Cyber-Identity, Authority and Trust in an Uncertain World

Prof. Ravi Sandhu

Laboratory for Information Security Technology

George Mason University

www.list.gmu.edu

sandhu@gmu.edu

Outline

- Perspective on security
- Role Based Access Control (RBAC)
- Objective Model-Architecture Mechanism (OM-AM) Framework
- Usage Control (UCON)

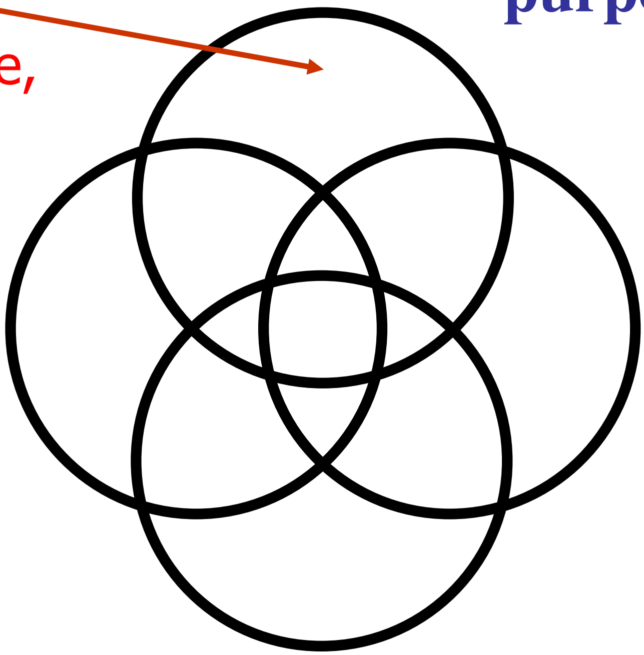
Security Conundrum

- Nobody knows WHAT security is
- Some of us do know HOW to implement pieces of it

Result: hammers in search of nails

Security Confusion

- electronic commerce, electronic business
- DRM, client-side controls



USAGE
purpose

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Successes

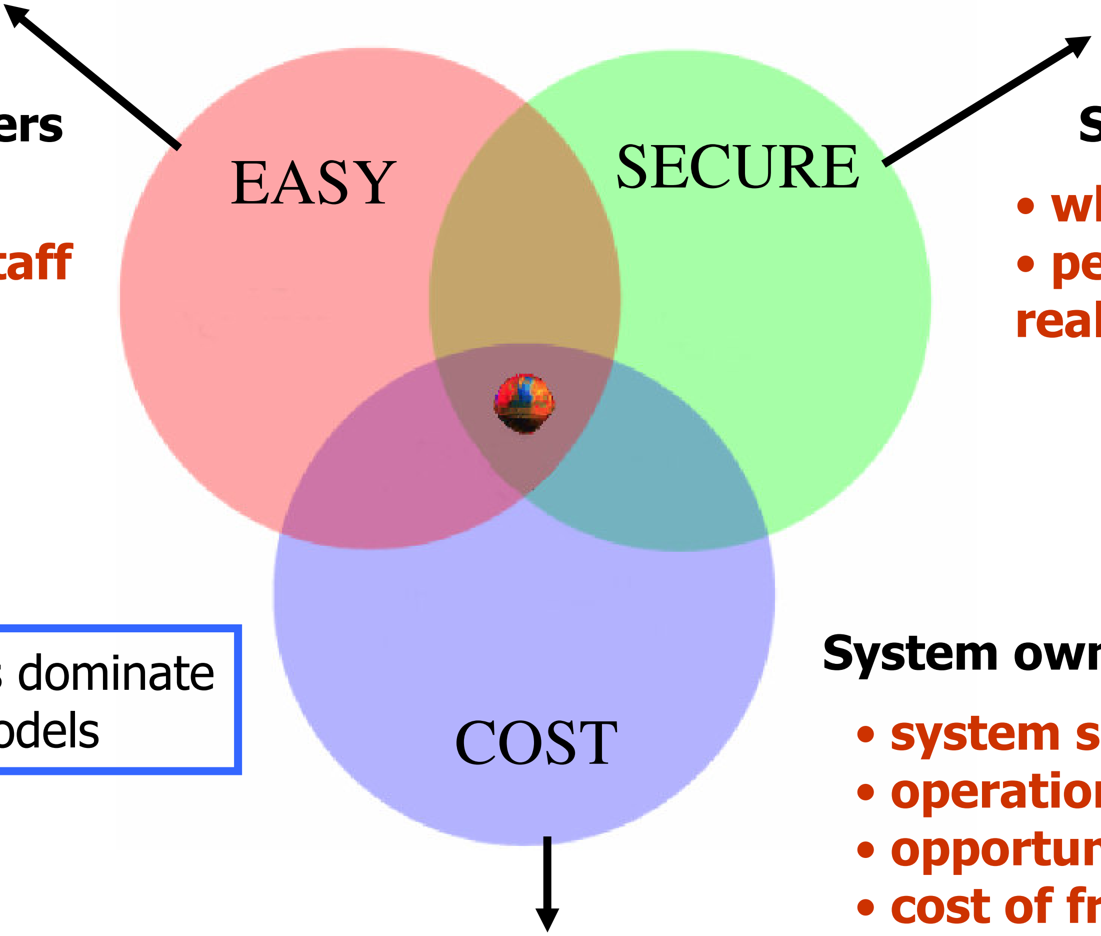
- On-line banking
- On-line trading
- Automatic teller machines (ATMs)
- GSM phones
- Set-top boxes
- ....

