Management Advantages of Object Classification in RBAC

(Pages 96-110)

Mohammad Jafari
(m_jafari@ind.iust.ac.ir)
Mohammad Fathian
(fathian@iust.ac.ir)

Department of Information Technology, Electronic Commerce,
Iranian University of Science and Technology

Prepared to present at the Asian'07 conference, Doha, Qatar, December 2007

Structure

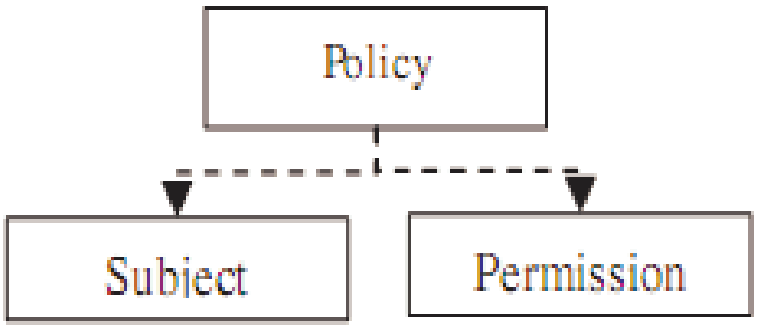
- Object classification in the literature
- Formulating object classification
  - A conceptual look at RBAC
    - Three reference models
    - Access control policy components
    - Concrete and abstract entities
- Ease of management
  - Comparing the three models by using seven criteria

Three typical reference models

- Trivial permission assignment model (TPA)
- Plain RBAC model (P-RBAC)
- Object-classification-enabled RBAC (OC-RBAC)

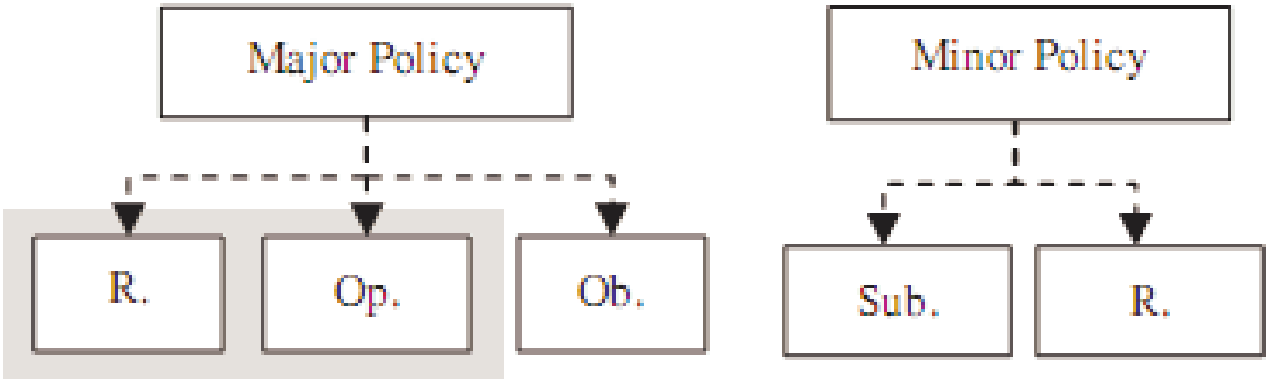
Trivial Permission Assignment Model

- Determine the access rights of every single subject to each object
- Example: Access matrix model
- Access control policy
  - Single component
  - System dependent



