What needs to be specified by the XACML model?

Ernesto Damiani and Pierangela Samarati

2nd XACML F2F

Boston, 7-8 September 2001

Model

A security model defines in a precise and unambiguous way the security policy and its working.

A model is usually expressed in a “formal” way to provide preciseness and unambiguousness.

Two aspects:

- syntax: what form do access control rules have?
- semantics: what is the intended meaning of an access control rule

Questions

- Against which subjects are access rules specified?

  Expression on “properties” associated with the requestor.

  It can be any any attributes or statements (SAML attribute assertions??) that the requestor can present. In particular it can include:

  - Identity
  - Location (property of the request)
  - Groups
  - Roles (dynamic property of the subject)

    (reason about digital certificates or simply about properties, not worrying if/how you extract them from certificates?)

- **Note**: difference between assertion subjects and authorization subjects (assertions can refer to someone different from the requestor). Ex: A patient (*requestor*) requests to send (*action*) some data (*object*) to some doctors (*parameter??*). Assertions can refer to the doctor, i.e., the *recipient* of the data.

- Against which objects are access rules specified?
- For which kinds of actions are access rules specified (can we reason about parameters)?
- Which form of abstraction/aggregation/composition relationships can be supported?
- Can access control rules have additional conditions? (e.g., restriction of use or dynamic conditions as payment procedures)
- Can access control rules be in positive and negative form?
- How do we solve the conflicts between contrasting rules?

Questions

- What kind of relationships between elements of the systems can be exploited in specifying the rules?
- What is the form of access control rules (e.g., simple triple, implication rule)
- Who can specify the access control rules? (administration)
- Would there be the need for supporting independent policies and composition of policies?
- Relationships with SAML?