Success is largely unrecognized
by the security community

Good enough security

Real-world users

- end users
- operations staff
- help desk



Security geeks

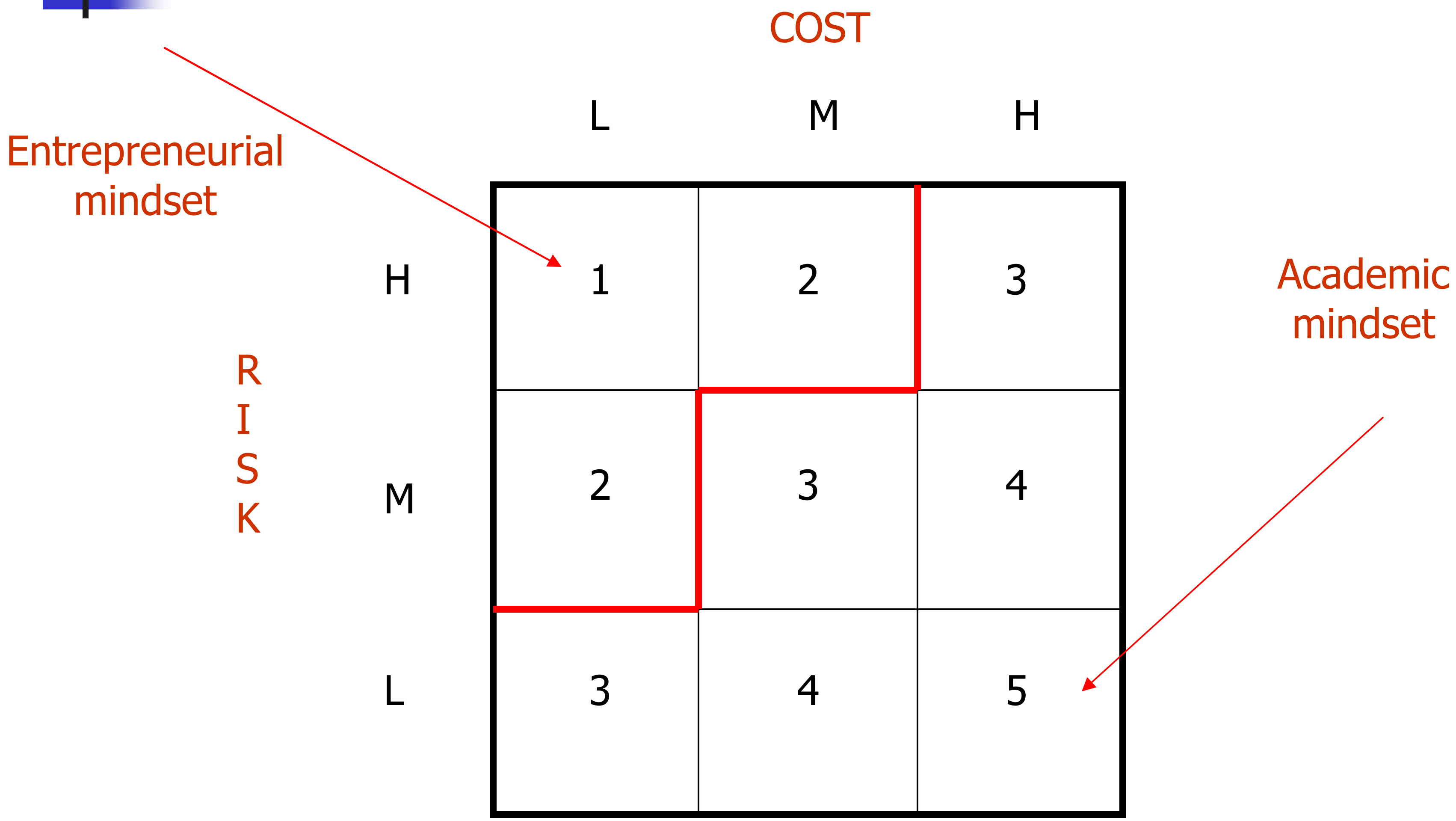
- whose security
- perception or reality of security

System owner

- system solution
- operational cost
- opportunity cost
- cost of fraud

Business models dominate security models

Good enough security



COST

RISK

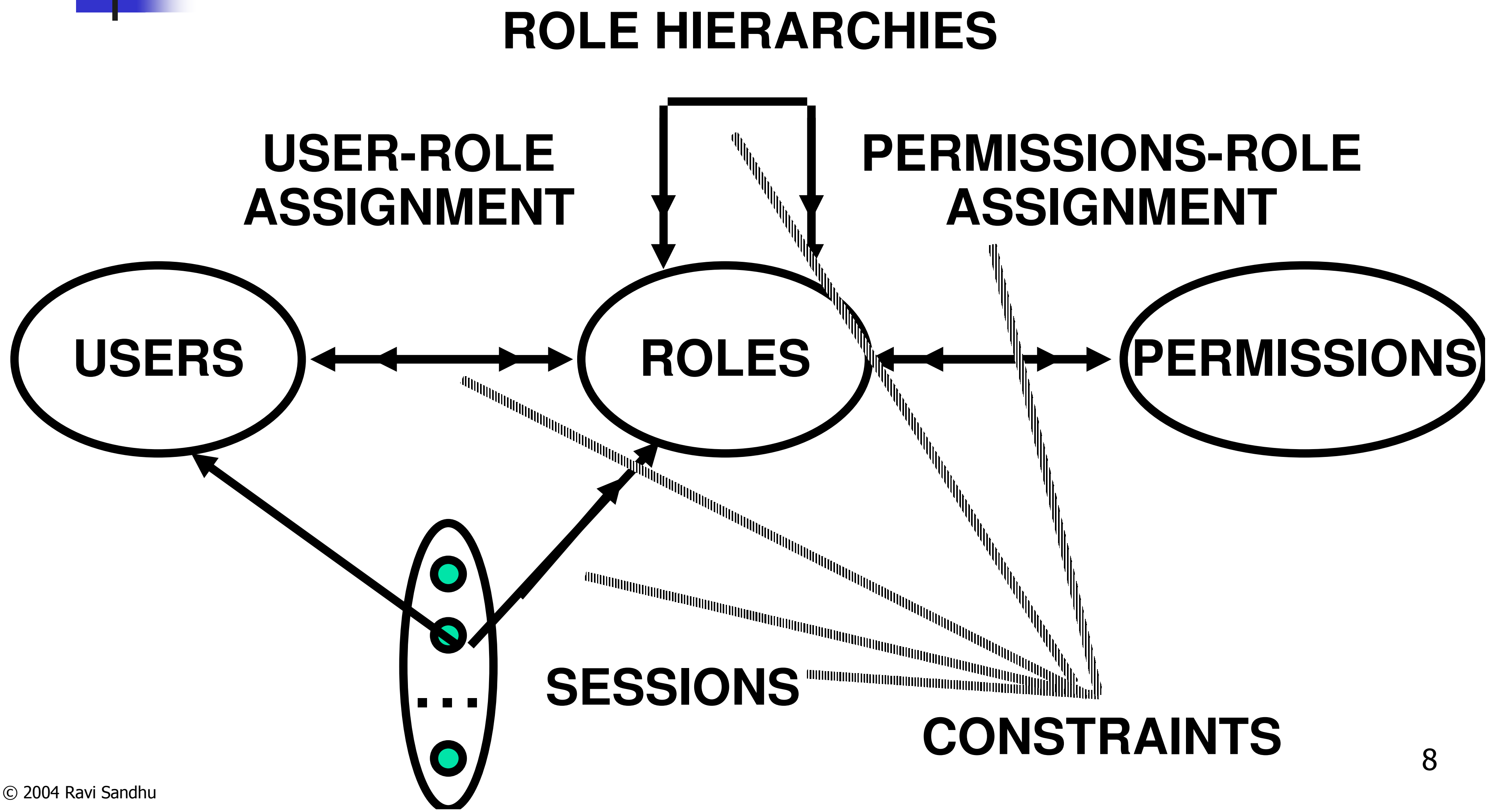
	L	M	H
H	1	2	3
M	2	3	4
L	3	4	5

Entrepreneurial mindset

Academic mindset

RBAC96 model

(Currently foundation of a NIST/ANSI/ISO standard)