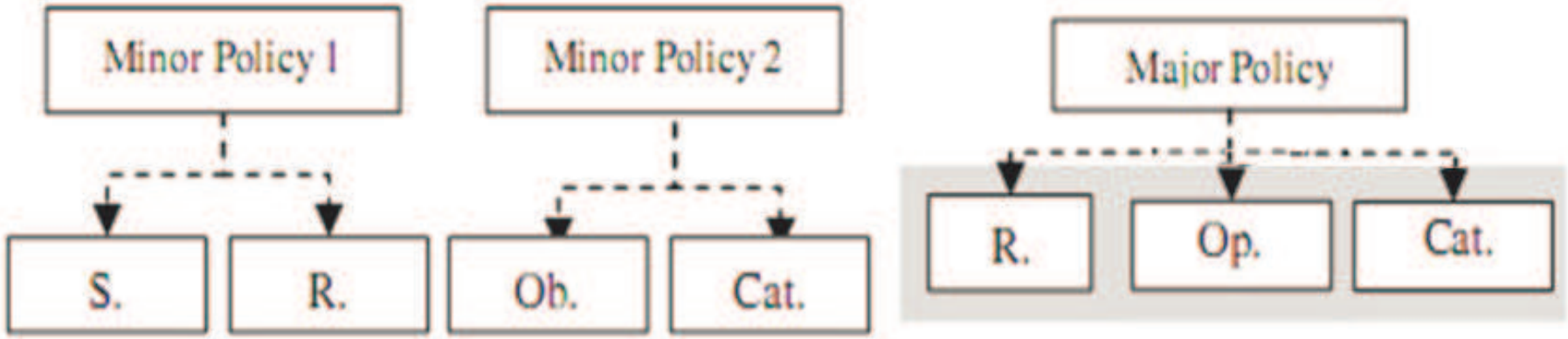
Plain RBAC

- Subjects are assigned roles
- Access rights of roles to objects are determined
- Two components in the access control policy
  - Subject-role assignment
  - Role-permission assignment
    - Permission: and operation practiced on an object



Object-classification-enabled RBAC

- Subjects are assigned roles
- Objects are classes (categories)
- Access rights of roles to objects classes are determined
- Three components in the access control policy
  - Subject-role assignment
  - Object-class assignment
  - Role-class access rights



Entities

- Subjects, Objects
  - Concrete and system-dependant
  - Example:
    - John
    - Perinter1, File1
- Roles, Categories (Object Classes)
  - Abstract and system-independent
  - Example:
    - Secretary
    - Secretary Printer, Financial Files
- Operations
  - System-independent

Design Rationale

- Removing dependency to system-specific entities by replacing them with abstract entities
  - Subject → Roles
  - Objects → Categories (Object Classes)

Comparing the three models

- Criteria
  - Number and complexity of decisions
  - Change management cost
  - Risk of error
  - Policy portability and reuse
  - Enforcement and compliance
  - Traditional information classification
  - Object grouping and management

Number and complexity of decisions

- Two types of decisions
  - Major decisions
    - Should be made by a security officer
    - Example:
      - Access rights of a user
      - Access rights of a role
  - Minor decision
    - Can be made by an operator
    - Example:
      - Role of new employee
      - Class of a new object

Number and complexity of decisions

- TPA:
  - Decide each triplet (subject, object, operation)
    - |S|*|O|*|Op| decisions
    - |Op|=constant, n=max(|S|,|O|)
    - ➔ $O(n^2)$ major decisions

Number and complexity of decisions

- P-RBAC:
  - Major Policy
    - Decide each triplet (role, object, operation)
    - |R|*|O|*|Op| decisions
    - |Op|=constant, |R|=constant
    - ➔ O(n) major decisions
  - Minor Policies
    - Decide the roles of each subject
      - (subject, role) =0 or 1?
    - |S|*|R| decisions
    - |R|=constant
    - ➔ O(n) minor decisions

Number and complexity of decisions

- OC-RBAC:
  - Major Policy
    - Decide each triplet (role, category, operation)
    - |R|*|C|*|Op| decisions
    - |Op|=constant, |R|=constant, |C|=constant
    - ➔ O(1) major decisions
  - Minor Policies
    - Decide the roles of each subject
      - ➔ O(n) minor decisions
    - Decide the class of each object
      - (object, class) =0 or 1?
    - |O|*|C| decisions
    - |C|=constant
      - ➔ O(n) minor decisions
    - ➔2*O(n) minor decisions

Number and complexity of decisions

	TPA	P-RBAC	OC-RBAC
Number and Complexity of Decisions	$M.O(n^2)$	$M.O(n) + m.O(n)$	$M.O(1) + m.O(n)$

