Towards Standardization of Distributed Access Control

Mario Lischka, Yukiko Endo
NEC Laboratories Europe

Elena Torroglosa, Alejandro Pérez, Antonio G. Skarmeta
University of Murcia

Presentation at W3C Workshop on Access Control Application Scenarios, 17./18. November 2009, Luxembourg
- identified different kind of policies
  - control the privacy of the user's identity
  - his/her data, as well as
  - interoperation between different participants.
- Decisions could not only be done locally, but have to be aligned with policies in other domains.
Overview

- Example
- Important Aspects
- Proposed Architecture
- Extension to Policy Language
- Complexity of Evaluation
- Conclusion
Example of Deductive Policies

- Access to service provider requires
  - approval of included service
  - access to additional values

- Decisions could not only be done locally, but have to be aligned with policies in other domains.
Important Aspects

- **Authoritative Domain** as new structuring entity
- **Hierarchical requests**: circular dependencies among Authoritative Domains have to be avoided
- **Abstraction**: details about other policy of other domains are not required
- **Independent**: definition of policies
- **Adaptive**: Policies support dynamic references to other authoritative domains
- **Bridging**: translation of local attribute names and value space into those of referred ones
- **Transparency**: location of the referred domain with respect to end-points is not explicitly required inside a policy
- **Confidentiality**: internal details on the rules and the attributes leading to the decision can be kept confidential

Presentation at W3C Workshop, 17./18. Nov. 2009, Luxembourg
Extension to the existing XACML architecture

- Two new entities responsible for deducting
  - Attributes (DPIP)
  - Authorization request (DPDP)

- Messages are an extension of XACML
• Redefinition of PolicySet
• Integration of distributed PolicyReference and local Policy through *(new) combining algorithm*
• depending on combining algorithm
  • local policies could be evaluated first, avoiding referred requests
  • Initiate parallel evaluation (saving time)
• referred request takes extra communication time

• referred Domains are always unique at evaluation time
  (e.g, in contrast to Datalog)
• Circular dependencies are avoided

Complexity of the evaluation not changed compared to XACML
• Deductive policies could be used to bridge different domains
  • distribute decisions
  • access to remote attributes
• Authoritative Domain provides a new abstraction level

• avoiding undecidability problem of Datalog
• integration into existing XACML standard

• extra communication costs,
  but no general increase of evaluation complexity

• Application of Deductive Polices in various prototypes of the EU FP7 project SWIFT