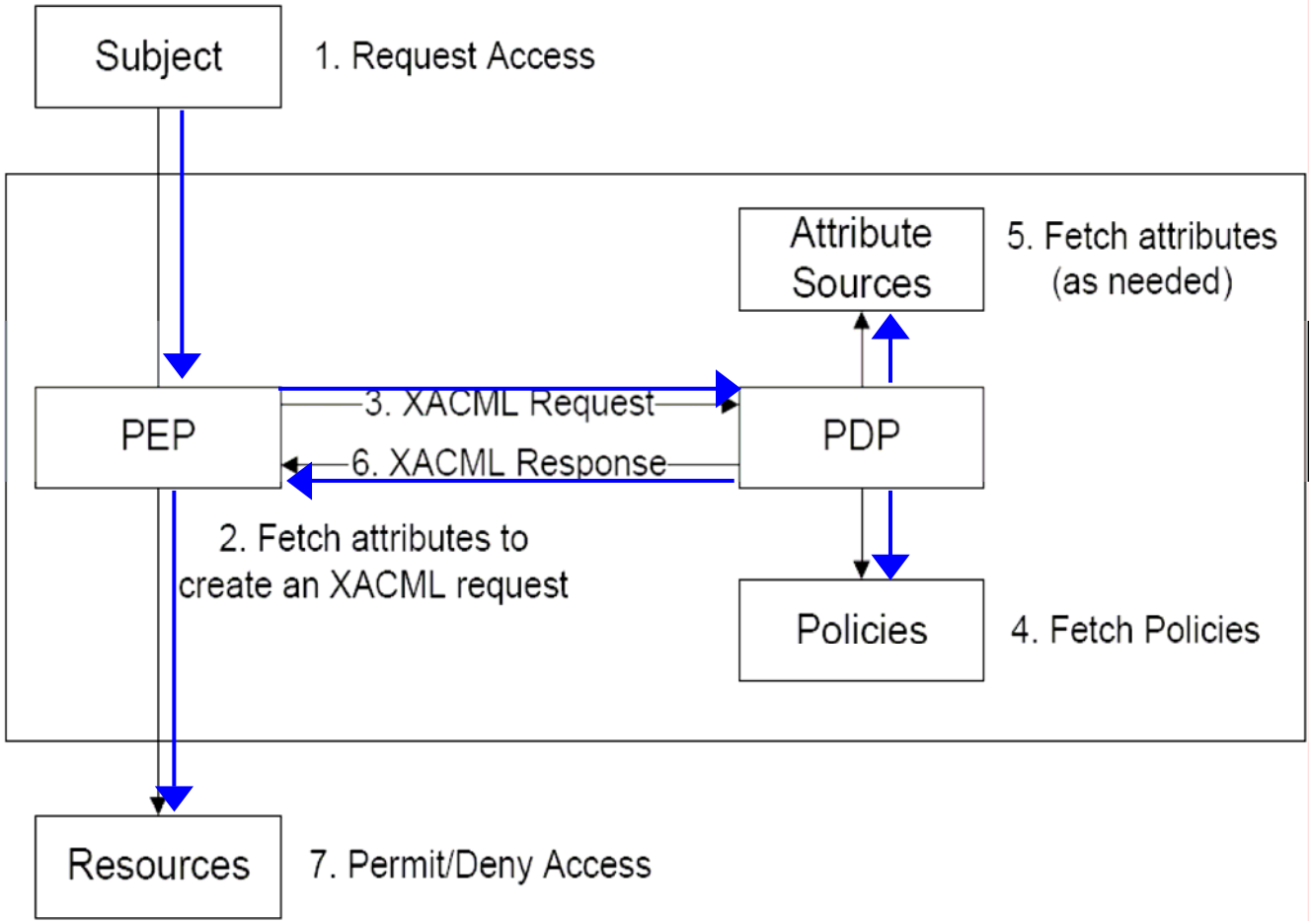

Figure 5: The XACML policy framework

Proposed Policy Framework: revisited with XACML and SAML

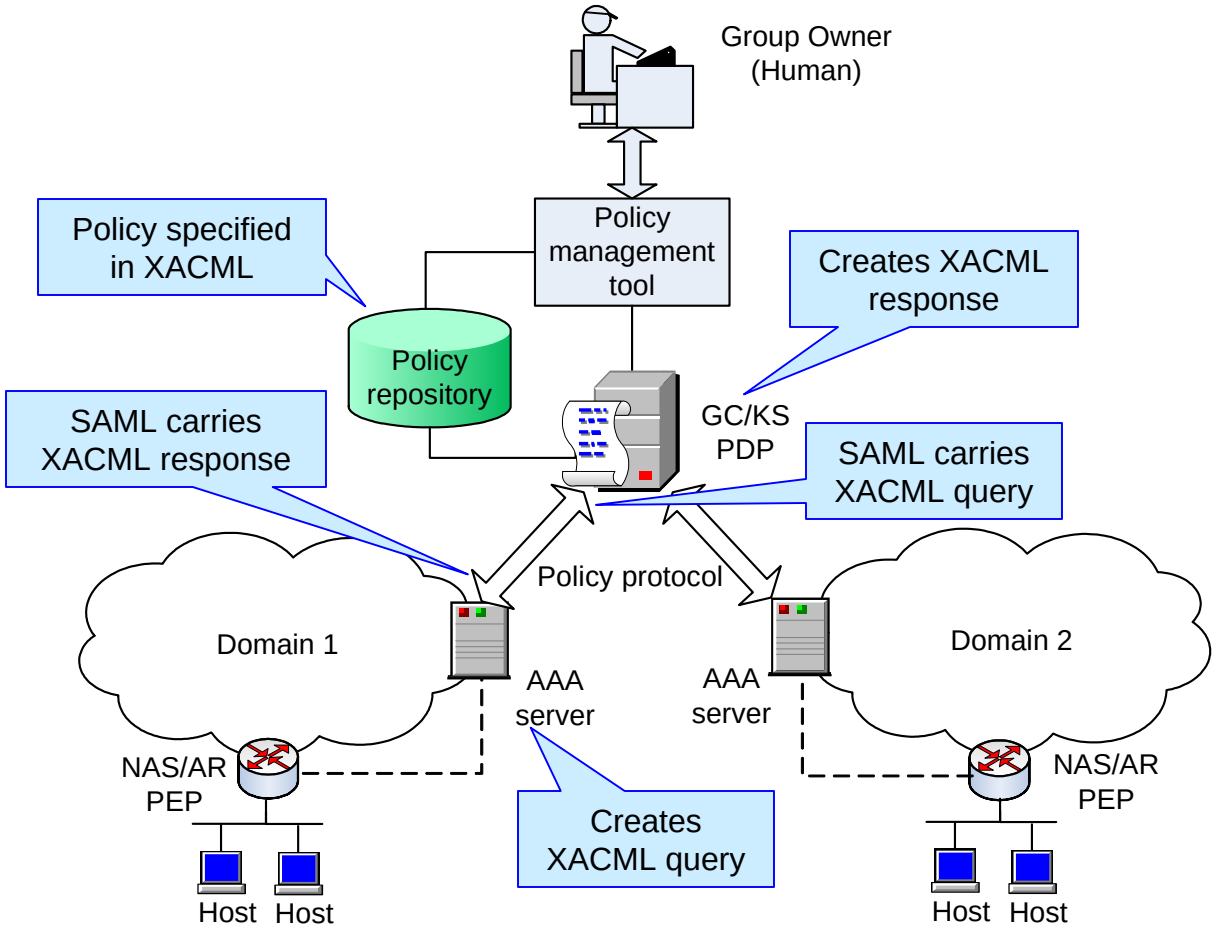

Figure 6: Proposed policy framework with XACML and SAML

Policy for On-line Course

- An access control policy for the on-line course, INTE290
- Offered by Concordia University from September to December, 2006
- Email address and password for authentication
- Lecture will be multicast during the class hours
- Receive a lecture through **http://www.econcordia.ca/INTE290/lectures**
- Students send questions in text/voice format in class hours
- Two groups:
  - 1toM for sending multimedia class lecture (shown in example)
  - MtoM of text/voice for sending questions (not shown in example)

XACML Policy for On-line Course


```
<Rule Effect="Permit" RuleId="StudentAccessControlRule">
  <Description> If a request is successfully matched
        against this rule an evaluating PDP will return
        Permit </Description>
  <Target>
      <Subjects>
         <Subject>
           <SubjectMatch>
               user-id@econcordia.ca
           </SubjectMatch>
           <SubjectMatch>
               Password
           </SubjectMatch>
         </Subject>
      </Subjects>
```

Both email address and password must match to get access

XACML Policy for On-line Course


```
<Resources>
    <Resource>