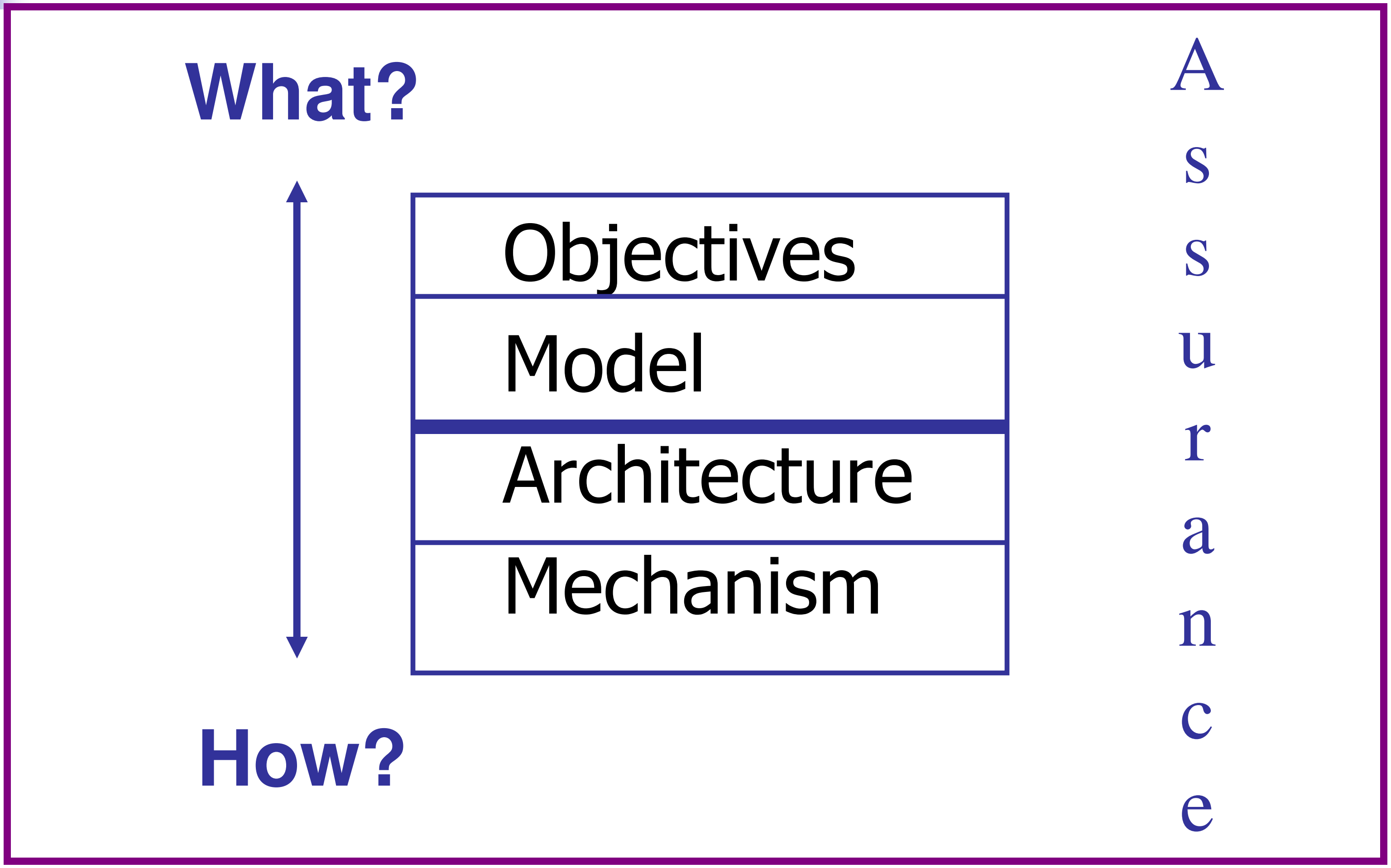


Fundamental Theorem of RBAC

- RBAC can be configured to do MAC
  - MAC is Mandatory Access Control as defined in the Orange Book
- RBAC can be configured to do DAC
  - DAC is Discretionary Access Control as defined in the Orange Book

RBAC is policy neutral

THE OM-AM WAY



What?

