Engineering Authority and Trust in Cyberspace: The OM-AM and RBAC Way

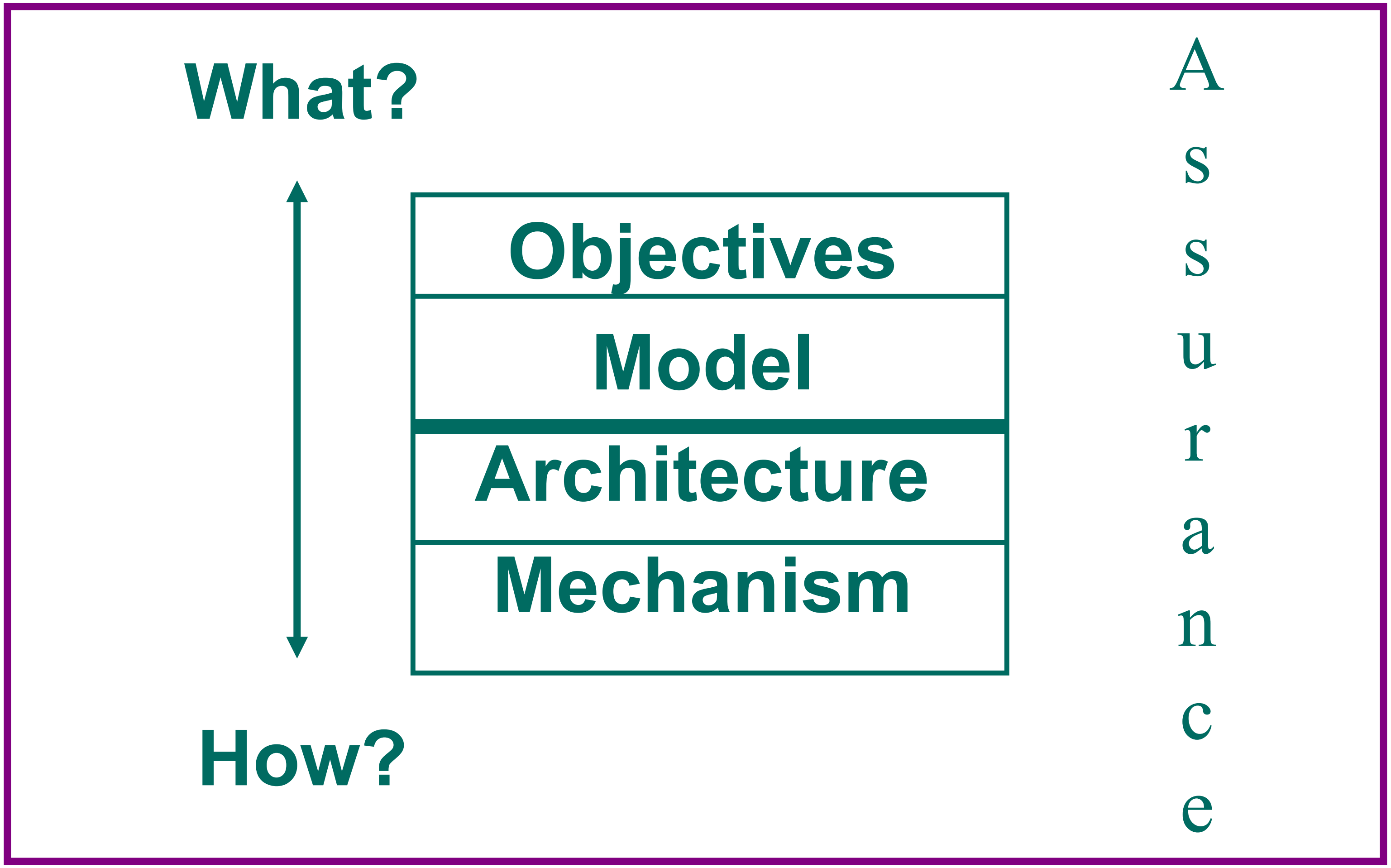
Prof. Ravi Sandhu
George Mason University
www.list.gmu.edu

AUTHORIZATION, TRUST AND RISK

- **Information security is fundamentally about managing**
  - **authorization and**
  - **trust**

  so as to manage risk

THE OM-AM WAY



What?

