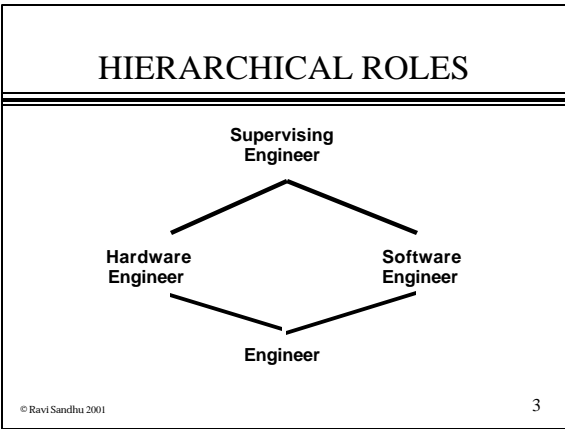
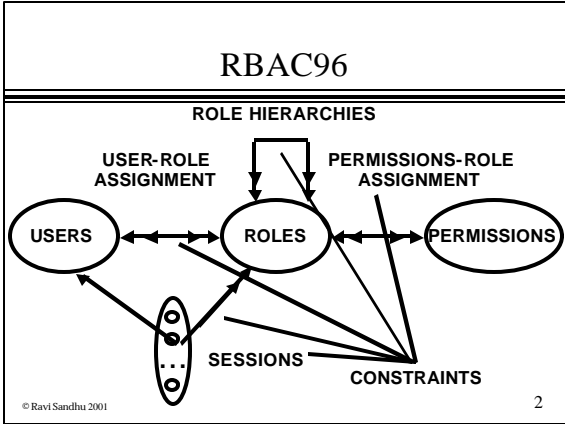


INFS 767 Fall 2001

RBAC-MAC-DAC

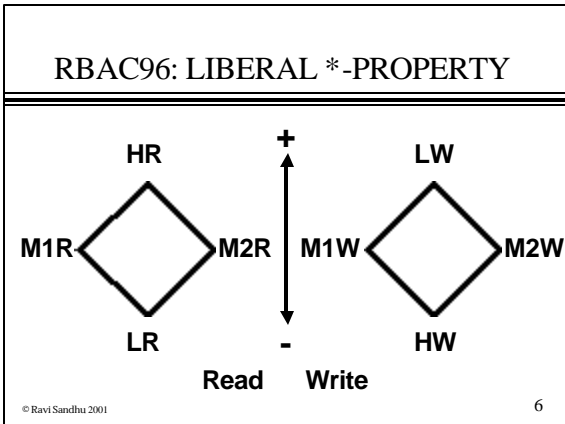
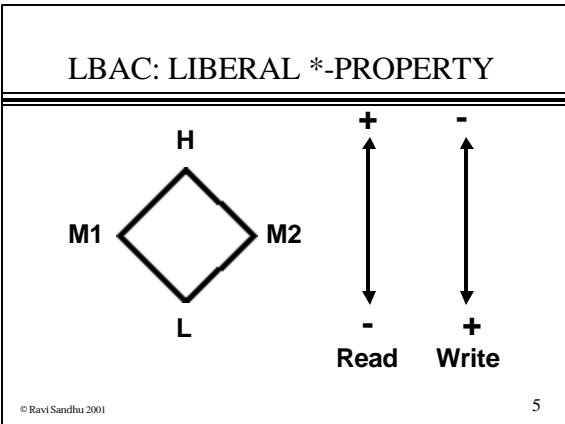
Prof. Ravi Sandhu



WHAT IS THE POLICY IN RBAC?

- ❖ **RBAC is policy neutral**
 - Role hierarchies facilitate security management
 - Constraints facilitate non-discretionary policies

© Ravi Sandhu 2001 4



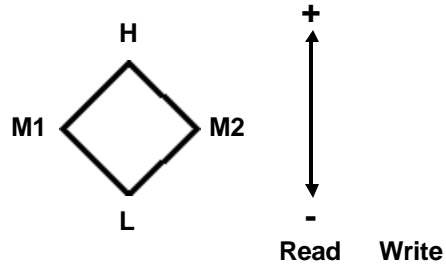
RBAC96: LIBERAL *-PROPERTY

- ❖ user \bar{I} xR, user has clearance x
- user \bar{I} LW, independent of clearance
- ❖ Need constraints
 - > session \bar{I} xR iff session \bar{I} xW
 - > read can be assigned only to xR roles
 - > write can be assigned only to xW roles
 - > (O,read) assigned to xR iff (O,write) assigned to xW