Objectives

Model

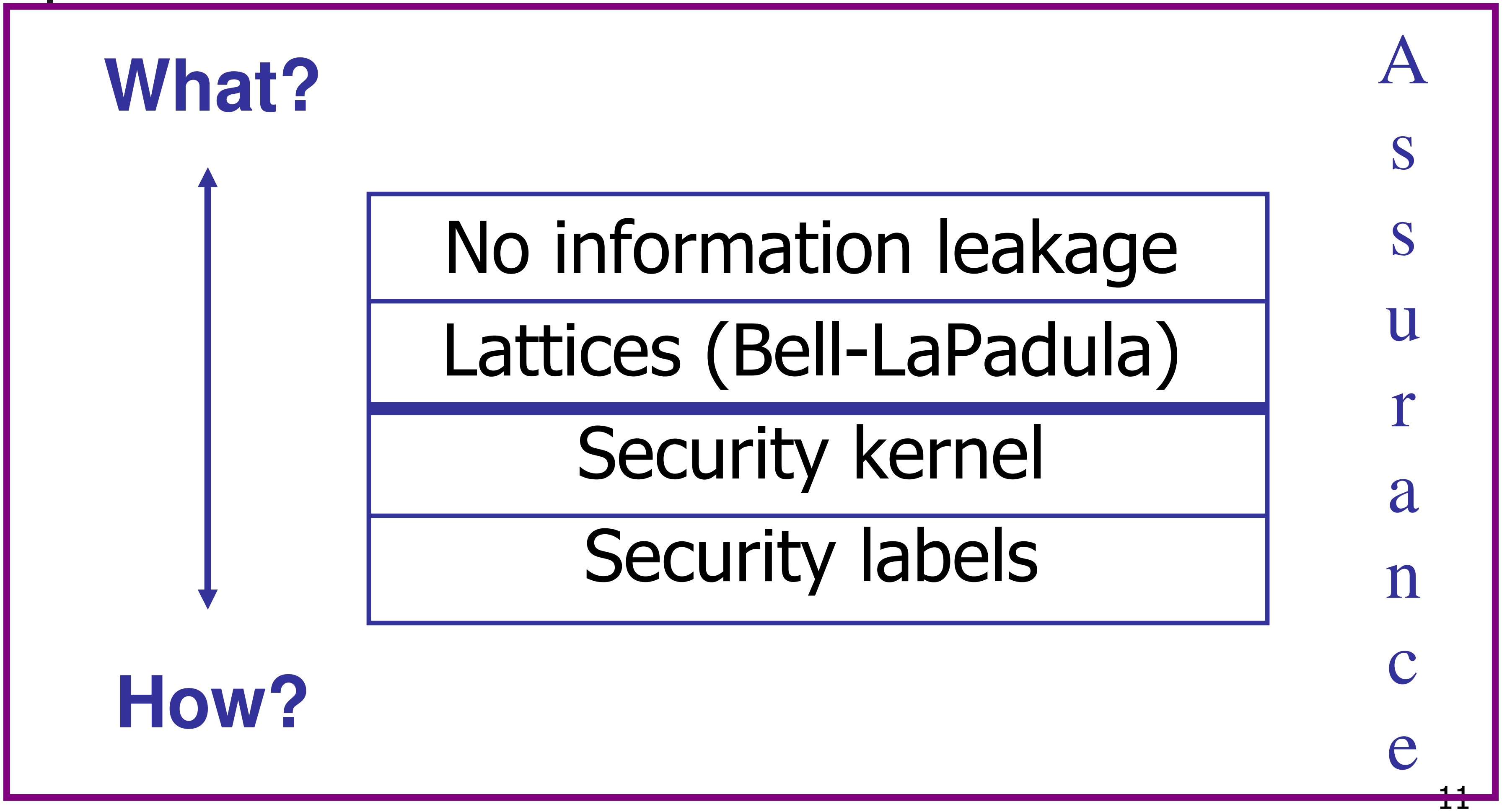
Architecture

Mechanism

How?

Assurance

OM-AM AND MANDATORY ACCESS CONTROL (MAC)



What?

No information leakage

Lattices (Bell-LaPadula)

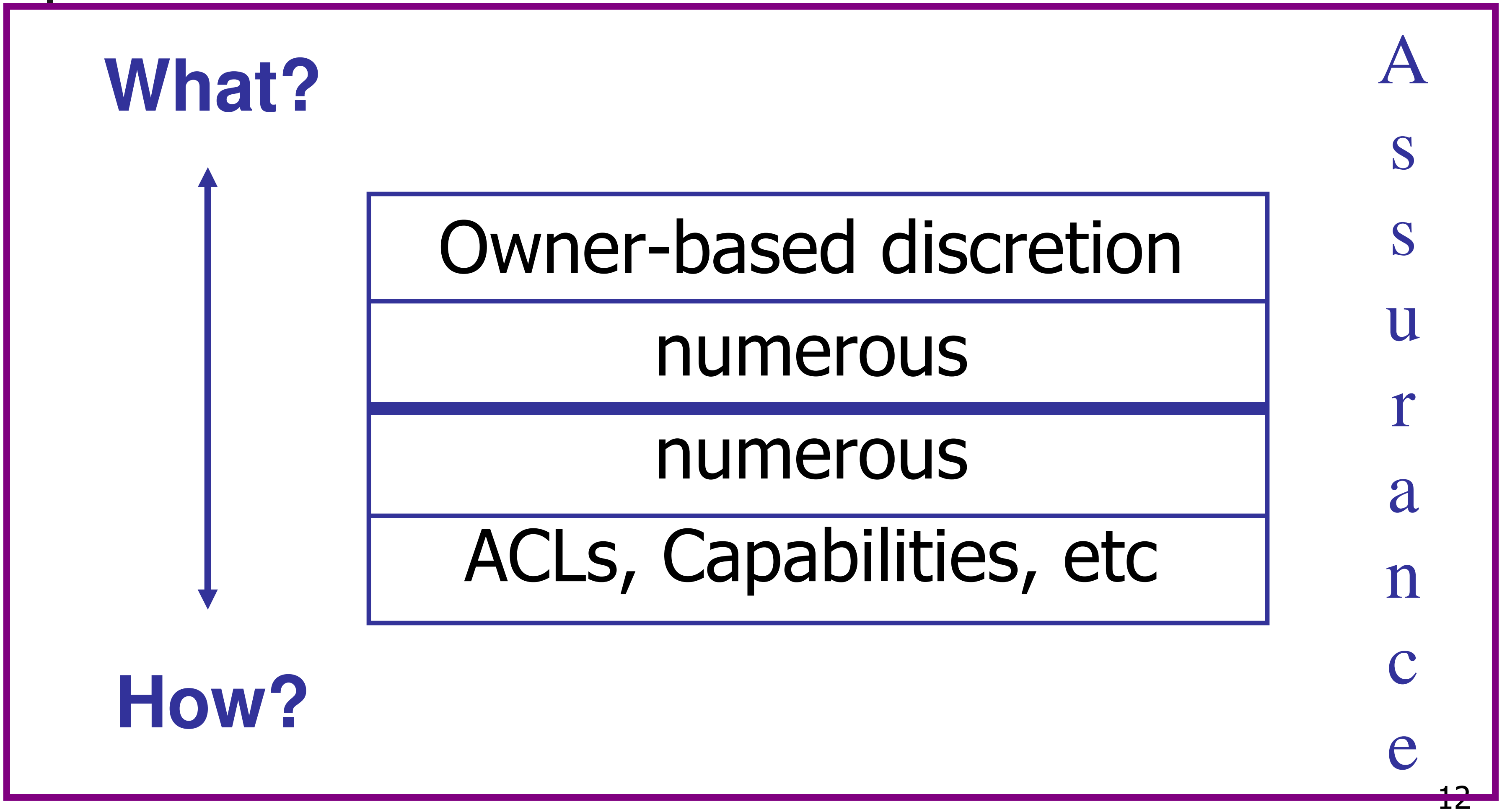
Security kernel

Security labels

How?

Assurance

OM-AM AND DISCRETIONARY ACCESS CONTROL (DAC)



What?