Change Management Costs

- Change in subject's access rights
  - TPA
    - Reviewing access rights of a the subject to all objects
    - |O| ➔ O(n) major decisions
  - P-RBAC/OC-RBAC
    - A change in subject's role
    - |R| ➔ O(1) minor decision
- Change in role's access rights
  - TPA
    - Reviewing access rights of a group of subjects to all objects
    - |S||O| ➔ $O(n^2)$ major decisions
  - P-RBAC
    - Reviewing access rights of a role to all objects
    - |R|*|O| ➔ O(n) major decisions
  - OC-RBAC
    - Reviewing access rights of a role to all categories
    - O(1) major decisions

Change Management Costs

- Change in an object's access permissions
  - TPA
    - Reviewing access rights of all subject to the object in question
    - |S|➔ O(n) major decision
  - P-RBAC
    - Reviewing access rights of all roles to the object in question
    - |R| ➔ O(1) major decisions
  - OC-RBAC
    - A change in the object's categories
    - |C| ➔ O(1) minor decisions

Change Management Costs

- Change in access permissions of a category
  - TPA
    - Reviewing access rights of all subjects to a group of objects
    - |S|*|O| ➔ $O(n^2)$ major decisions
  - P-RBAC
    - Reviewing access rights of all roles to a group of objects
    - |R|*|O|➔O(n) major decisions
  - OC-RBAC
    - Reviewing access rights of all roles to the category in question
    - |R|*|C| ➔ O(1) major decisions
- Total change in some area
  - Similar to utter policy design in a subset of the system

Change Management Costs

Change Type	TPA	P-RBAC	OC-RBAC
Subject's access rights	M.O(n)	m.O(n)	m.O(n)
Role's access rights	$M.O(n^2)$	M.O(n)	M.O(1)
Object's access permissions	M.O(n)	M.O(1)	m.O(1)
Access permissions of a category	$M.O(n^2)$	M.O(n)	M.O(1)
Total change in some area	$M.O(n^2)$	M.O(n) + m.O(n)	M.O(1) + m.O(n)

Risk of Error

- Risk = Probability * Impact
- Major Decisions
  - Made by a manager
    - ➔ More elaboration
      - ➔ Low probability
  - More profound consequences
    - ➔High impact
- Minor Decisions
  - Made by operator
    - Less elaboration
      - ➔High probability
  - Less severe consequences
    - ➔ Lower impact

Risk of Error

- I.p : High-impact, less likely
- i.P : Low-impact, more likely

	TPA	P-RBAC	OC-RBAC
Risk of Error	$I.p.O(n^2)$	I.p.O(n) + i.P.O(n)	I.p.O(1) + i.P.O(n)

Policy Portability

- Less system dependency provides higher chance for portability
- TPA
  - tightly system-dependent
    - No chance for portability
- P-RBAC
  - Roles can be reused
  - Decide access rights of each role to each object
    - O(n) major decisions
  - Decide roles of each subject
    - O(n) minor decisions
- OC-RBAC
  - Both roles and categories can be reused
  - Decide roles of each subject and categories of each object
    - O(n) minor decisions

Other advantages

- Automatic enforcement and compliance-checking
  - Standard policies with standard roles and categories and standard access rights
- Support for traditional information classification policies
  - Object categories can be used to implement security labels
- Object management and grouping
  - Object classification provides a grouping mechanism for better management of objects

Summary

	TPA	P-RBAC	OC-RBAC
Number and Complexity of Decisions	$M.O(n^2)$	$M.O(n) + m.O(n)$	$M.O(1) + m.O(n)$
Change management cost (Detailed previously)	Poor	Good	Better
Risk of Error	$I.p.O(n^2)$	$I.p.O(n) + i.P.O(n)$	$I.p.O(1) + i.P.O(n)$
Policy portability and reuse	None	$M.O(n)+m.O(n)$	$m.O(n)$
Enforcement and compliance	None	Manual	Automated
Traditional classification policies	None	Complex	Trivial
Object grouping	Implementation-level	Implementation-level	Direct support from model

Conclusion

- Limitations
  - A real case study showing the benefits
  - Neglecting role-engineering and category engineering practices
- Future works
  - Policy portability when multiple superior policies exist
  - Policy portability when the acquiring system need to extend roles/categories while preserving compliance to the higher-level policy
  - Practical value of “Category hierarchies” and “Separation of categories”