

WISAC 2000

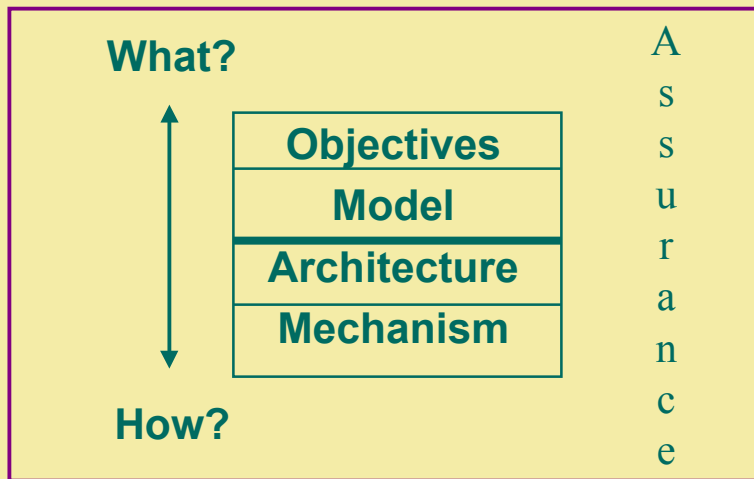
**Strong Access Control:
The OM-AM and RBAC Way**

**Prof. Ravi Sandhu
George Mason University
www.list.gmu.edu
sandhu@gmu.edu**

AUTHORIZATION, TRUST AND RISK

- ◆ **Information security is fundamentally about managing**
 - **authorization and**
 - **trust**
- so as to manage risk**

THE OM-AM WAY



© Ravi Sandhu 2000

3

LAYERS AND LAYERS

- ◆ Multics rings
- ◆ Layered abstractions
- ◆ Waterfall model
- ◆ Network protocol stacks
- ◆ Napoleon layers
- ◆ RoFi layers
- ◆ OM-AM
- ◆ etcetera

© Ravi Sandhu 2000

4

OM-AM AND MANDATORY ACCESS CONTROL (MAC)

What?



How?

No information leakage

Lattices (Bell-LaPadula)

Security kernel

Security labels

A
S
S
U
R
A
N
C
E

OM-AM AND DISCRETIONARY ACCESS CONTROL (DAC)

What?



How?

Owner-based discretion

numerous

numerous

ACLs, Capabilities, etc

A
S
S
U
R
A
N
C
E

OM-AM AND ROLE-BASED ACCESS CONTROL (RBAC)

What?



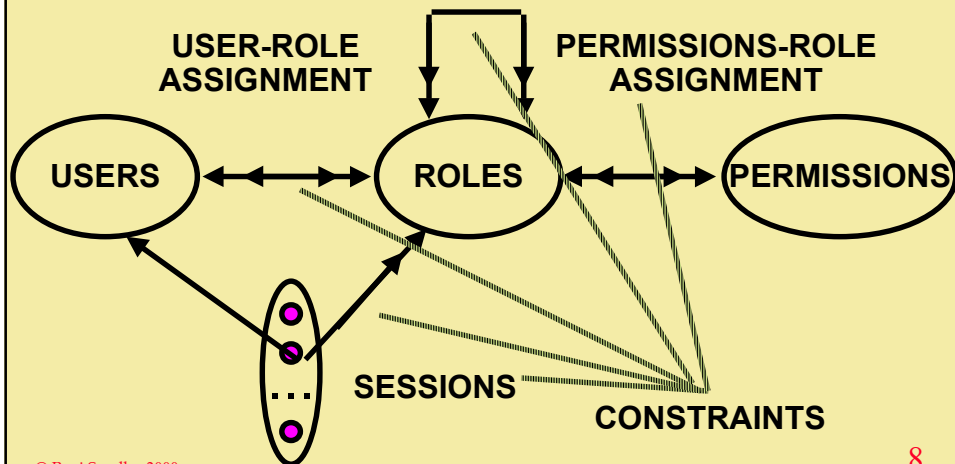
Objective neutral
RBAC96, ARBAC97, etc.
user-pull, server-pull, etc.
certificates, tickets, PACs, etc.

How?