Owner-based discretion

numerous

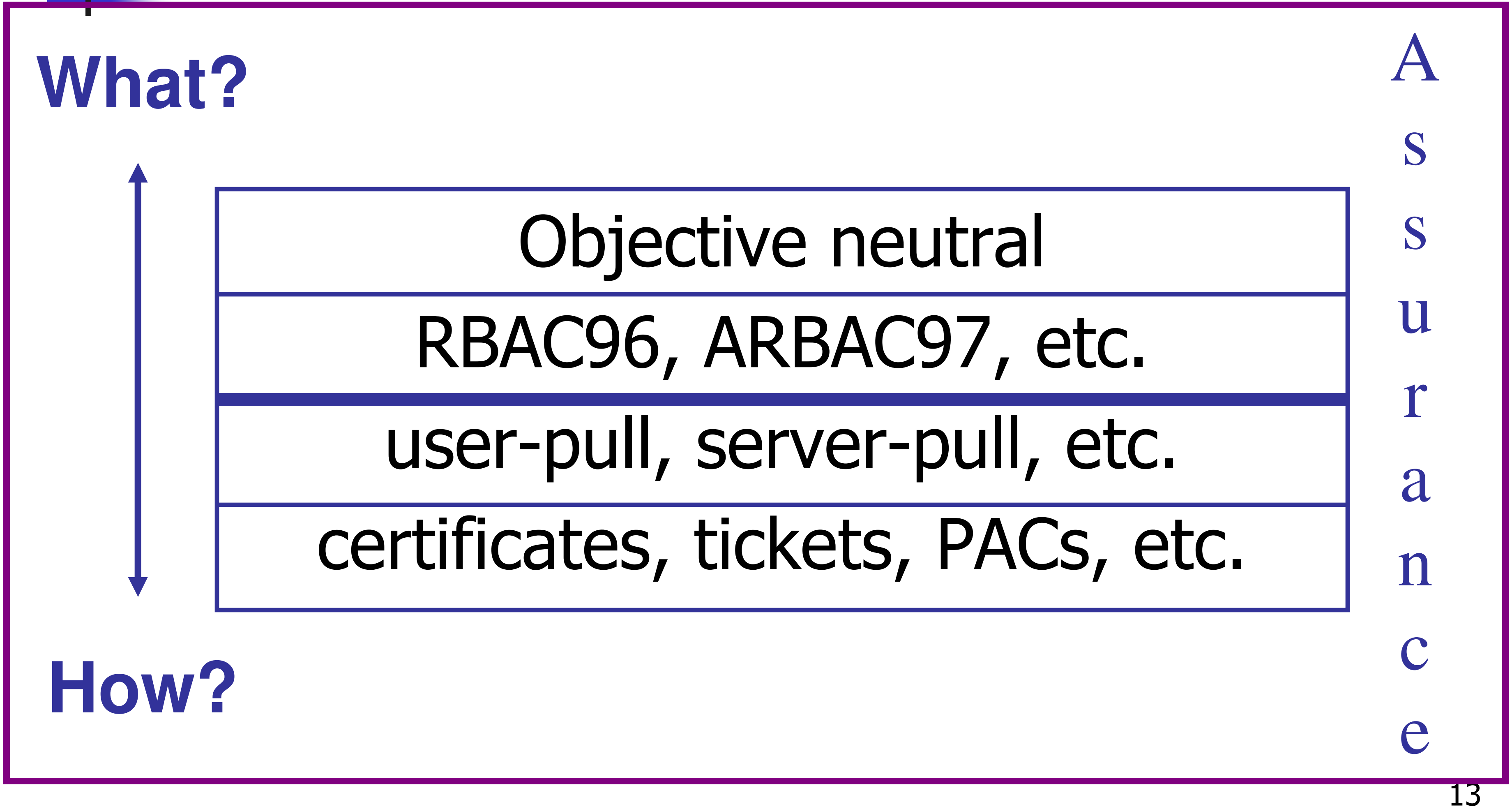
numerous

ACLs, Capabilities, etc

How?

Assurance

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



What?

Objective neutral

RBAC96, ARBAC97, etc.

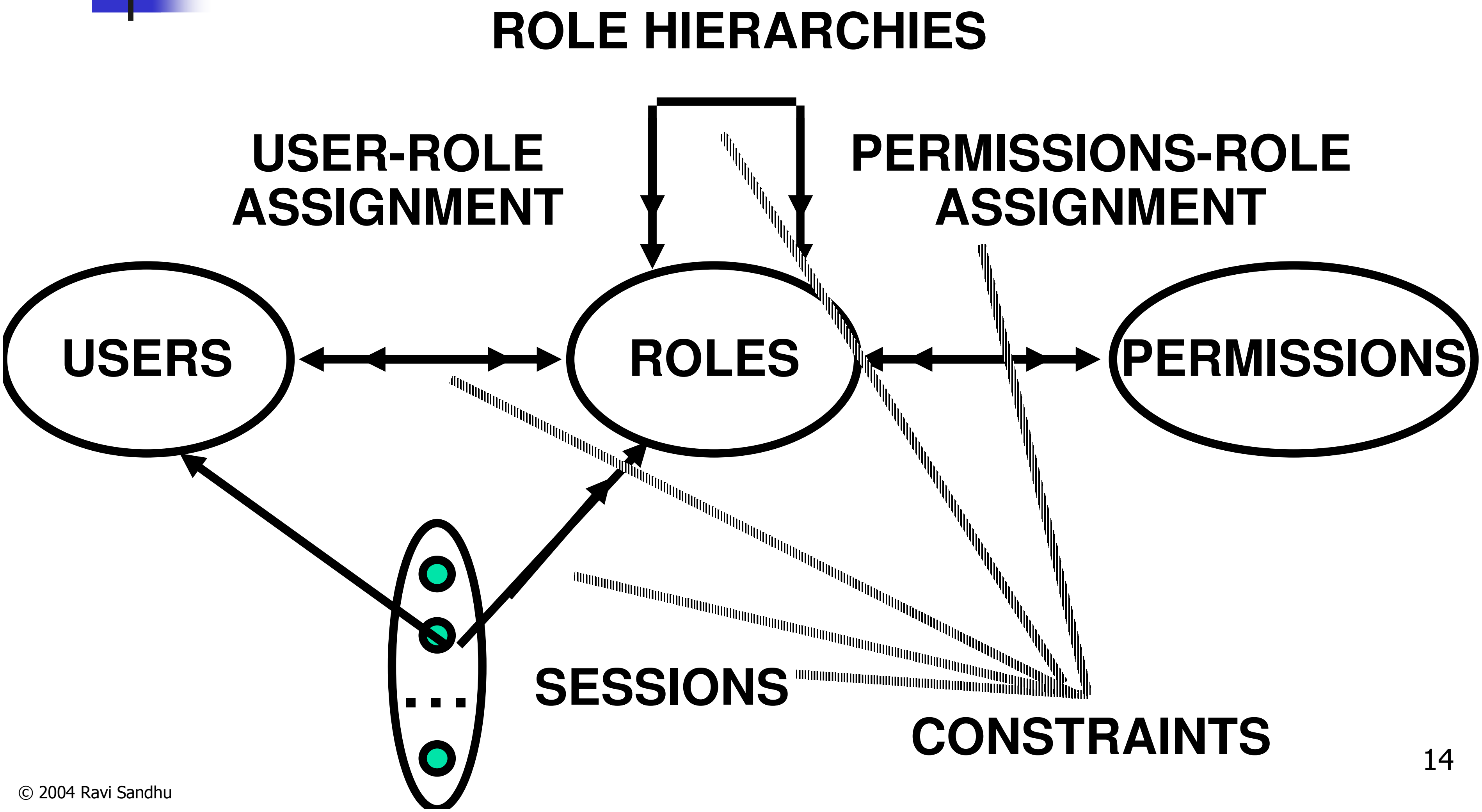
user-pull, server-pull, etc.

certificates, tickets, PACs, etc.