Objectives

Model

Architecture

Mechanism

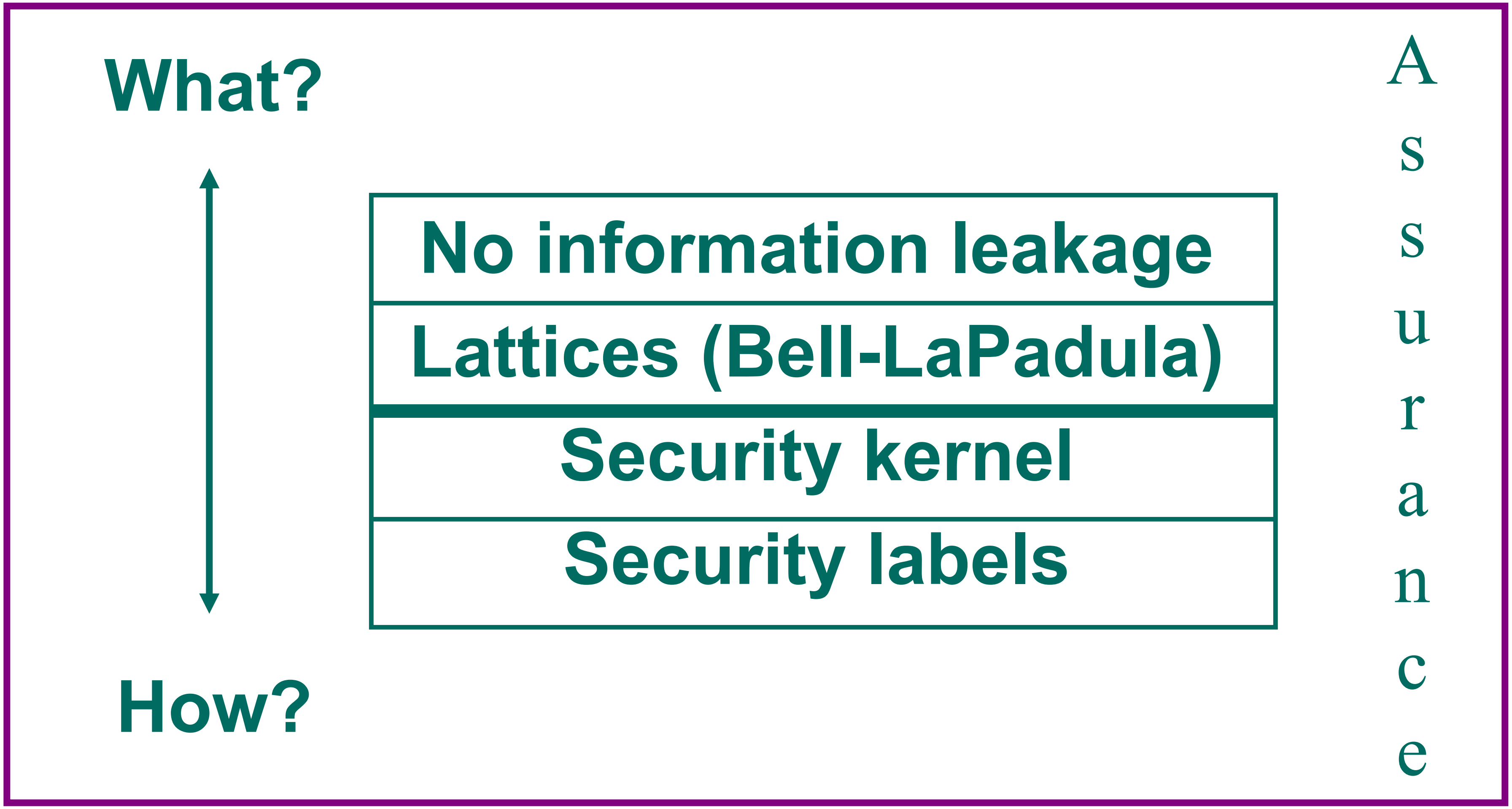
How?

Assurance

LAYERS AND LAYERS

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

OM-AM AND MANDATORY ACCESS CONTROL (MAC)



What?

No information leakage

Lattices (Bell-LaPadula)