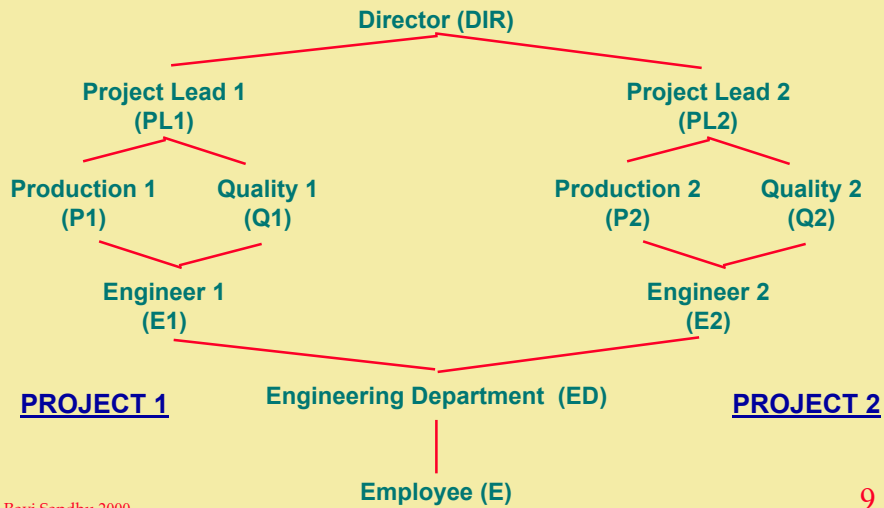
A
S
S
U
R
A
N
C
E

RBAC96

ROLE HIERARCHIES



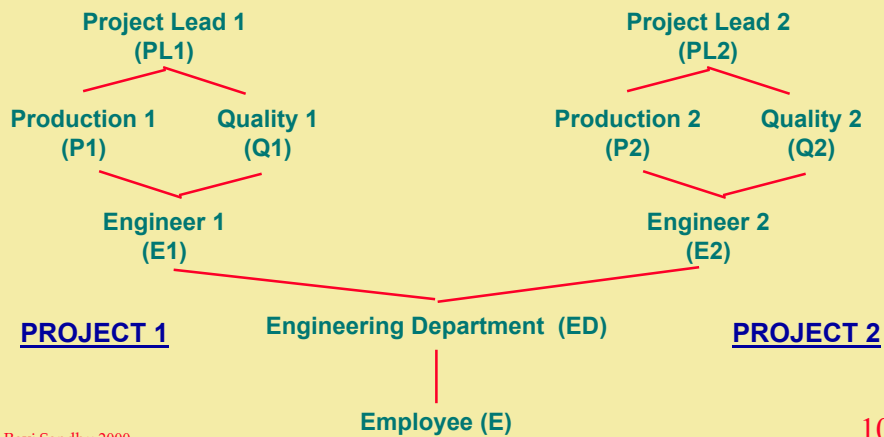
EXAMPLE ROLE HIERARCHY



© Ravi Sandhu 2000

9

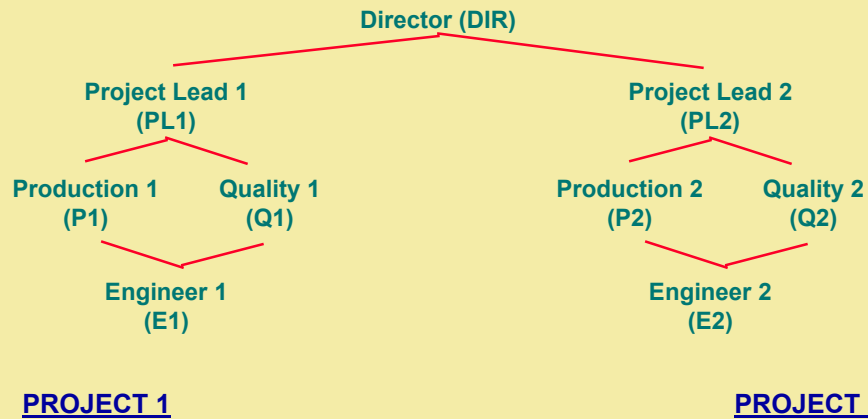
EXAMPLE ROLE HIERARCHY



© Ravi Sandhu 2000

10

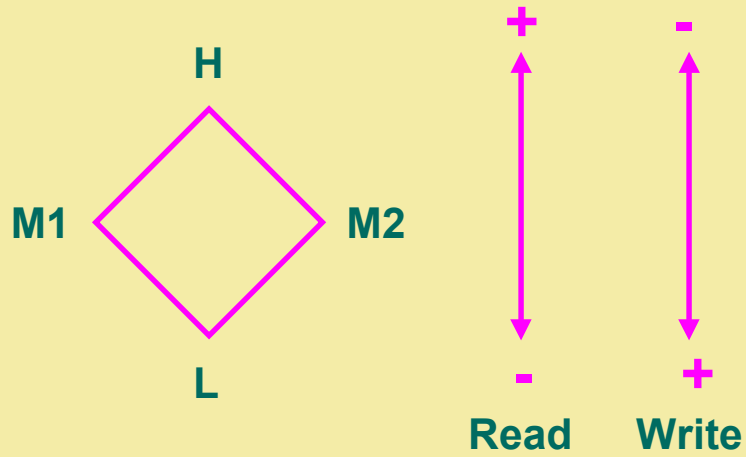
EXAMPLE ROLE HIERARCHY



EXAMPLE ROLE HIERARCHY



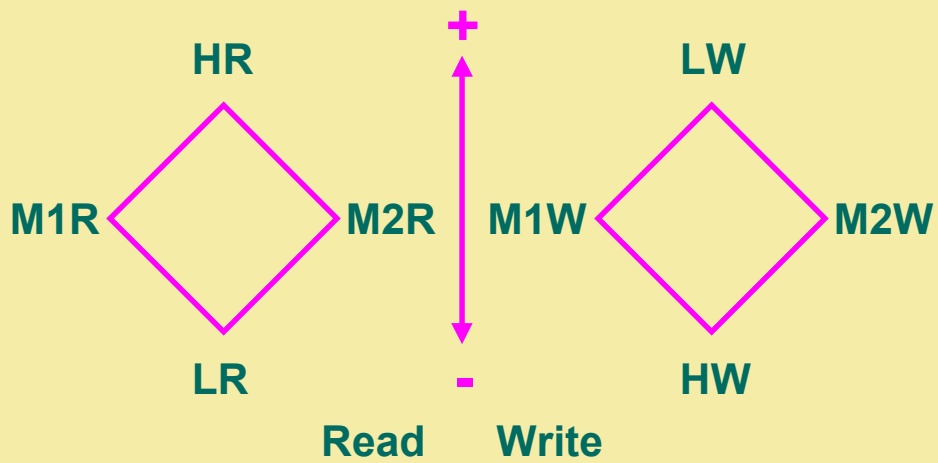
LBAC: LIBERAL *-PROPERTY



© Ravi Sandhu 2000