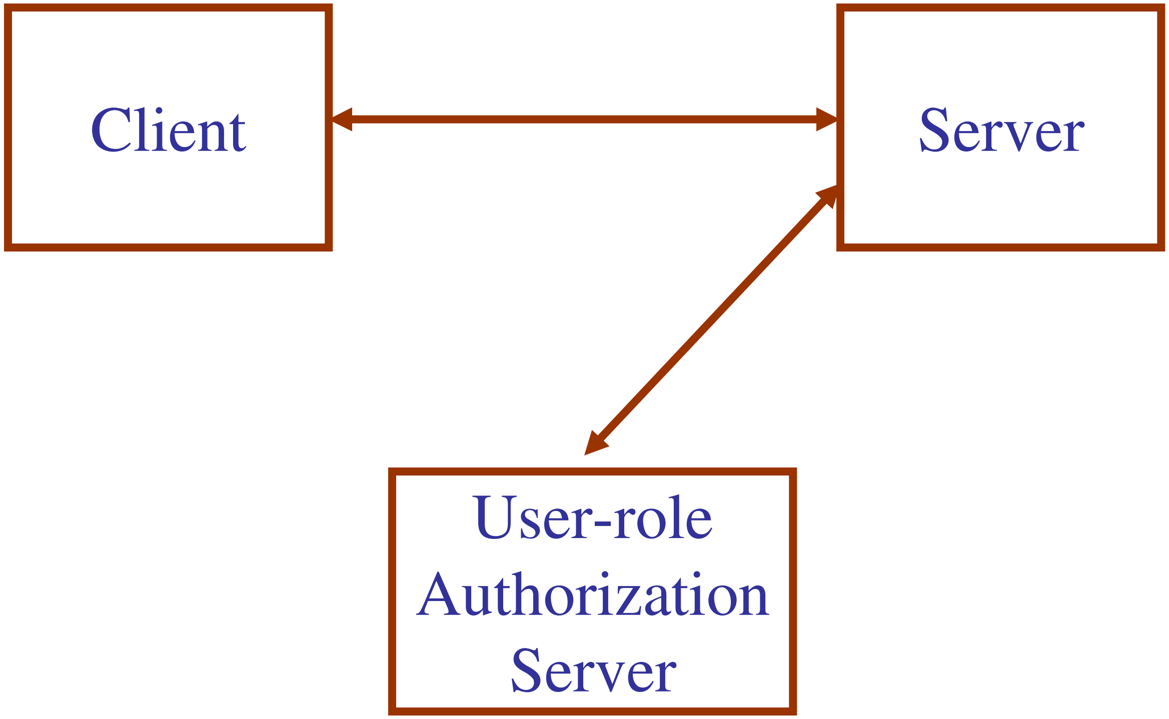
How?