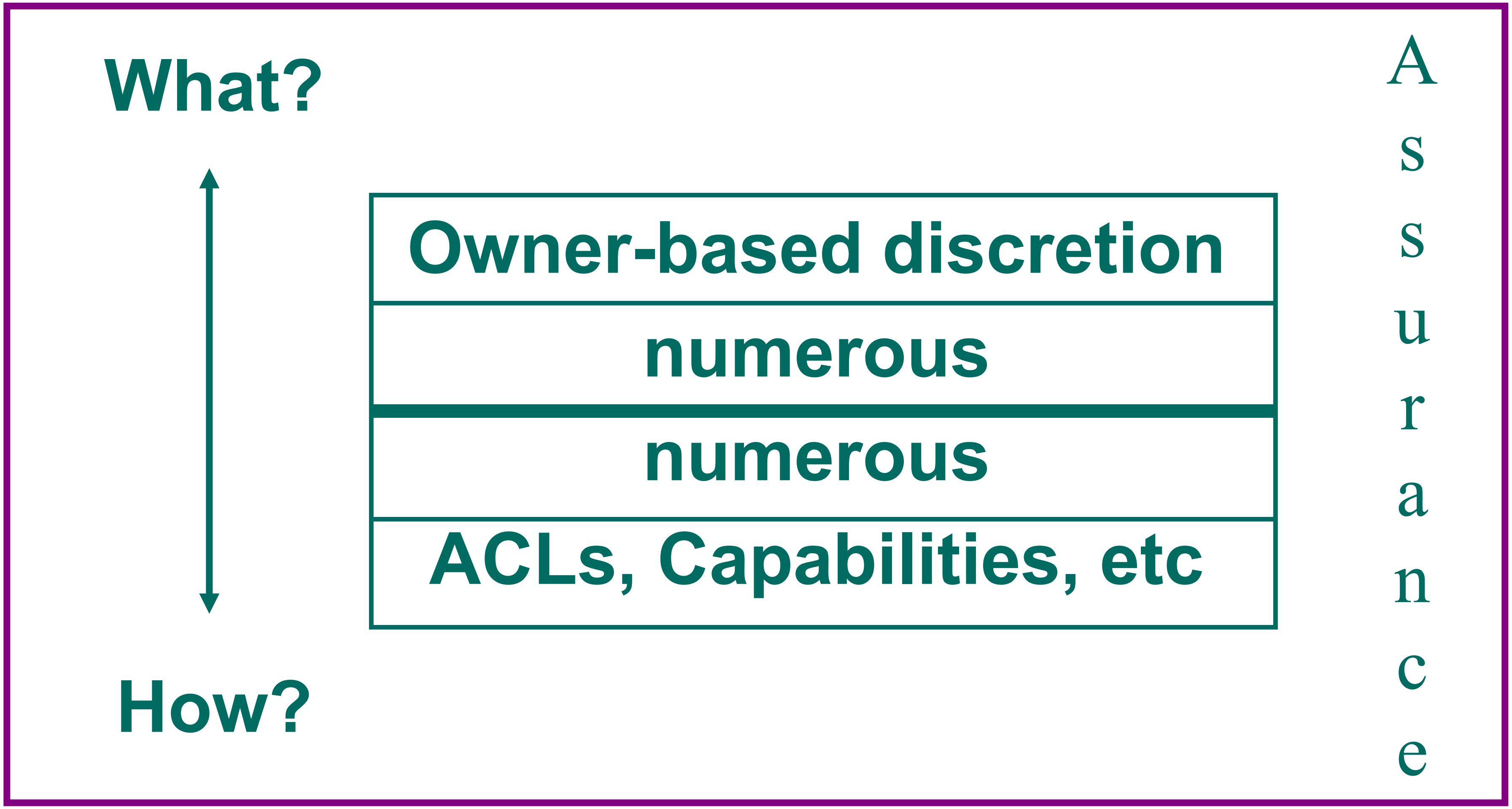
Security kernel

Security labels

How?

Assurance

OM-AM AND DISCRETIONARY ACCESS CONTROL (DAC)



What?