© Ravi Sandhu 2001

7

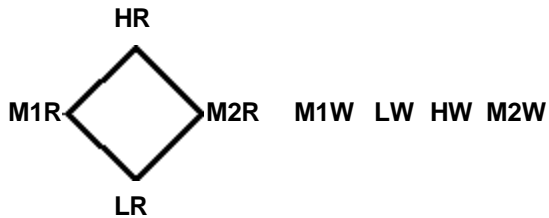
LBAC: STRICT *-PROPERTY



© Ravi Sandhu 2001

8

RBAC96: STRICT *-PROPERTY



© Ravi Sandhu 2001

9

Variations of DAC

- ❖ Strict DAC
- ❖ Liberal DAC

© Ravi Sandhu 2001

10

Strict DAC

- ❖ Only owner has discretionary authority to grant access to an object.
- ❖ Example:
 - > Alice has created an object (she is owner) and grants access to Bob. Now Bob cannot grant propagate the access to another user.

© Ravi Sandhu 2001

11

Liberal DAC

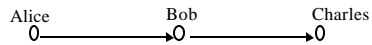
- ❖ Owner can delegate discretionary authority for granting access to other users.
 - > One Level grant
 - > Two Level Grant
 - > Multilevel Grant

© Ravi Sandhu 2001

12

One Level Grant

- ❖ Owner can delegate authority to another user but they cannot further delegate this power.

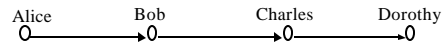


© Ravi Sandhu 2001

13

Two Level Grant

- ❖ In addition a one level grant the owner can allow some users to delegate grant authority to other users.



© Ravi Sandhu 2001

14

Revocation

- ❖ Grant-Independent Revocation.
- ❖ Grant-Dependent Revocation.

© Ravi Sandhu 2001

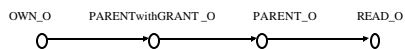
15

Common Aspects

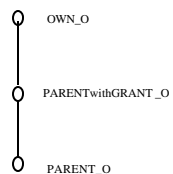
- ❖ Creation of an object in the system requires the simultaneous creation of
 - three administrative roles
 - OWN_O, PARENT_O, PARENTwithGRANT_O
 - One regular role
 - READ_O

© Ravi Sandhu 2001

16



Administration of roles associated with object O



Administrative role hierarchy

Common Aspects II

- ❖ We require simultaneous creation of Eight Permissions
 - canRead_O
 - destroyObjet_O
 - addReadUser_O, deleteReadUser_O
 - addParent_O, deleteParent_O
 - addParentWithGrant_O, deleteParentWithGrant_O

© Ravi Sandhu 2001

18

Roles and associated Permissions

- ❖ **OWN_O**
 - destroyObject_O, addParentWithGrant_O, deleteParentWithgrant_O
- ❖ **PARENTwithGRANT_O**
 - addParent_O, deleteParent_O
- ❖ **PARENT_O**
 - addReadUser_O, deleteReadUser_O
- ❖ **READ_O**
 - canRead_O

© Ravi Sandhu 2001

19

Common Aspects III

- ❖ **Destroying an object O requires deletion of four roles and eight permissions in addition of destroying the object O.**

© Ravi Sandhu 2001

20

Strict DAC in RBAC96

- ❖ **Cardinality constraints as:**
 - Role OWN_O = 1
 - Role PARENTwithGRANT_O = 0
 - Role PARENT_O = 0

© Ravi Sandhu 2001

21

One level DAC in RBAC96

- ❖ **Cardinality constraints as:**
 - Role OWN_O = 1
 - Role PARENTwithGRANT_O = 0

© Ravi Sandhu 2001

22

Two Level DAC in RBAC96

- ❖ **Cardinality constraints as:**
 - Role OWN_O = 1

© Ravi Sandhu 2001

23

U1_PARENT_O O-----+0 U1_READ_O

U2_PARENT_O O-----+0 U2_READ_O

Un_PARENT_O O-----+0 Un_READ_O

READ_O role associated with members of PARENT_O

© Ravi Sandhu 2001

24