Assurance

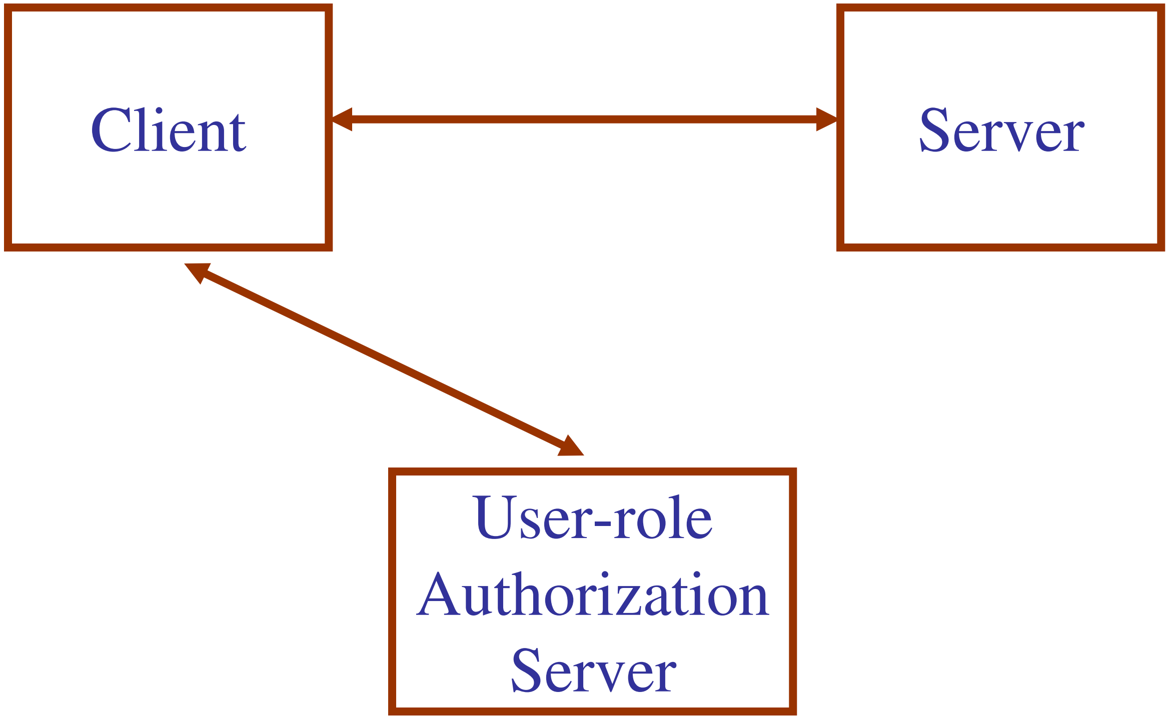
RBAC96 Model



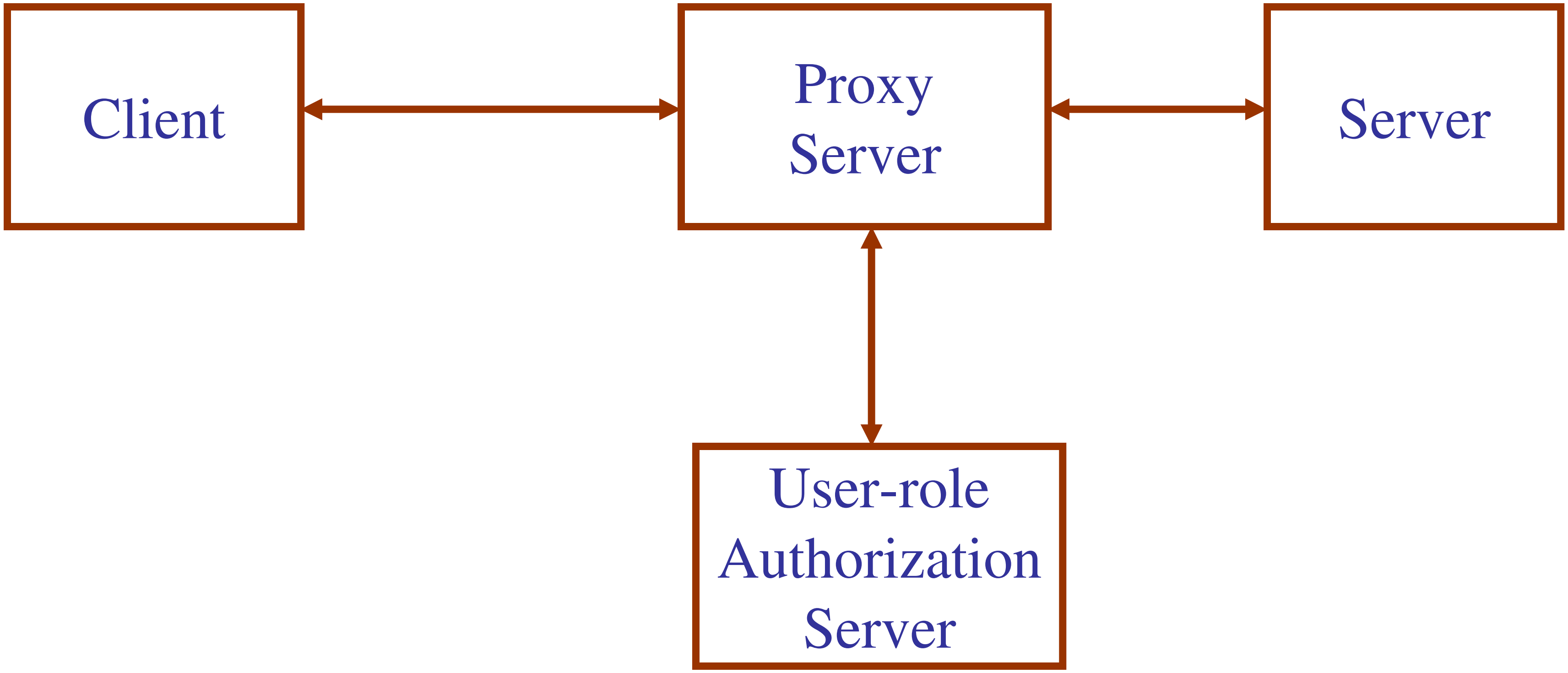
Server-Pull Architecture



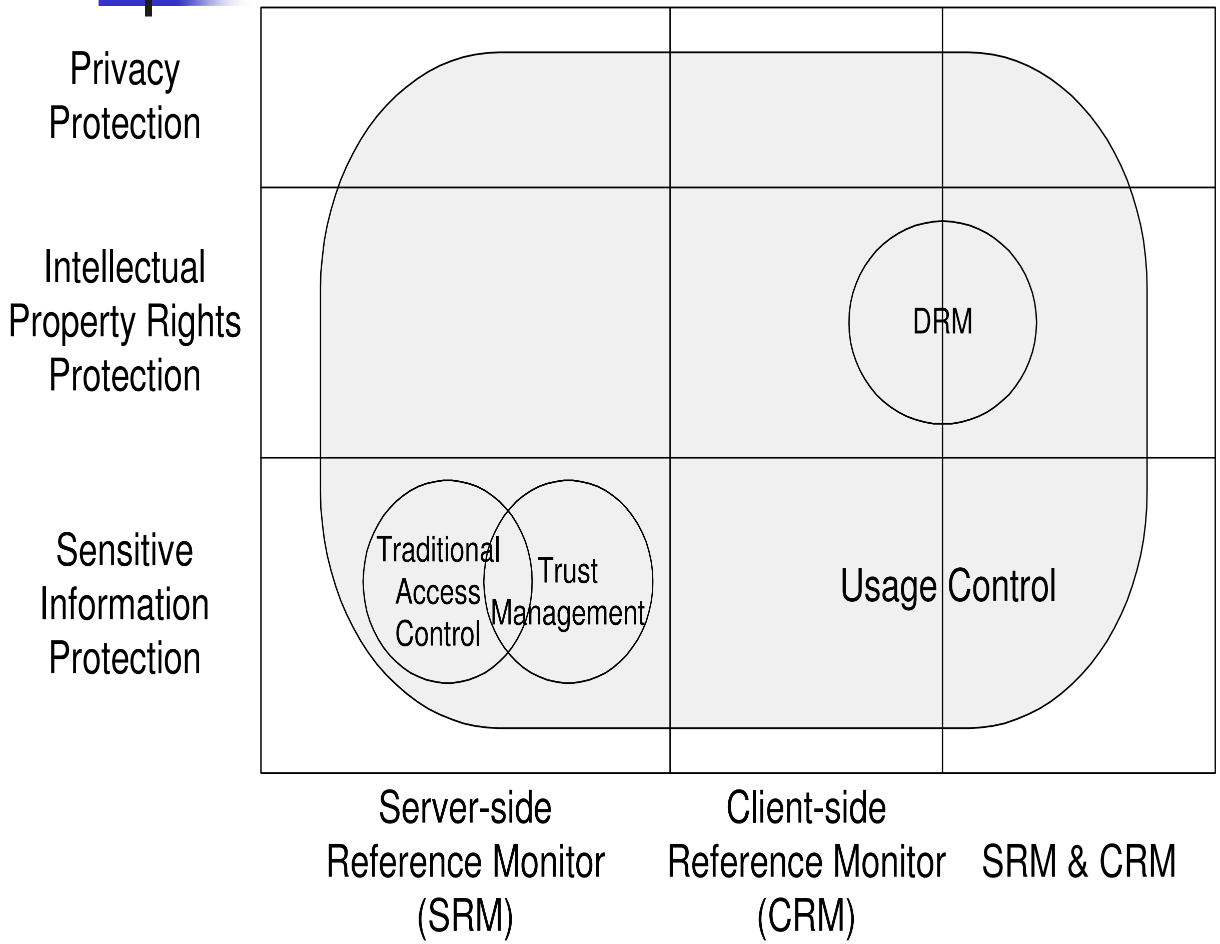
User-Pull Architecture



Proxy-Based Architecture

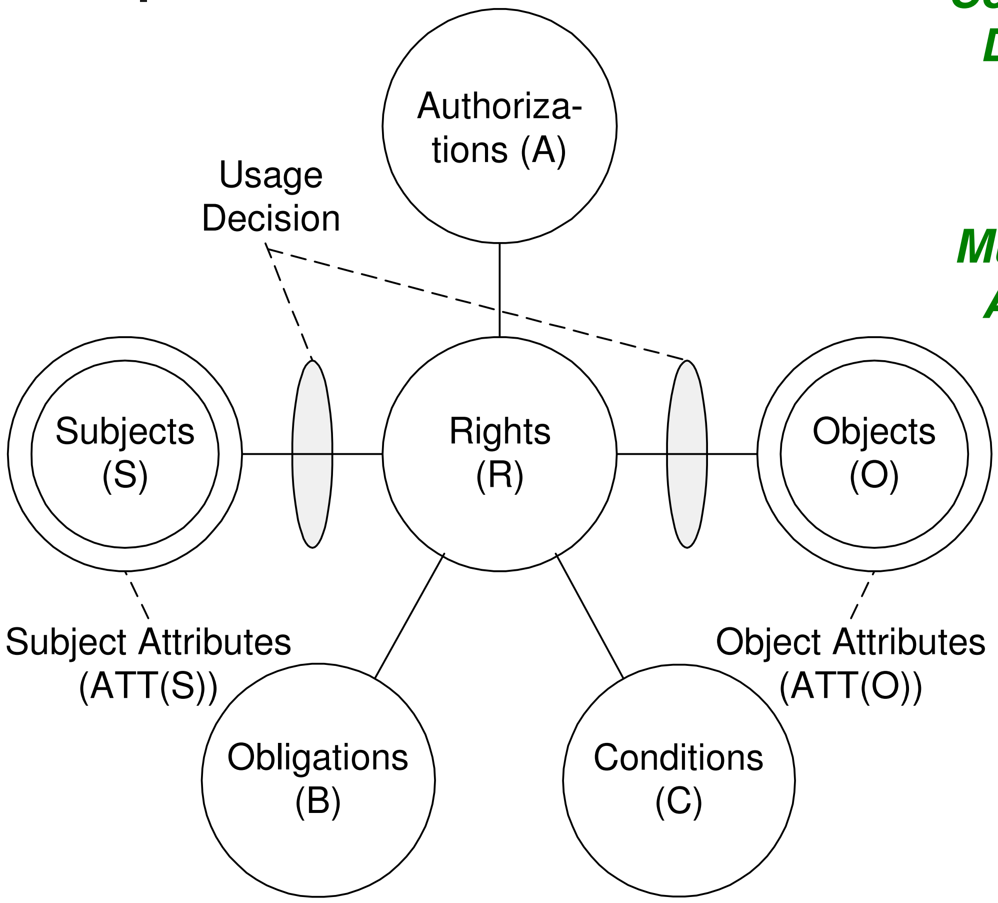


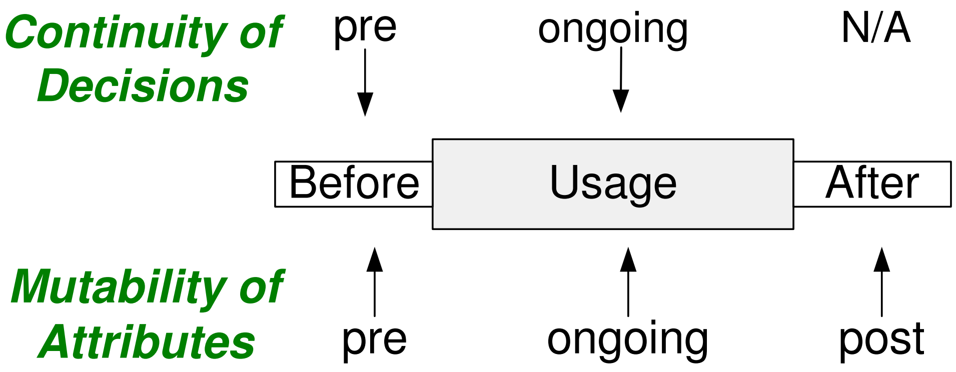
Usage Control (UCON) Coverage


Privacy Protection
Intellectual Property Rights Protection
Sensitive Information Protection
DRM
Traditional Access Control
Trust Management
Usage Control
Server-side Reference Monitor (SRM)
Client-side Reference Monitor (CRM)
SRM & CRM

- Protection Objectives
  - Sensitive information protection
  - IPR protection
  - Privacy protection
- Protection Architectures
  - Server-side reference monitor
  - Client-side reference monitor