Owner-based discretion

numerous

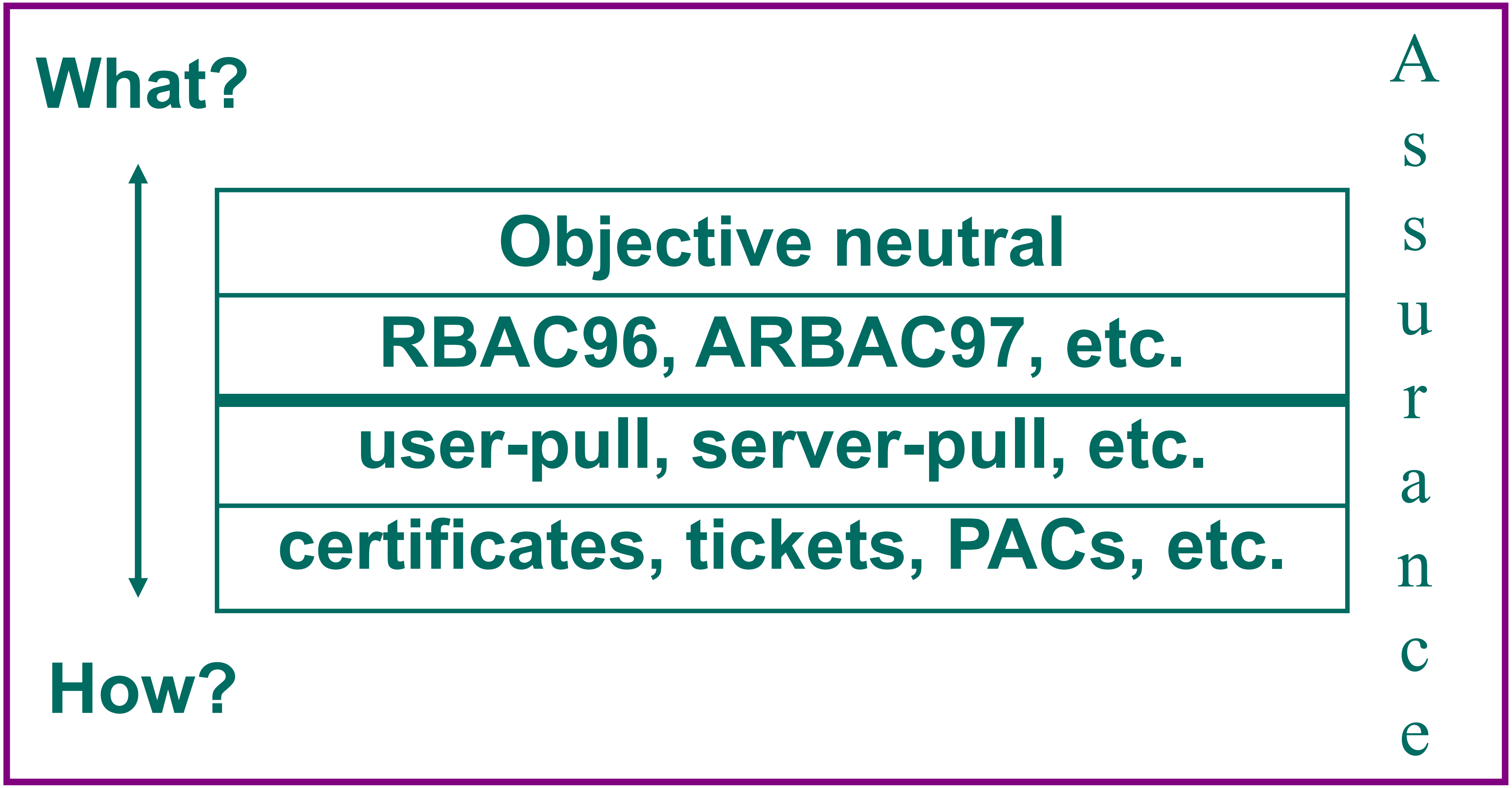
numerous

ACLs, Capabilities, etc

How?

Assurance

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



What?

Objective neutral

RBAC96, ARBAC97, etc.

user-pull, server-pull, etc.

certificates, tickets, PACs, etc.

How?

Assurance

DISTRIBUTED RBAC (DRBAC) CASE STUDY

- Approximately a dozen physical sites
- Approximately 2-3 simulation models/site
- Fewer than 100 roles structured in a very shallow hierarchy
  - A subset of roles is used in any single simulation model
- Fewer than 100 users
- A user uses only one role at a time
  - Convenient but not critical
- Moderate rate of change

