INFS 767 Fall 2001

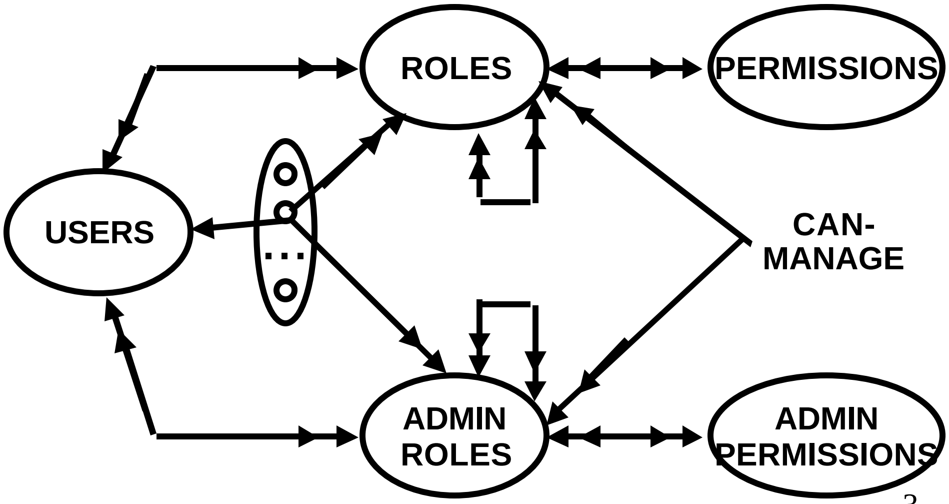
Administrative RBAC
ARBAC97

Prof. Ravi Sandhu

SCALE AND RATE OF CHANGE

- **roles: 100s or 1000s**
- **users: 1000s or 10,000s or more**
- **Frequent changes to**
  - **user-role assignment**
  - **permission-role assignment**
- **Less frequent changes for**
  - **role hierarchy**

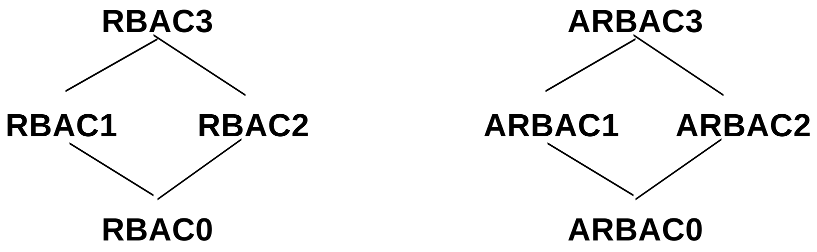
ADMINISTRATIVE RBAC



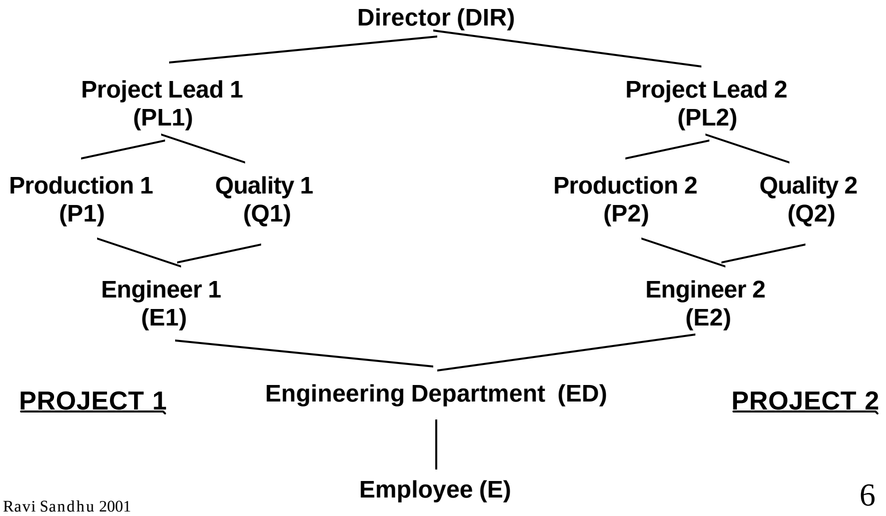
ARBAC97 DECENTRALIZES

- **user-role assignment (URA97)**
- **permission-role assignment (PRA97)**
- **role-role hierarchy**
  - **groups or user-only roles (extend URA97)**
  - **abilities or permission-only roles (extend PRA97)**
  - **UP-roles or user-and-permission roles (RRA97)**