  - SRM & CRM

Core UCON (Usage Control) Models





- Continuity
  - Decision can be made during usage for continuous enforcement
- Mutability
  - Attributes can be updated as side-effects of subjects’ actions

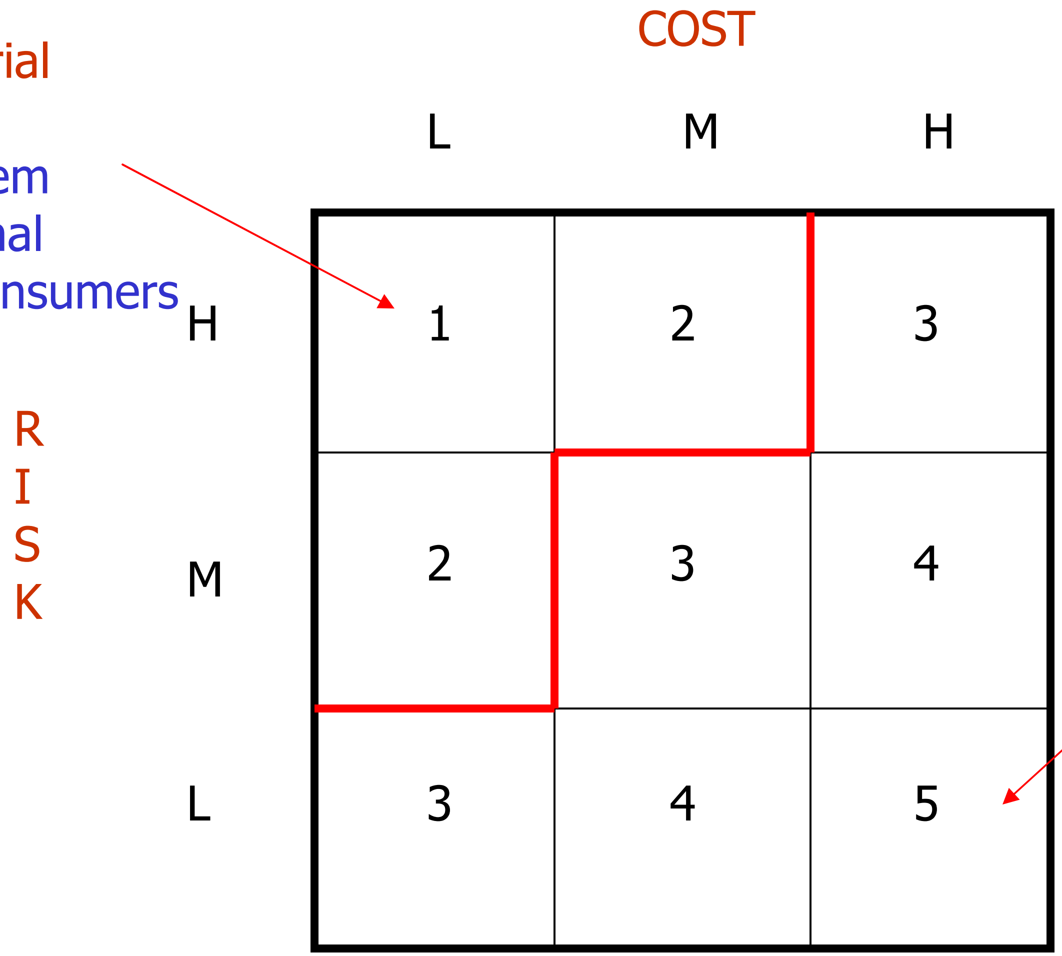
Examples

- Long-distance phone (pre-authorization with post-update)
- Pre-paid phone card (ongoing-authorization with ongoing-update)
- Pay-per-view (pre-authorization with pre-updates)
- Click Ad within every 30 minutes (ongoing-obligation with ongoing-updates)
- Business Hour (pre-/ongoing-condition)

Good enough security

Entrepreneurial Mindset

- 80% problem
- soft, informal
- ordinary consumers



COST

RISK	L	M	H
H	1	2	3
M	2	3	4
L	3	4	5

Academic Mindset

- 120% problem
- hard, informal
- techno-geeks