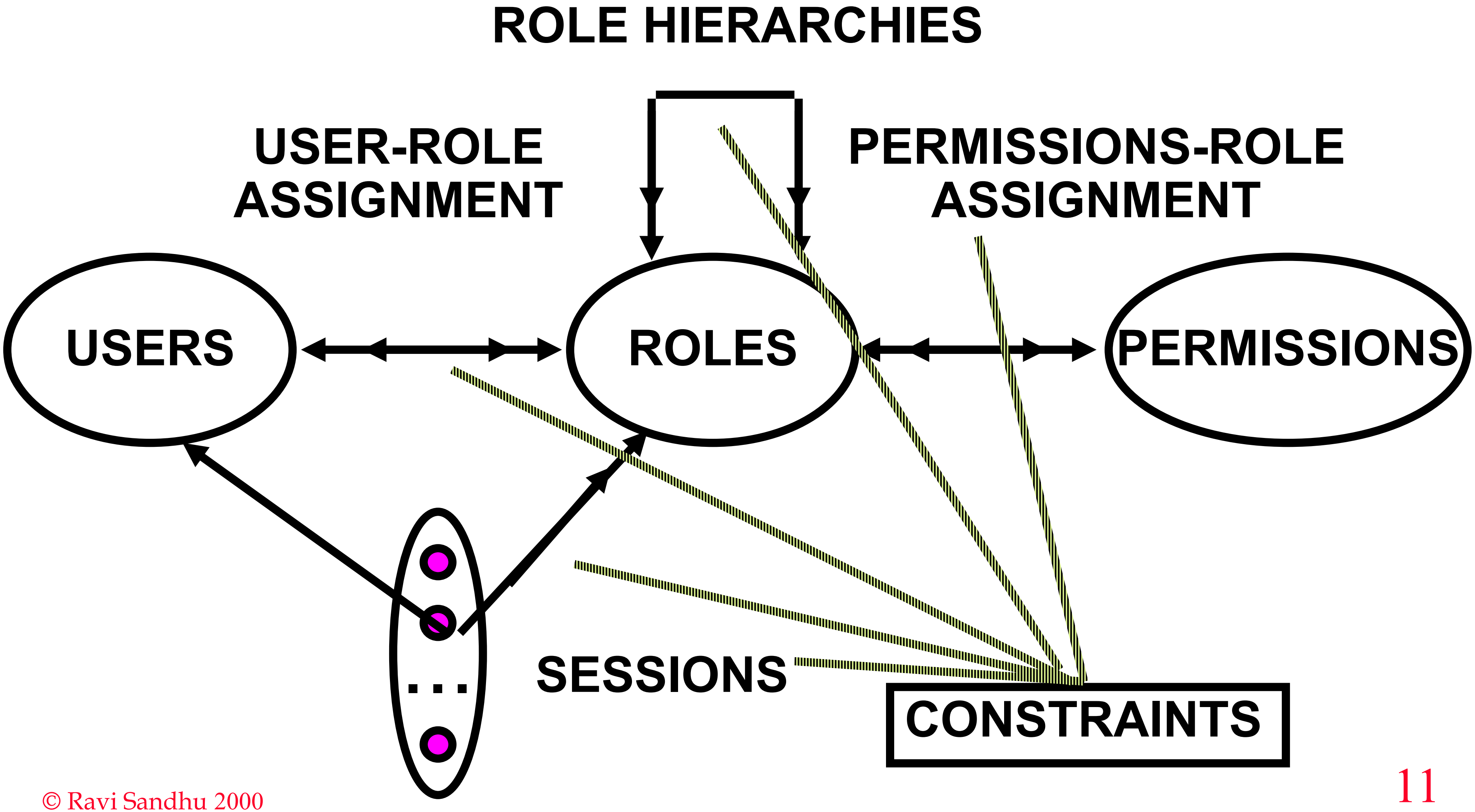
DISTRIBUTED RBAC (DRBAC) CASE STUDY

- Permission-role assignment
  - Locally determined at each simulation model
- User-role assignment
  - A user can be assigned to a role if and only if all simulation models using that role agree
  - A user is revoked from a role if and only if any simulation model using that role revokes the user

DISTRIBUTED RBAC (DRBAC) CASE STUDY

- Each simulation model has a security administrator role authorized to carry out these administrative tasks
- A simulation model can assign permissions to a role X at any time
  - even if X is previously unused in that simulation model
- Consequently any simulation model can revoke any user from any role!

RBAC3



© Ravi Sandhu 2000

MODEL CUSTOMIZATION

- Each session has a single role
- SM = {sm1, …, smk}, simulation models
- OP = {op1, …, opl}, operations
- P= SM X OP, permissions
- SMA = {sma1, …, smk}, administrative roles
- $R \cap SMA = \emptyset$
- Admin: $SM \leftrightarrow SMA$