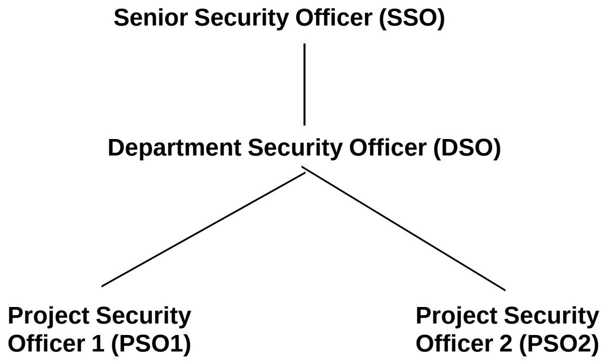
ADMINISTRATIVE RBAC



EXAMPLE ROLE HIERARCHY



EXAMPLE ADMINISTRATIVE ROLE HIERARCHY


Senior Security Officer (SSO)
Department Security Officer (DSO)
Project Security Officer 1 (PSO1)
Project Security Officer 2 (PSO2)

URA97 GRANT MODEL: can-assign

ARole	Prereq Role	Role Range
PSO1	ED	[E1,PL1)
PSO2	ED	[E2,PL2)
DSO	ED	(ED,DIR)
SSO	E	[ED,ED]
SSO	ED	(ED,DIR]

URA97 GRANT MODEL : can-assign

ARole	Prereq Cond	Role Range
PSO1	ED	[E1,E1]
PSO1	ED & ¬ P1	[Q1,Q1]
PSO1	ED & ¬ Q1	[P1,P1]
PSO2	ED	[E2,E2]
PSO2	ED & ¬ P2	[Q2,Q2]
PSO2	ED & ¬ Q2	[P2,P2]

URA97 GRANT MODEL

- **“redundant” assignments to senior and junior roles**
  - **are allowed**
  - **are useful**

URA97 REVOKE MODEL

- **WEAK REVOCATION**
  - **revokes explicit membership in a role**
  - **independent of who did the assignment**

URA97 REVOKE MODEL

- **STRONG REVOCATION**
  - **revokes explicit membership in a role <u>and</u> its seniors**
  - **authorized only if corresponding weak revokes are authorized**
  - **alternatives**
    - **all-or-nothing**
    - **revoke within range**

URA97 REVOKE MODEL : can-revoke

ARole	Role Range
PSO1	[E1,PL1)
PSO2	[E2,PL2)
DSO	(ED,DIR)
SSO	[ED,DIR]

PERMISSION-ROLE ASSIGNMENT

- dual of user-role assignment
- can-assign-permission
  can-revoke-permission
- weak revoke
  strong revoke (propagates down)

PERMISSION-ROLE ASSIGNMENT CAN-ASSIGN-PERMISSION

ARole	Prereq Cond	Role Range
PSO1	PL1	[E1,PL1)
PSO2	PL2	[E2,PL2)
DSO	E1 Ú E2	[ED,ED]
SSO	PL1 Ú PL2	[ED,ED]
SSO	ED	[E,E]

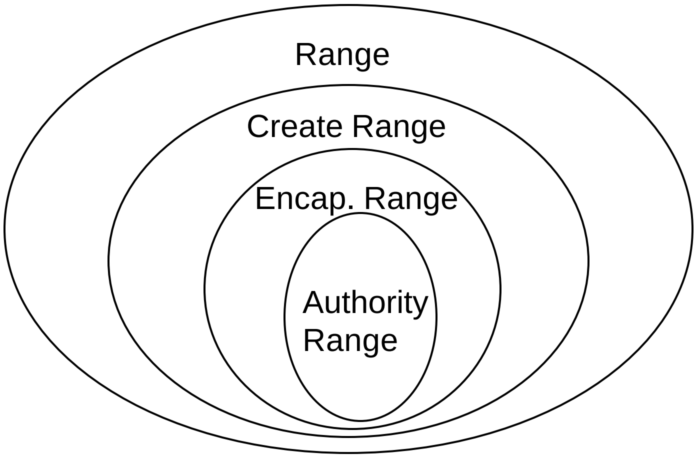
PERMISSION-ROLE ASSIGNMENT CAN-REVOKE-PERMISSION

ARole	Role Range
PSO1	[E1,PL1]
PSO2	[E2,PL2]
DSO	(ED,DIR)
SSO	[ED,DIR]

ARBAC97 DECENTRALIZES

- ❖ **user-role assignment (URA97)**
- ❖ **permission-role assignment (PRA97)**
- ❖ **role-role hierarchy**
  - **groups or user-only roles (extend URA97)**
  - **abilities or permission-only roles (extend PRA97)**
  - **UP-roles or user-and-permission roles (RRA97)**

