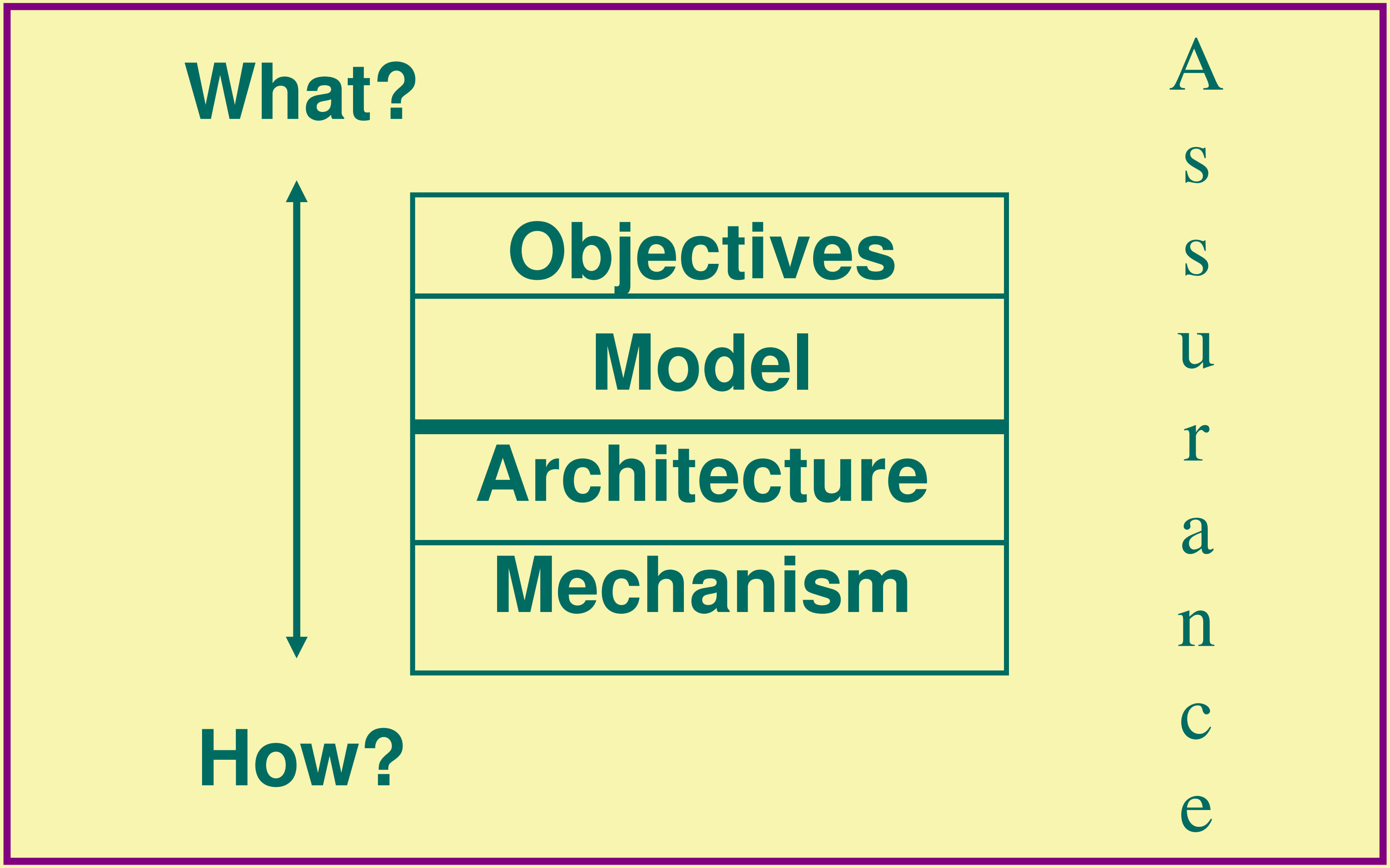
OM-AM and PEI

Prof. Ravi Sandhu

THE OM-AM WAY



What?

