Meta-policies for Distributed Role-based Access Control

András Belokosztolszki, Ken Moody
{ab374,km}@cl.cam.ac.uk
University of Cambridge, Computer Laboratory, OPERA
Outline

• Role-Based Access Control
• OASIS
• Meta-Policies
  – Meta-Policy Types
  – Compliance
• Summary
Role-Based Access Control

Sessions → Activation → Roles → Authorization → Privileges

Policy 2002
OASIS Rules
(Open Architecture for Secure Interworking Services)
Administrative Domains

Policy 2002
Problems

• SLA maintenance
  – New domain, change to a domain, …
• Policy evolution
• Information hiding
• Information about the policy
• Local Autonomy
Meta-Policies

- Data types
- Objects (privileges)
- Functions and Predicates
- Roles (parameters)
- Appointment Certificates (parameters)
- Rules (membership conditions)
  - Explicit / Implicit
  - Negation
- Constraints (SSoD, …)
Meta-Policy Types

• Compliance
  – For a single domain
  – Information for users
  – Higher level policies
  – Policy evolution

• Interface
  – Communication with other Domains
Mappings

• Meta-Policies are mapped to Policies
  – Data-types (one-to-one, one directional)
  – Functions / Environmental Predicates
  – Roles / Appointments
  – Rules
  – Other Constraints (SSOD, …)

• Policy or subset of a policy is considered

• Direction of Mappings

• Parameters (and constants)
Compliance Check

• Existence of the mappings
• Prerequisite services?
• Rules:
  1. Translating into policy context
  2. Checking explicit rules
  3. Checking Implicit rules
     • Negation (entire policy is considered)
  4. Other Constraints
• Result: Certificate
SLA generation

• For Interface Meta-Policies:
• Automatic generation
Implementation

Desert:
Mapping Editor
SLA generator
Summary

• Meta-Policies (Compliance/Interface)
• Implementation (Desert)
  – Mapping editor
  – SLA generator
Acknowledgement

• King’s College Cambridge Graduate Student Fund
• Overseas Research Students Award Scheme