Range Definitions



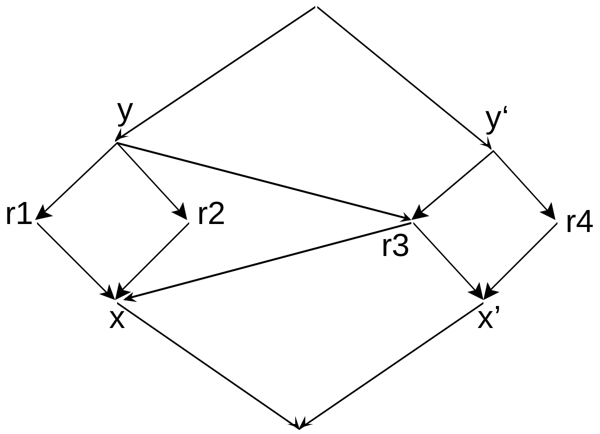
Authority Range

- ❖ **Range:**
  - ➢ **(x, y) = {r : Roles | x < r < y}**
- ❖ **Authority Range:**
  - ➢ **A range referenced in *can-modify* relation**
- ❖ **Partial Overlap of Ranges:**
  - ➢ **The ranges Y and Y’ partially overlap if**
    - **Y Ç Y’ ¹ f and**
    - **Y Ë Y’ Ù Y’ Ë Y**
- ❖ **Partial Overlap of Authority Ranges is forbidden**

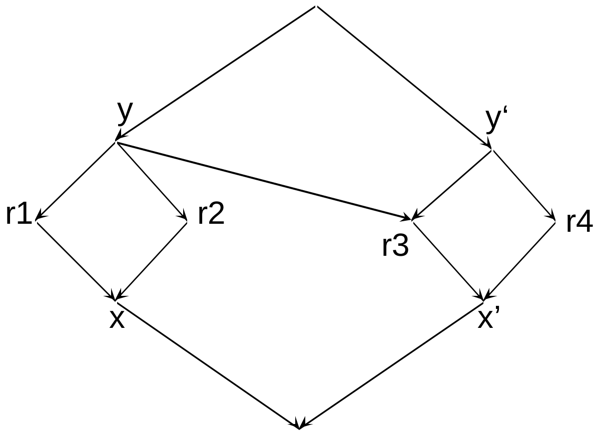
Authority Range

- ❖ **Encapsulated Authority Range:**
  - ➢ **The authority range (x, y) is said to be encapsulated if**
    - **" r1 Î (x, y) and " r2 Ï (x, y)**
      - – r2 > r1 ⇔ r2 > y ∧
      - – r2 < r1 ⇔ r2 < x

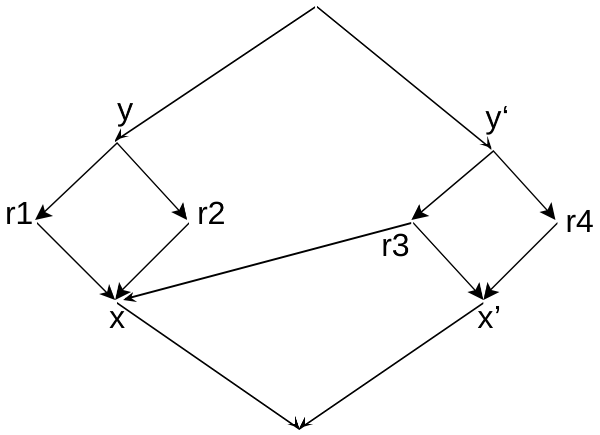
Non-encapsulated Range (x, y)



Encapsulated Range (x, y)



Encapsulated Range (x, y)



ROLE CREATION

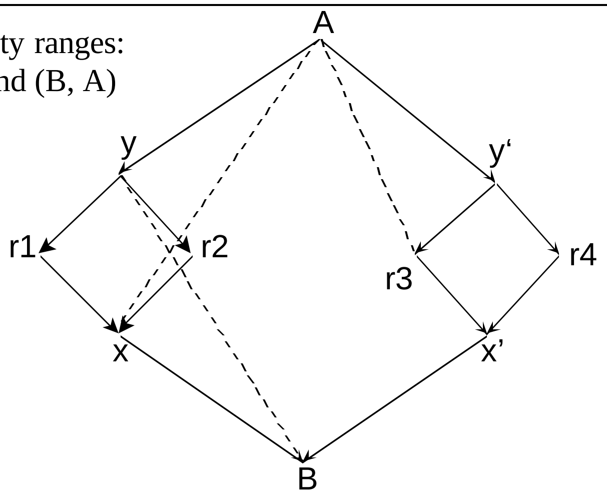
- ❖ **New roles are created one at a time**
- ❖ **Creation of a role requires specification of immediate parent and child**
  - ➢ **immediate parent and child must be a create range**