Objectives

Model

Architecture

Mechanism

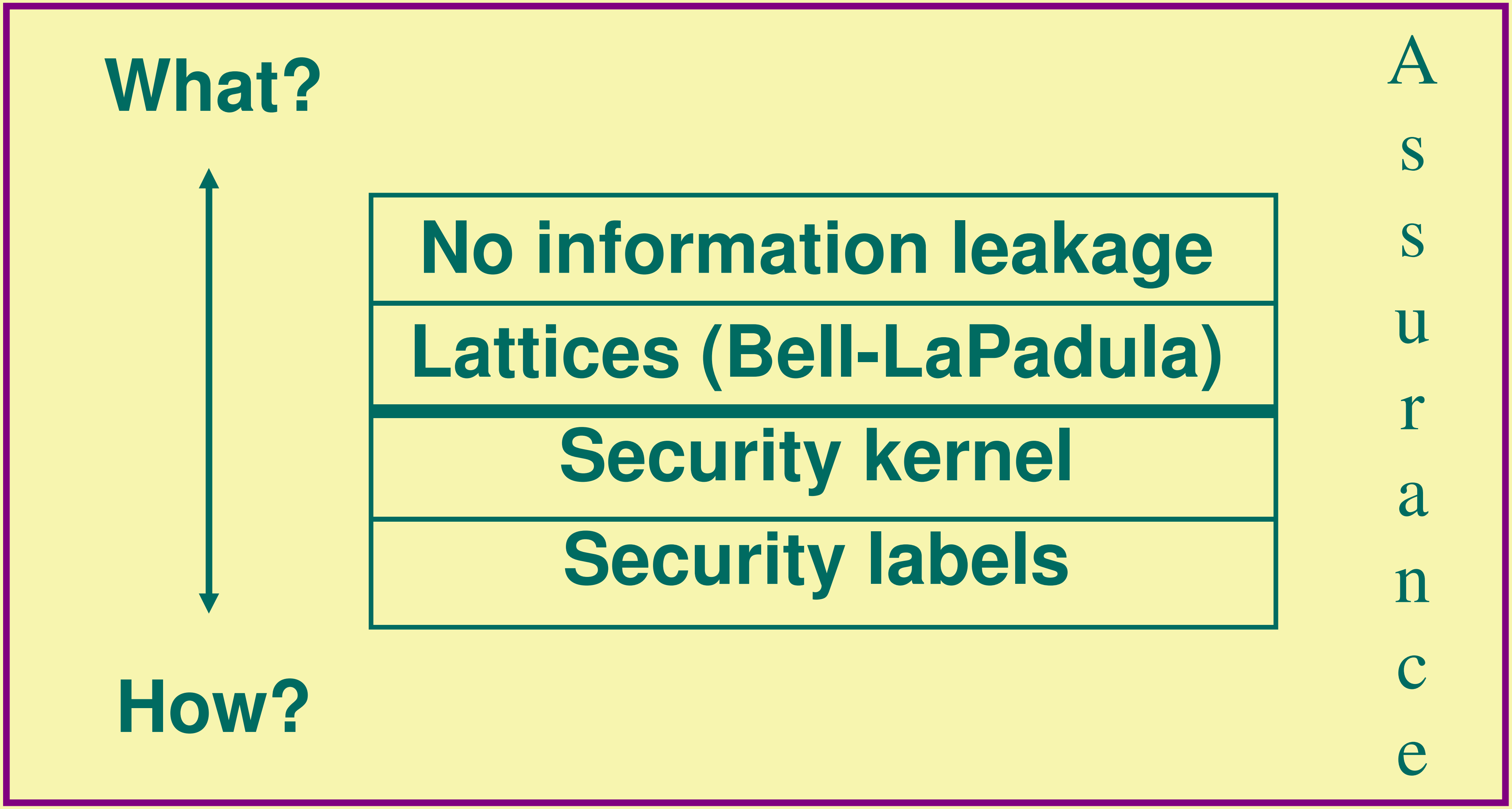
How?

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)