13

RBAC96: LIBERAL *-PROPERTY



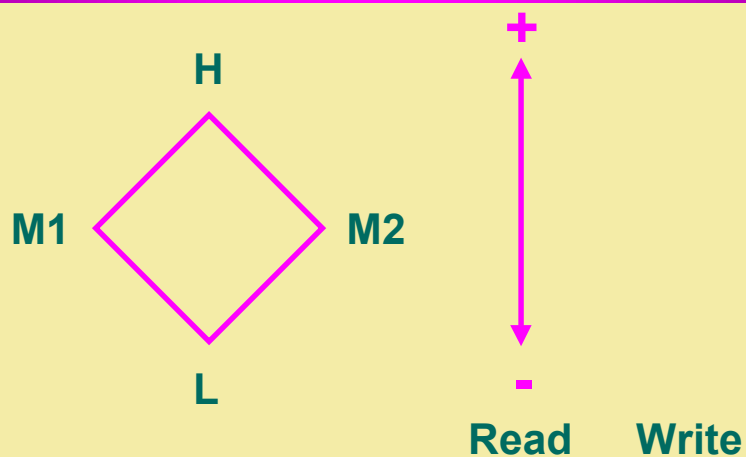
© Ravi Sandhu 2000

14

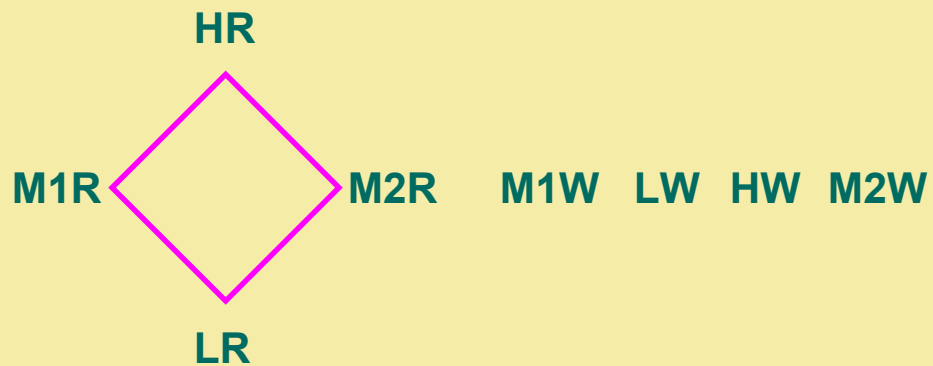
RBAC96: LIBERAL *-PROPERTY

- ◆ **user** \in **xR**, **user** has clearance **x**
user \in **LW**, independent of clearance
- ◆ **Need constraints**
 - **session** \in **xR** iff **session** \in **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**

LBAC: STRICT *-PROPERTY



RBAC96: STRICT *-PROPERTY