Role Creation

- **Create Range:**
  - **The range (x, y) is a create range if**
    - **(a) $AR_{immediate}(x) = AR_{immediate}(y)$ Ú**
    - **(b) x = End point of $AR_{immediate}(y)$ Ú**
    - **(c) y = End point of $AR_{immediate}(x)$**
  - **Note: only comparable roles constitute a create range.**

Create Range

Authority ranges:
(x, y) and (B, A)



Role Deletion

- Roles in the authority range can be deleted by administrator of that range.
- End points of authority ranges cannot be deleted.

Inactive Roles

- End points of authority ranges can be made inactive.
- Inactive Roles:
  - A user associated to it cannot use it.
  - Inheritance of permissions is not affected.
  - Permissions and users can be revoked.

Other Restrictions on deletion of roles

- ❖ Roles can be deleted only when they are empty.
- ❖ Delete the role and at the same time:
  - ➢ assign permissions to immediate senior roles.
  - ➢ Assign the users to immediate junior roles.

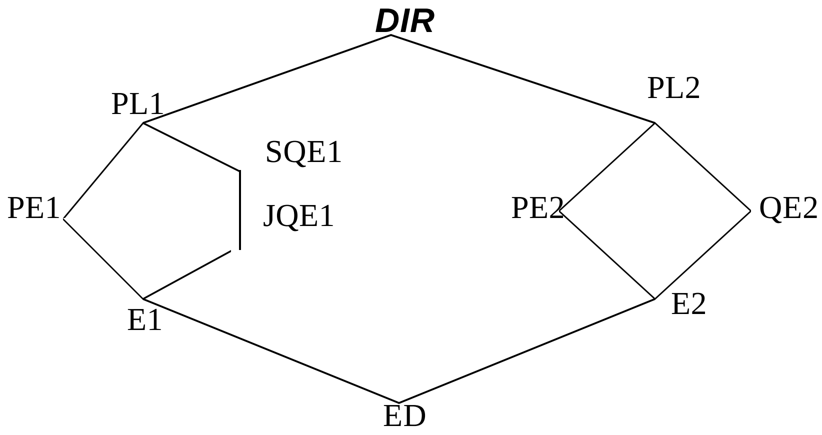
INSERTION OF AN EDGE

- ❖ Inserted only between incomparable roles (No Cycles)
- ❖ Inserted one at a time.
- ❖ The edge AB is inserted if
  - ➢ (a) $AR_{immediate}(A) = AR_{immediate}(B)$ and
  - ➢ (b) For a junior authority range (x, y):
    - (A = y Ù B > x) or (B = x Ù A < y) must ensure encapsulation of (x, y).

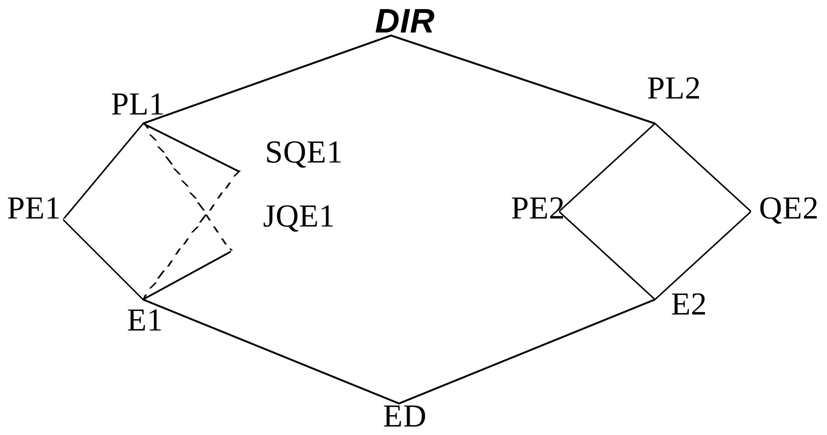
DELETION OF AN EDGE

- ❖ Deleted one at a time.
- ❖ The edges in transitive reduction are candidates for deletion.
- ❖ Edges connecting the end points of an authority range cannot be deleted.
- ❖ Implied edges are not deleted

Example : Before deletion (SQE1, JQE1)



Example : After deletion (SQE1, JQE1)



Conclusion

- ❖ **RRA97 completes ARBAC97**
- ❖ **RRA97 provides decentralized administration of role hierarchies.**
- ❖ **Gives administrative role autonomy within a range but only so far as the side effects of the resulting actions are acceptable.**