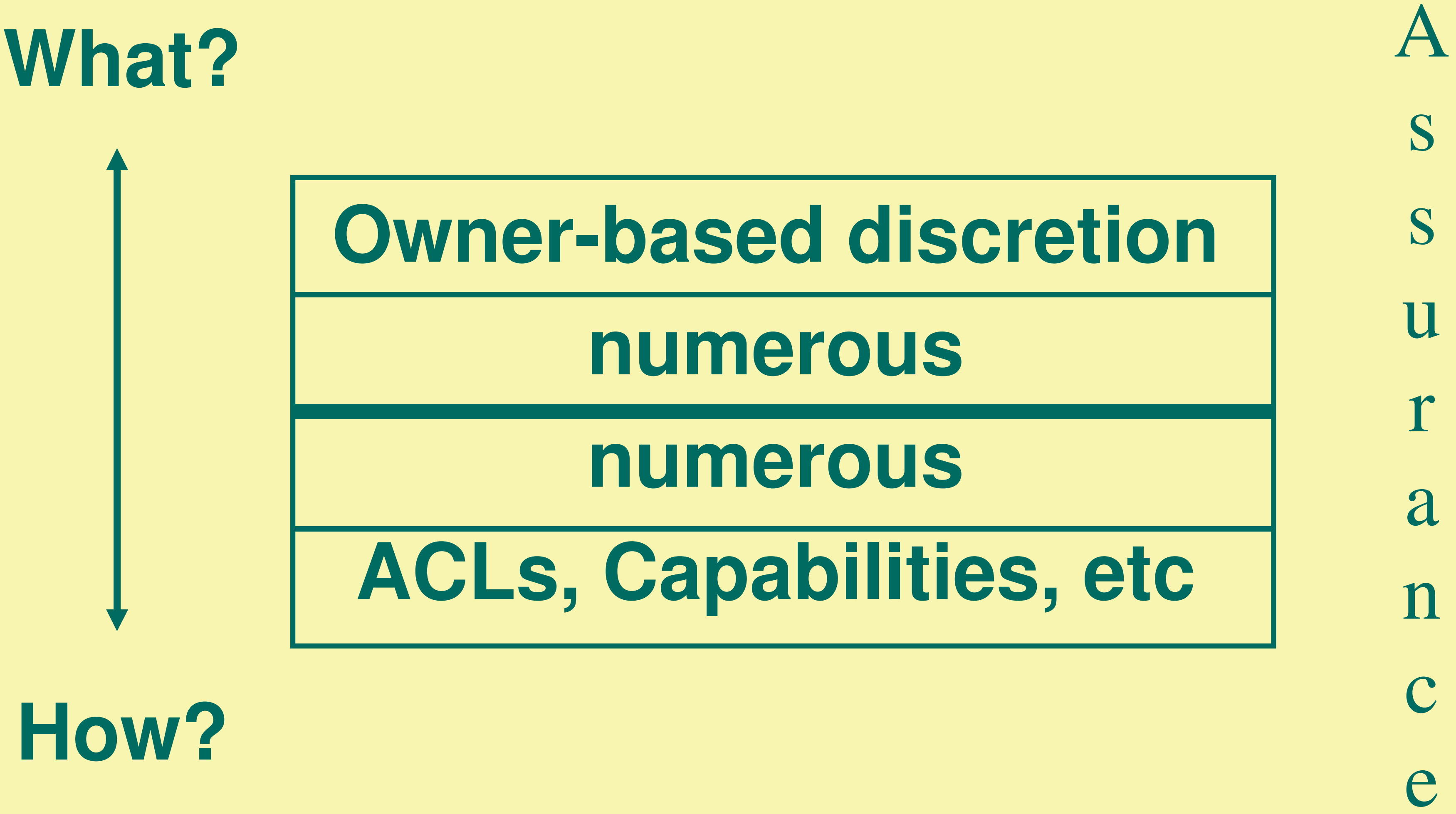
Security kernel

Security labels

How?

Assurance

OM-AM AND DISCRETIONARY ACCESS CONTROL (DAC)



What?

