Comparing AIR and XACML In A Nutshell

Fatih Turkmen (University of Trento)

Ian Jacobi (MIT)

Lalana Kagal (MIT)

AIR vs XACML

- AIR is logic-based (**REASONING**), XACML is not (**ACCESS CONTROL**)

→ AIR (Phyton) can be serialized to XML??

→ AIR depends on the N3 semantics,

→ XACML has an XML based syntax

- XACML is dedicated for access control, AIR has been designed for information accountability

- Scalability must be studied in AIR

- AIR does reasoning which means it can intrinsically supports justifications while in XACML it totally depends on the Policy Decision Point (PDP) engine. For example; rules conflicting each other. AIR has been grounded with the idea of “tell me why I can do this?”

AIR vs XACML (Cont.)

- Obligations can be addressed in AIR

  - The requirements to be met after the decision.

  - AIR is focused on the compliance rather than the access prior to the actual event happening. Maintaining the states is not currently available for usage control while it is left to the Policy Enforcement Point (PEP) entity of the XACML architecture.

AIR vs XACML (Cont.)

- AIR does not have a specific mechanism, profile, or ontology to handle delegation, but it can be achieved through special rules.

- One of the strengths of AIR lies in the ability to use concepts from other ontologies. For example; foaf:knows where the foaf namespace defines the meaning of "knows“.

AIR vs XACML (Cont.)

	XACML	AIR
Constructs	PolicySet, Policy, {*Subject, Resource, Action, Environment*}, Rule, Condition, Obligation	Policy, Pattern (Variable), Assertion, Rule, MatchedGraph, Justification
Inference Capability	No	Yes (e.g. subject is the brother of an entity described in the policy)
Evaluation Mechanism	Request against Policy (Request - Response)	Forward Chaining (based on Policy and the generated data) Reasoning
Language Complexity	Low (both advantage and disadvantage)	High (both advantage and disadvantage)
Conflict Resolution	Flexible Combining Algorithms	Left to the reasoner

AIR vs XACML (Cont.)

	XACML	AIR
Delegation	Available (profile available)	Available (e.g. Delegation ontology/policy)
Administration	V3 provides Administration Policy	Similar to Delegation Case (e.g. Administration Policy)
Profiles	Yes	Access Control Profile
Extensibility	Yes	Yes (built-in functions extension → implementation specific)