A Design of An Authorization Service

Konstantin Beznosov
http://www.cs.fiu.edu/~beznosov/

February 12, 1999

Presentation at
CADSE, FIU
Today Objectives

• Critically analyze:
  – the prototype objectives
  – the design
    – directions
    – details
What Will Be Discussed

• CORBA security model
• What CORBA Access Model does[ not] Cover
• Healthcare Resource Access Control (H-RAC) high level view
• Authorization Service framework design details
CORBA Access Control Model
CORBASEC Does Not Cover Non-Object Entities
HRAC Compliments CORBASEC
HRAC High Level View

Client

Target Object (ADO client)

AccessDecision

1. Application Request
2. Authorization request
3. Reply to authorization request
4. Reply to application request

CORBA Object Request Broker

Scope is Application

Scope is HRAC
HRAC model: logical view
Authorization Service
Implementation Objectives

• Create a framework for future
  – experiments
  – proofs of concepts
  – measurements
  on authorization systems

• HRAC feasibility proof
Authorization Service Impl. View 1/3

<<Interface>>
Access Decision

- access_allowed()
- multiple_access_allowed()

<<Interface>>
AccessDecisionExt

- admin : AccessDecisionAdmin

<<Interface>>
PolicyEvaluatorAdmin

- replace_policy()
- add_policy()
- list_policy()
- set_default_policy()

<<Interface>>
PolicyEvaluator

- policy_evaluator_admin : PolicyEvaluatorAdmin

- evaluate()
- multiple_evaluate()

<<Interface>>
Authorization

- policy_evaluator_locator : PolicyEvaluatorLocator
- dynamic_attribute_service : DynamicAttributeService

- shutdown()
Authorization Service: Impl. View 2/3

- **<<Interface>>**
  - PolicyEvaluator
    - `policy_evaluator_admin : PolicyEvaluatorAdmin`
    - `evaluate()`
    - `multiple_evaluate()`

- **<<Interface>>**
  - PolicyEvaluatorAdmin
    - `replace_policy()`
    - `add_policy()`
    - `list_policy()`
    - `set_default_policy()`

- **GenericEvaluator**

- **AlwaysDenyEvaluator**
Authorization Service: Interact. View 1/2

an Application System

an Access Decision Object: AccessDecision

a Locator: PolicyEvaluator

an Attribute Service: DynamicAttribute

an Evaluator: PolicyEvaluator

a Combinator: Decision

get_policy_decision_evaluators(ResourceName)

get_dynamic_attributes(AttributeList, ResourceName, String)

* evaluate(ResourceName, String, AttributeList)

combine_decisions(DecisionResultList)
Authorization Service: Interact. View 2/2

- an Access Decision Object: AccessDecision
- a Locator: PolicyEvaluatorLocator
- an Attribute Service: DynamicAttribute
- an Evaluator: PolicyEvaluator
- a Combinator: Decision

- multiple_access_allowed(AccessDefinitionList, AttributeList)
  - * get_policy_decision_evaluators(ResourceName)
  - * get_dynamic_attributes(AttributeList, ResourceName, String)
  - * multiple_evaluate(AccessDefinitionList, AttributeList)
  - * combine_decisions(DecisionResultList)
ADO State Diagram

Start

Registering Offer

Registering DynamicAttributeService

[ offer registered ]

Registering PolicyEvaluatorLocator

[ all decisions made ]

 Obtaining Dynamic Attributes
 entry: ^DynamicAttributeService.get_dynamic_attributes
 exit: ^PolicyEvaluator.evaluate

 / get evaluations

 Obtaining Policy Evaluators
 exit: ^PolicyEvaluatorLocator.get_policy_decision_evaluators

 / get policy evaluators

 Obtaining Final Decision
 entry: ^DecisionCombinator.combine_decisions

[ some decisions made ]

Access allowed

Multiple_access_allowed

Returning

Not Ready

Waiting

Ready

Error

Shutdown / Record Shutdown

Registering DynamicAttributeService

entry: Register DAS

Registering PolicyEvaluatorLocator

entry: Register PE_Locator

Registering Offer

[ offer registered ]

Registering PolicyEvaluatorLocator

entry: Register PE_Locator

Registering DynamicAttributeService

entry: Register DAS

[ all decisions made ]

[ the offer and all services are registered ]

access_allowed

multiple_access_allowed

Shutdown / Record Shutdown

[ all decisions made ]

[ some decisions made ]

access_allowed, multiple_access_allowed

Error

entry: Record Error
Authorization Service: Component View

- ResourceAuthorizationService
- PolicyEvaluatorLocator
- PolicyEvaluatorLocator
- PolicyEvaluatorLocatorAdmin
- AccessDecision
- PolicyEvaluator
- SimplePolicyEvaluator
- PolicyEvaluatorAdmin
- AndCombinator
- AccessDecisionExt
- DynamicAttributeServiceExt
- DynamicAttributeServiceAdmin
- DynamicAttribute
- SpecializedDynamicAttribute
- UnixUserAttributesService