Owner-based discretion

numerous

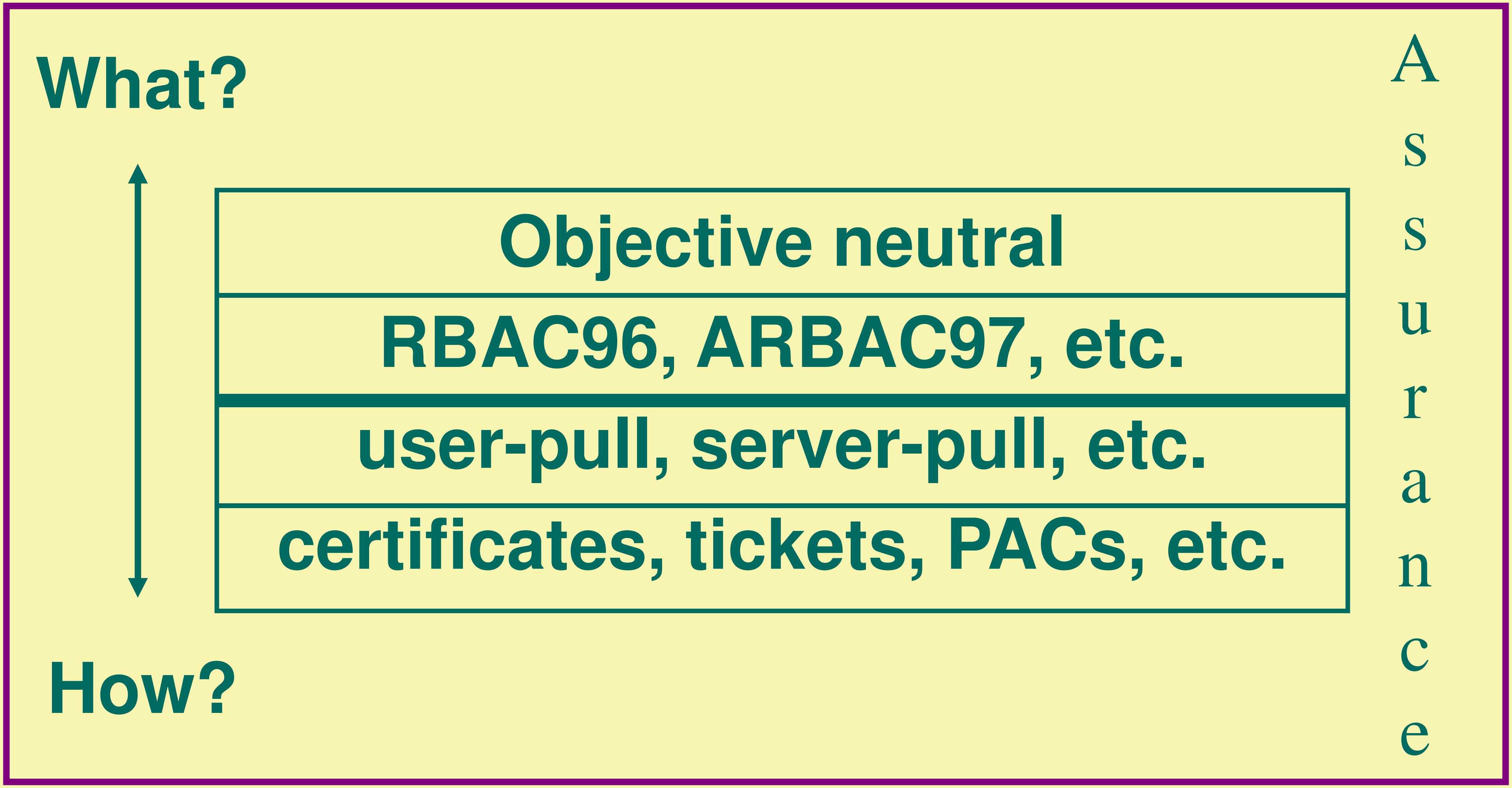
numerous

ACLs, Capabilities, etc

How?

Assurance

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



What?

Objective neutral

RBAC96, ARBAC97, etc.

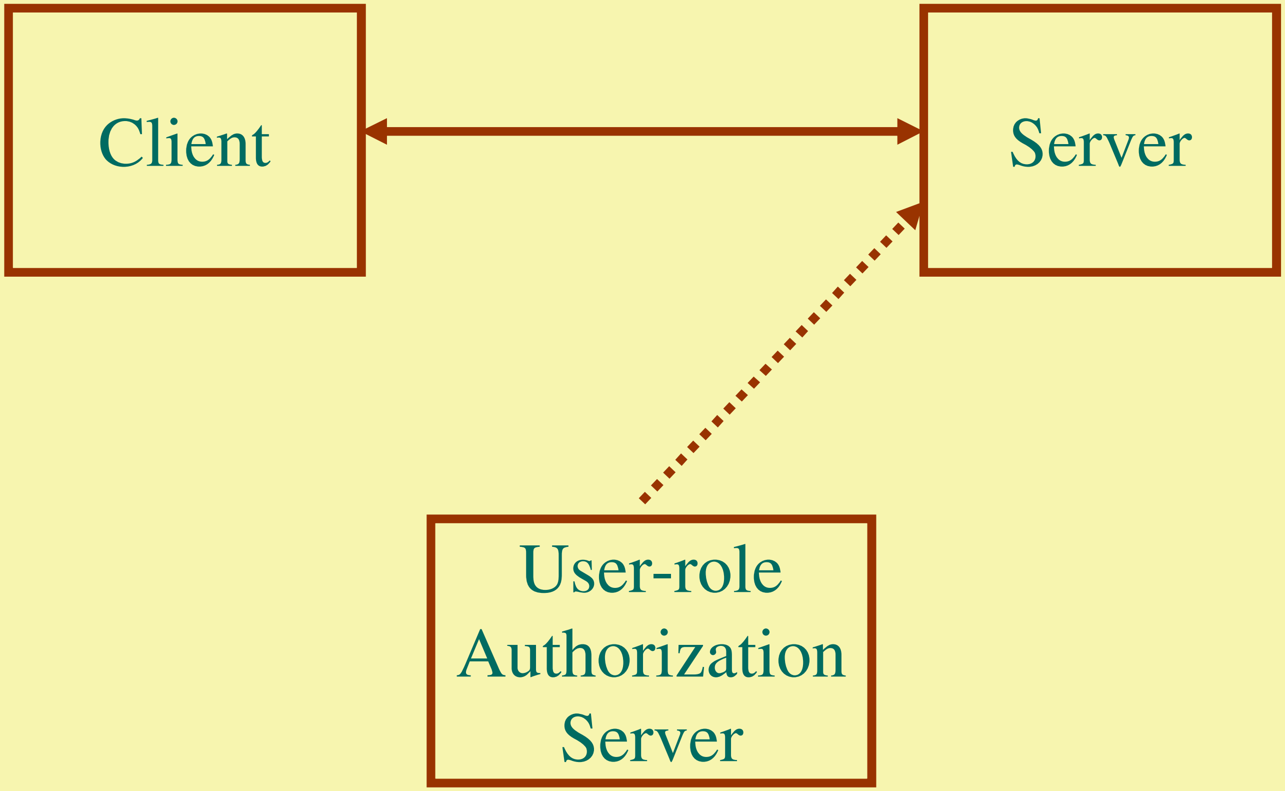
user-pull, server-pull, etc.