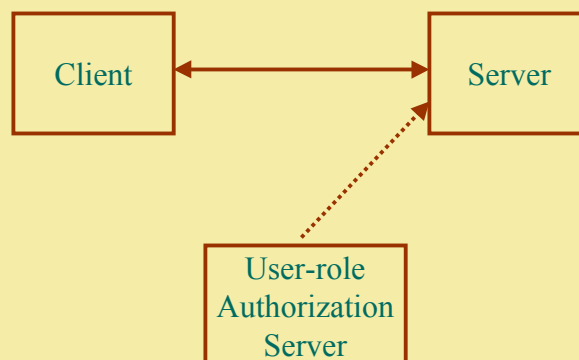
Variations of DAC

- ◆ Strict DAC
- ◆ Liberal DAC

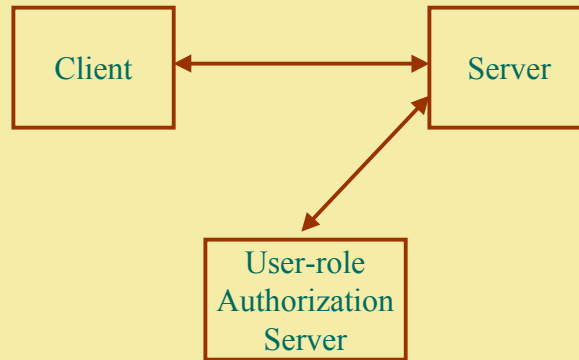
Revocation

- ◆ Grant-Independent Revocation.
- ◆ Grant-Dependent Revocation.

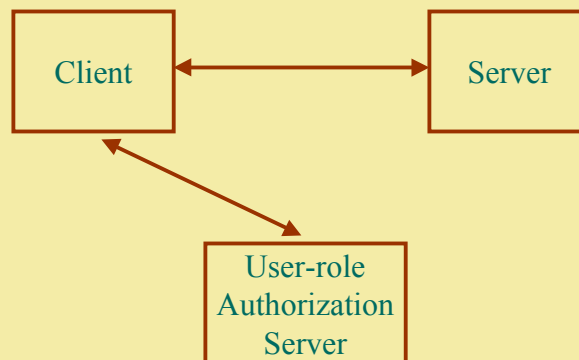
SERVER MIRROR



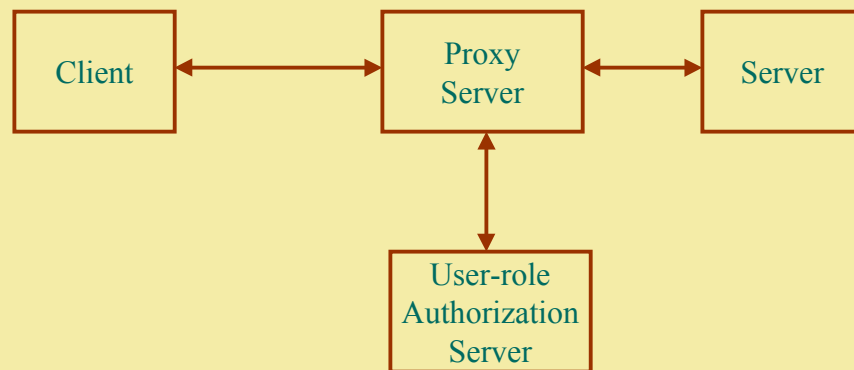
SERVER-PULL



USER-PULL



PROXY-BASED



MECHANISMS

- ◆ **SSL**
- ◆ **X.509 certificates**
- ◆ **Secure cookies**
- ◆ **LDAP**
- ◆ **Etc**