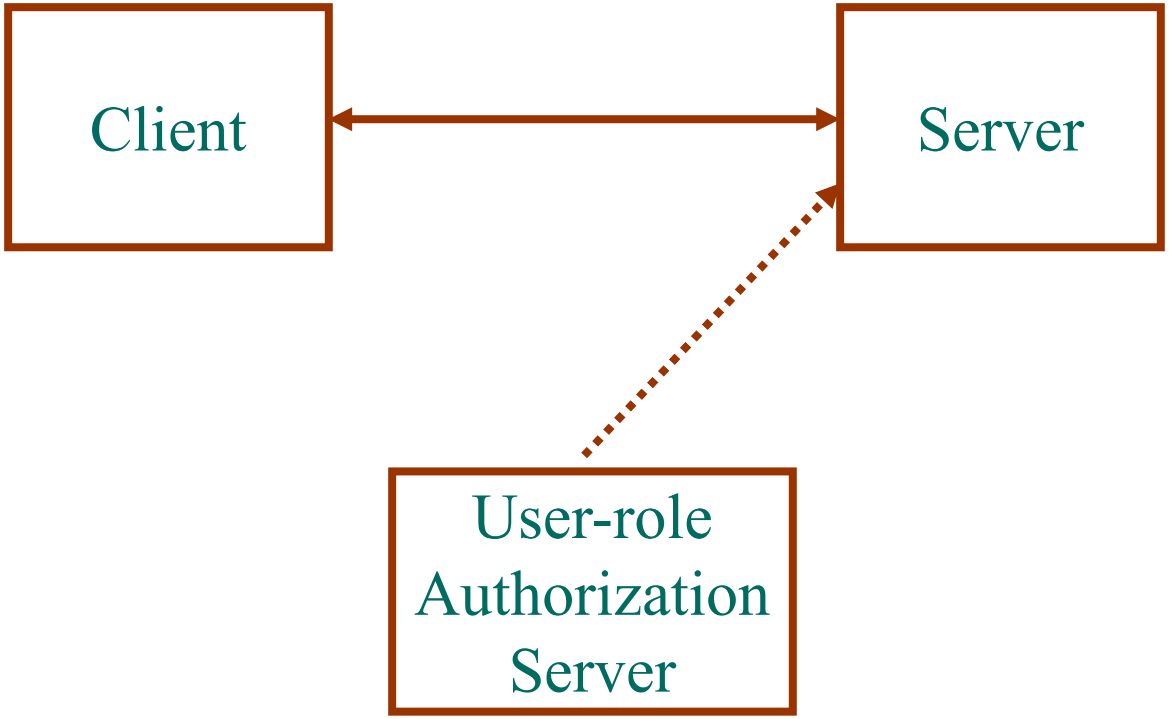
MODEL CUSTOMIZATION

- Can formalize the administrative rules given earlier
- For each simulation model designate a unique user to be the chief security administrator who is authorized to assign and revoke users from the security administrator role for that model

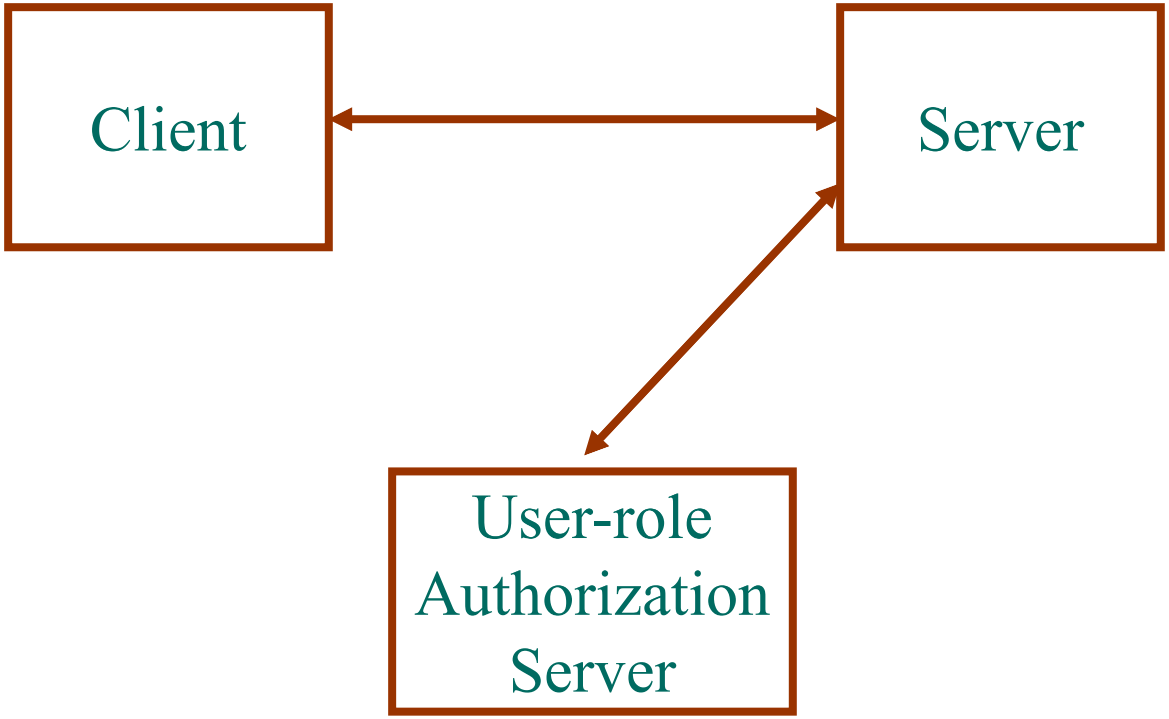
DRBAC ARCHITECTURES

- Permission-role
  - Enforced locally at each simulation model
- Permission-role administration
  - Enforced locally at each simulation model
  - May need to communicate to other simulation models
- User-role
  - See following slides
- User-role administration
  - Centralized or decentralized