certificates, tickets, PACs, etc.

How?

Assurance

SERVER MIRROR

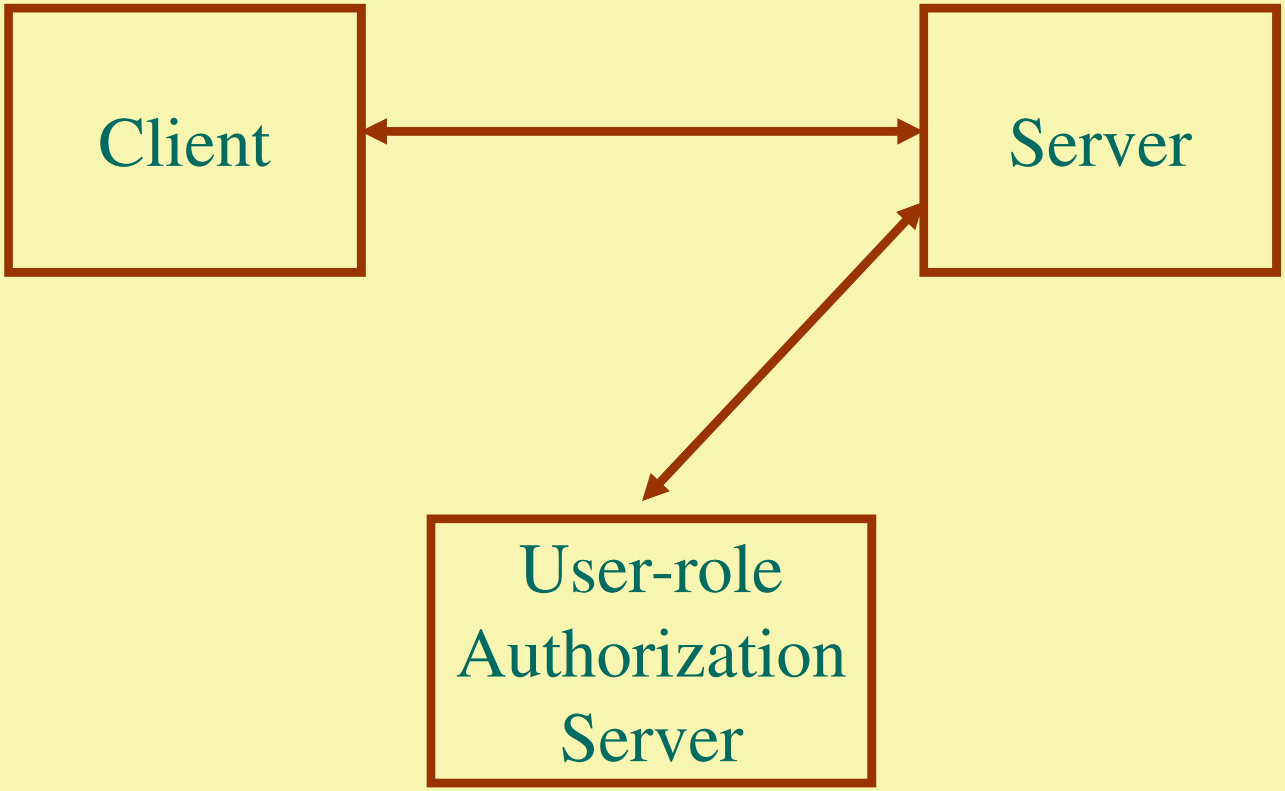


Client

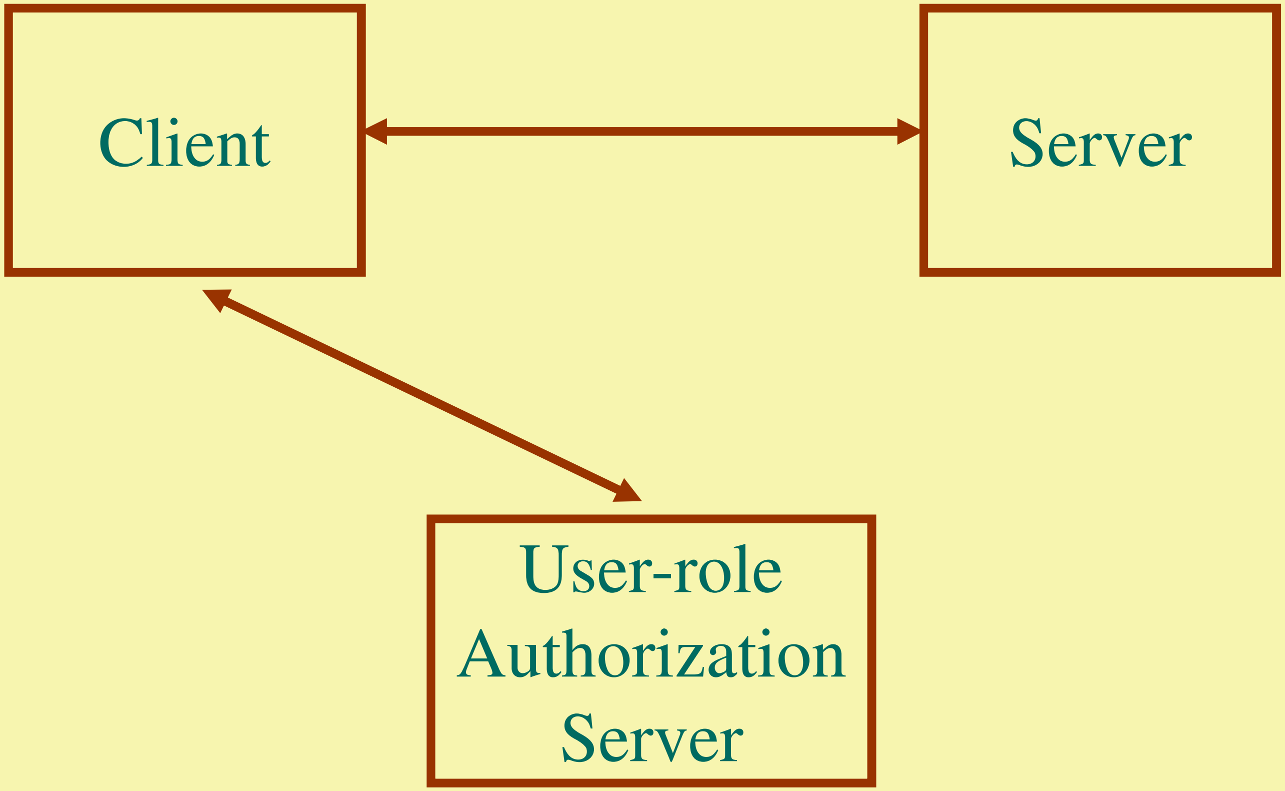
Server

User-role Authorization Server

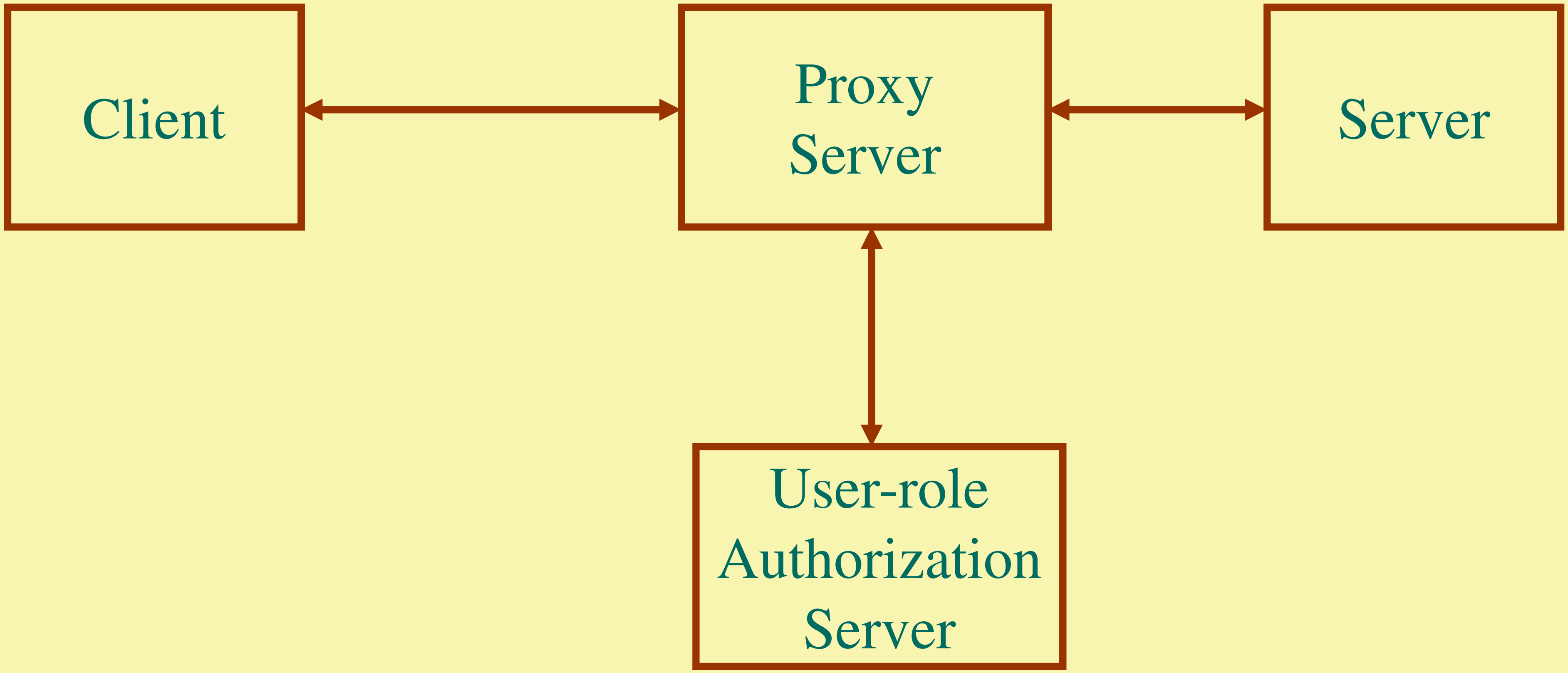
SERVER-PULL



