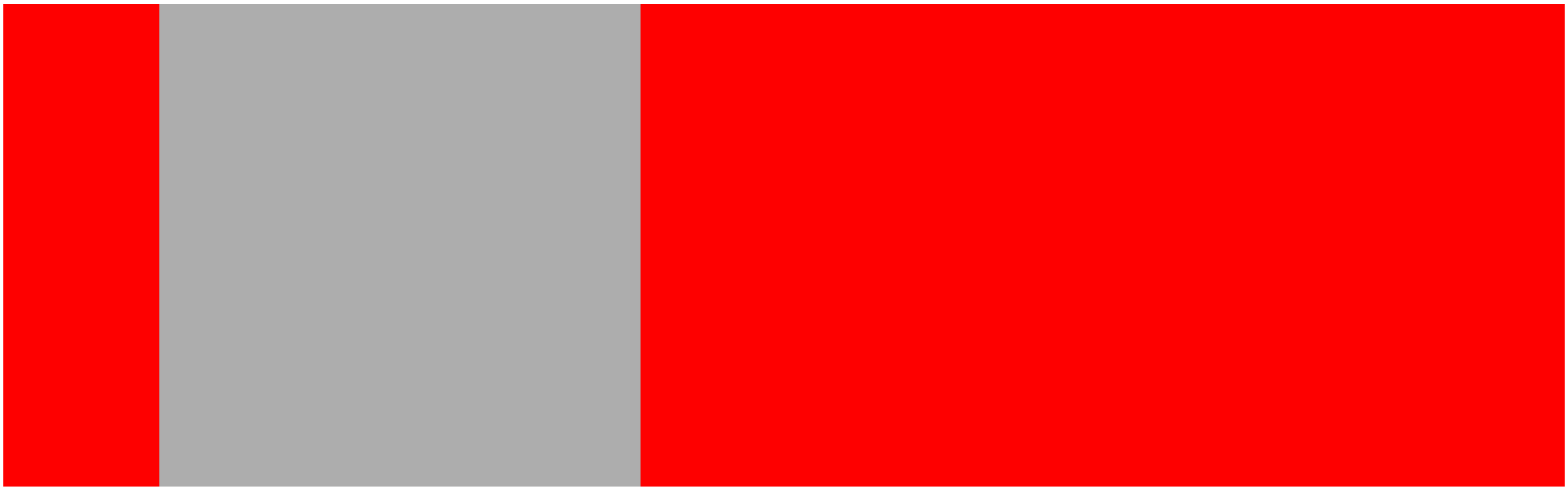

ORACLE

The State of Access Control 2009

Hal Lockhart

Authorization Principles

- Federation principle – authoritative source
- Externalize policy
  - Encapsulate policy – PDP as black box
  - Add functionality by calling PDP – don't open box
    - Multi-request, What-if, Administrative policies
  - Standard policy expression – permits analysis
  - All policy in the box – not spread around
- Use data already being maintained (not artificially constructed for Authorization)
- Limit complexity – human comprehension

General Requirements

- Access Control System requires multiple components
- PDP – XACML
- PEP – environment specific, but tools would help
- PIP – undeveloped area
- Policy authoring tools
- Policy analysis tools

XACML Current Status

- XACML 2.0 OASIS Standard – Feb 2005
- ITU-T Recommendation X.1142 – Jun 2006
- XACML 3.0 In progress
  - Core & base profiles recently completed Public Review
    - Administration/delegation {New}
    - Hierarchical resource {Enhanced}
    - Multiple resource {Enhanced}
    - SAML {Enhanced}
    - Digital Signature
    - Privacy
    - RBAC
  - Additional profiles under development
    - XSPA, Obligation families, Export Compliance, Policy Distribution, Metadata, WS-XACML
  - Face to face Meeting December 8-10, Redwood Shores, CA

Constructing Policy Enforcement Points

- XACML defines an abstract XML interface and a wire protocol for decision requests
- Desirable to have Program APIs in popular languages
- High performance local PDP & ease in calling remote
- Support non-XACML PDP
- Facilitate migration to XACML
- Oracle & Cisco contributed draft Java API to XACML TC
- Based on XACML abstract interface
- OpenAz open source project to develop useful components (http://www.openliberty.org)
- Other languages to follow (C++, C#, scripting)

Policy Inputs (Attributes)

- Little standardization of formats and semantics
  - Recent efforts in GeoSpatial, Healthcare, Areospace
  - Applicability of Semantic Web technologies?
- Distribution of attributes
  - Low level standards for Subject, SQL, LDAP, SAML, WS-Trust
  - Privacy & security not addressed – see IGF
- Almost nothing for Resource Attributes
  - Where? How? Format? Semantics?
  - Work on Open Document Format
- Needed Attribute Metadata
  - AMF also contributed to XACML TC
  - OpenAz to build AMF-driven PIPs
  - Semantic Web here too?

Tools for Policy Authoring

- Low level (IDE model) GUI
  - Integration with AMF
  - Integrated analysis, what if?
- High Level (Enterprise Policy)
  - Broader scope than access control
  - Generate XACML policies automatically
- Policy libraries, idioms, best practices, training

Tools for Policy Analysis

- Reverse queries not feasible in large scale settings
- Three possible approaches
  - Partial evaluation
    - Also useful for PDP performance optimization
  - What If? Tools
  - Language analysis
    - Reduce structure to logical expressions
    - Treat data formatting & selection functions as black box
    - Potential for annotation conventions?
- XACML has avoided standardizing tools to create market opportunities