      <ResourceMatch>
          http://www.econcordia.ca/INTE290/lectures
      </ResourceMatch>
    </Resource>
</Resources>

<Actions>
    <Action>
      <ActionMatch>
          Read
      </ActionMatc>
    </Action>
</Actions>
```

Lectures will be multicast here

The only permitted action is to read/receive data

XACML Policy for On-line Course


```
<Condition>
    <Apply "function:and">
        <Apply "function:date-greater-than">
              2006-09-01
         </Apply>
        <Apply "function:date-less-than">
              2006-12-31
        </Apply>
    </Apply>
</Condition>
```

Flexible condition

Any date between 1st of September and 31st of December, 2006 is valid

Conclusion and future work

- A new policy framework for multicast access control
- The proposed framework
  - is based on XACML
  - fully complies with the MSEC Framework
  - follows the IETF Policy Framework.
- An example access control policy for an on-line course
- Future goals:
  - Complete the IGMP-AC project
  - Define inter domain behaviour
  - Performance study

For more information

- High Speed Protocols Laboratory of Concordia University is doing extensive research on IP multicast,

  http://users.encs.concordia.ca/~bill/hspl/

- To know more about IGMP-AC visit,

  http://users.encs.concordia.ca/~salek_is

- For questions and comments:

  salek_is@cse.concordia.ca

  bill@cse.concordia.ca