USER-PULL

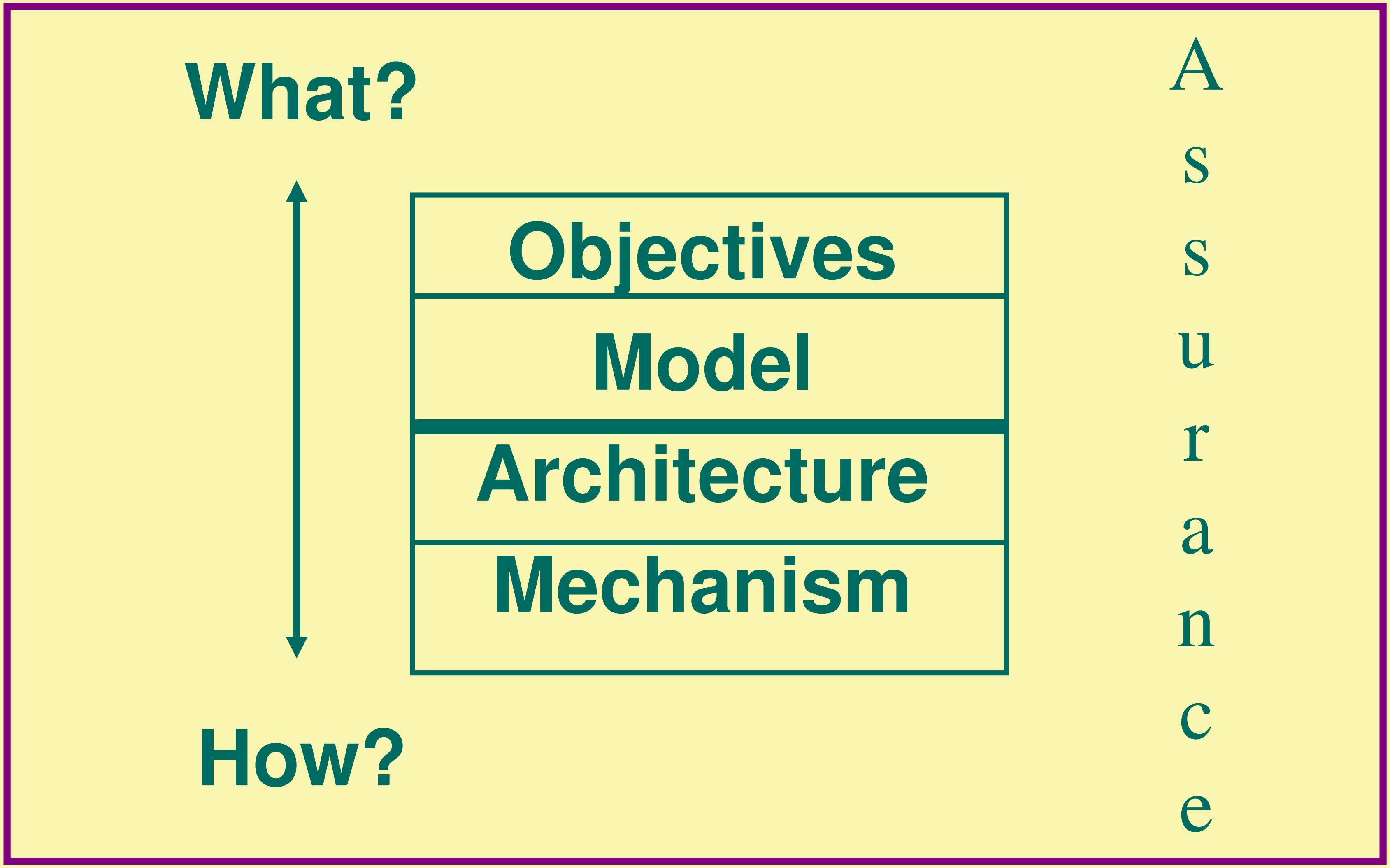


PROXY-BASED



© Ravi Sandhu

THE OM-AM WAY



What?

Objectives

Model

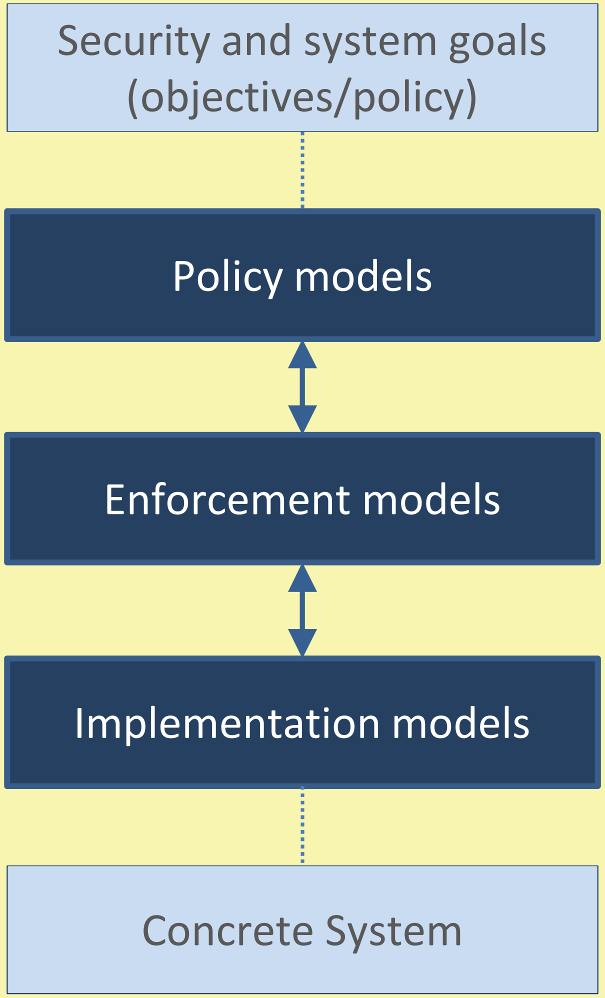
Architecture

Mechanism

How?

Assurance

PEI



- Necessarily informal

- Specified using users, subjects, objects, admins, labels, roles, groups, etc. in an ideal setting.
- Security analysis (objectives, properties, etc.).

- Approximated policy realized using system architecture with trusted servers, protocols, etc.
- Enforcement level security analysis (e.g. stale information due to network latency, protocol proofs, etc.).
- Technologies such as Cloud Computing, Trusted Computing, etc.
- Implementation level security analysis (e.g. vulnerability analysis, penetration testing, etc.)

- Software and Hardware