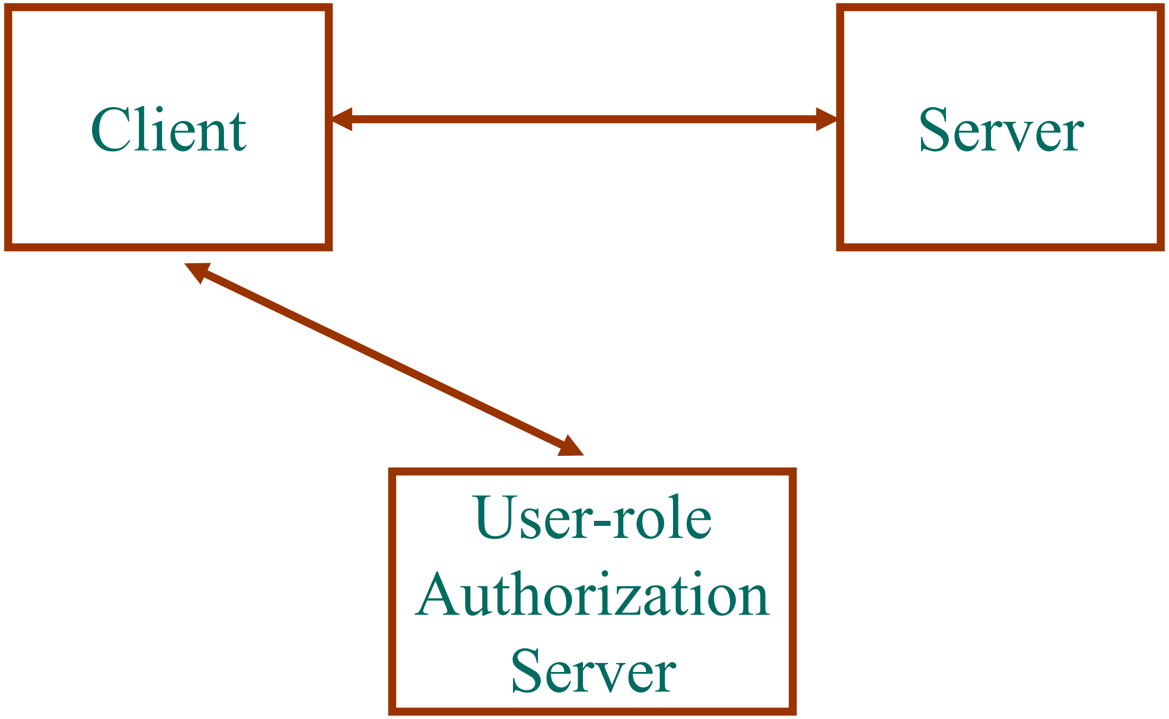
SERVER MIRROR



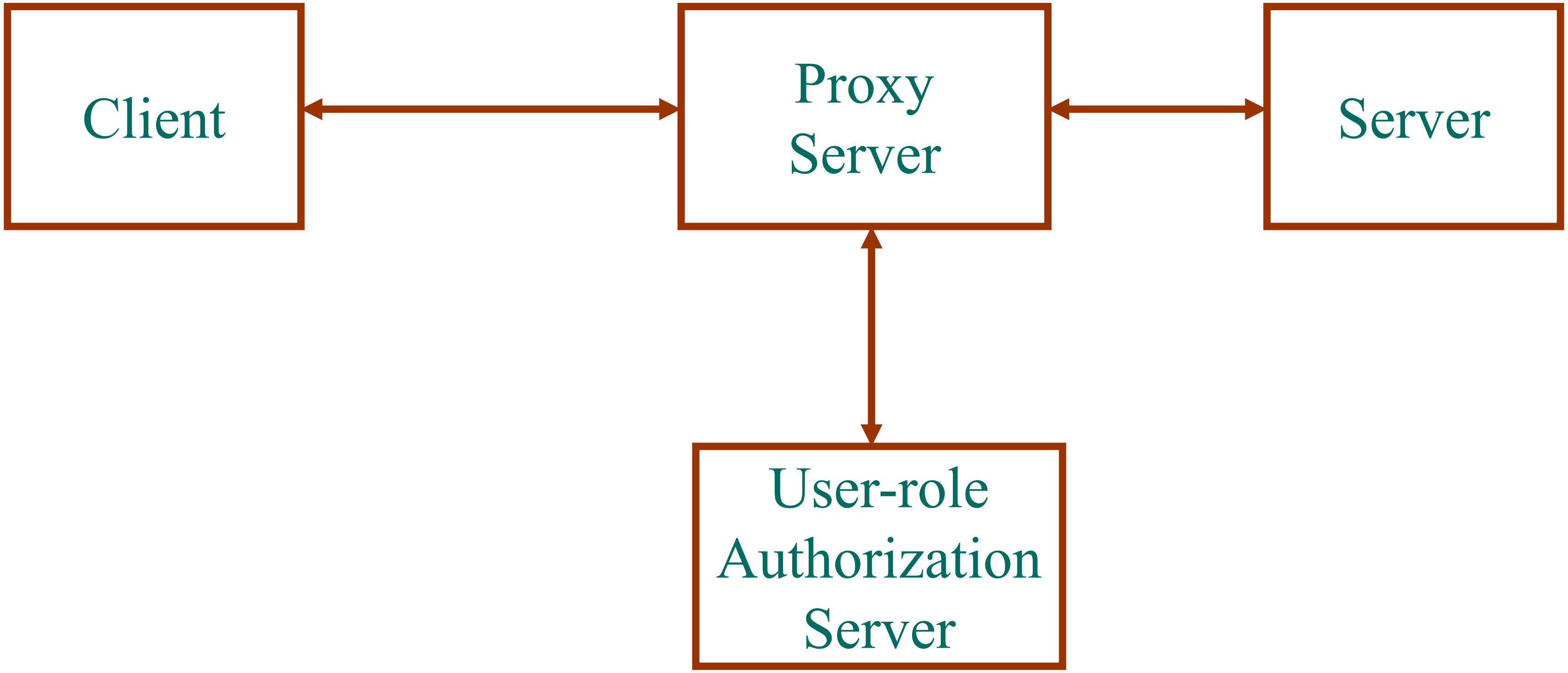
SERVER-PULL



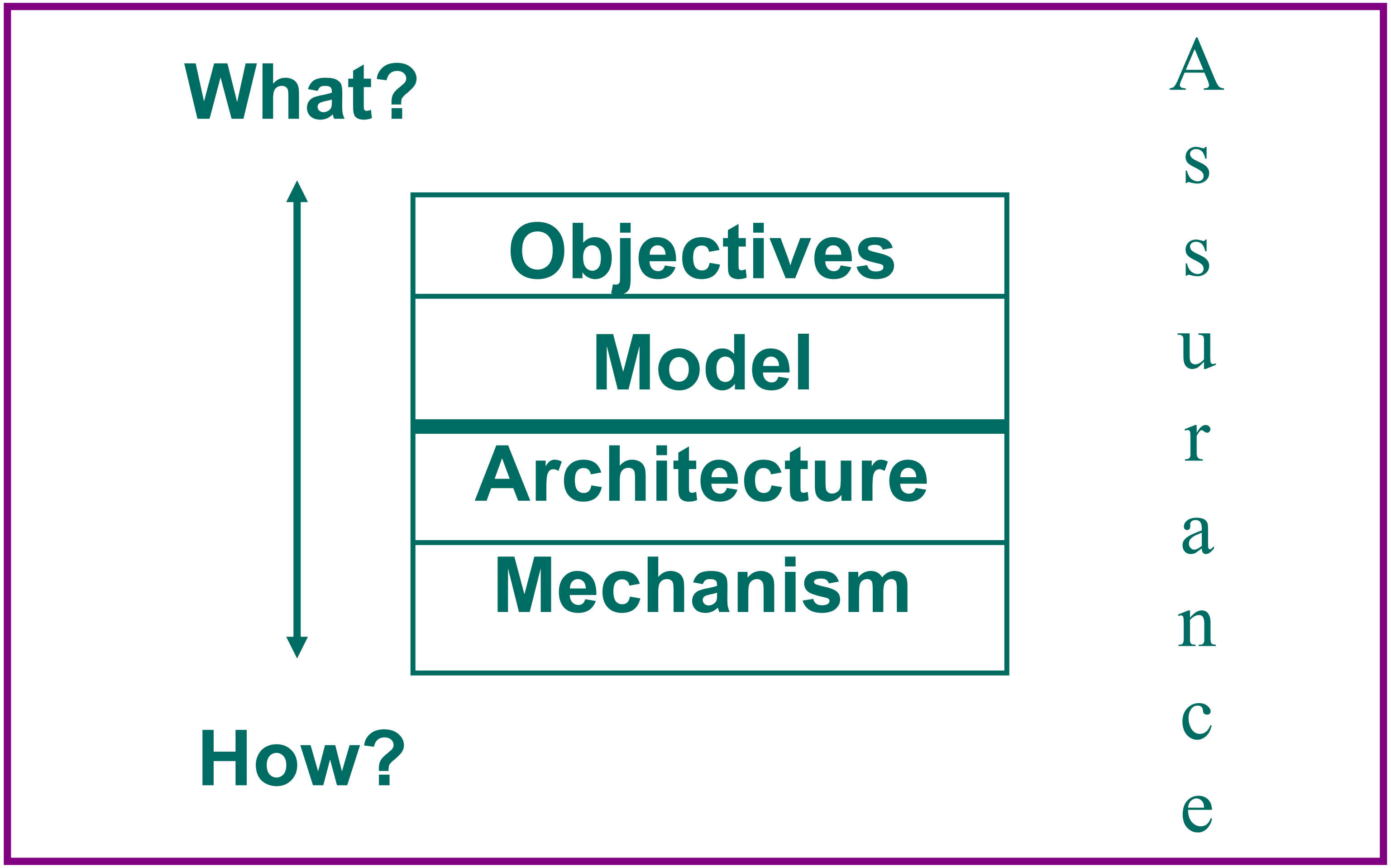
USER-PULL



PROXY-BASED


Client
Proxy Server
Server
User-role Authorization Server

THE OM-AM WAY



What?

Objectives

Model

Architecture

Mechanism

How?

Assurance