DAC and MAC

Prof. Ravi Sandhu
Executive Director and Endowed Chair

January 22, 2016

ravi.sandhu@utsa.edu
www.profsandhu.com

© Ravi Sandhu

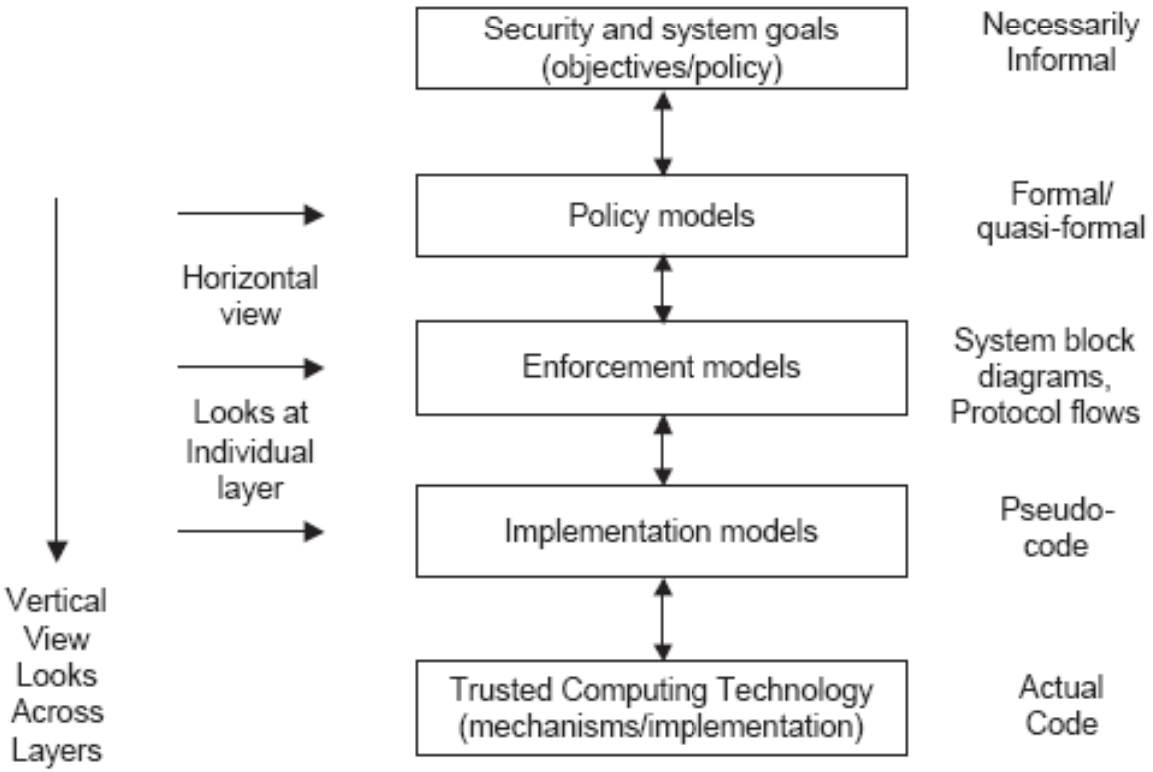
Access Control Models

- Discretionary Access Control (DAC)
  - Owner controls access but only to the original, not to copies
- Mandatory Access Control (MAC)
  Same as Lattice-Based Access Control (LBAC)
  - Access based on security labels
  - Labels propagate to copies
- Role-Based Access Control (RBAC)
  - Access based on roles
  - Can be configured to do DAC or MAC

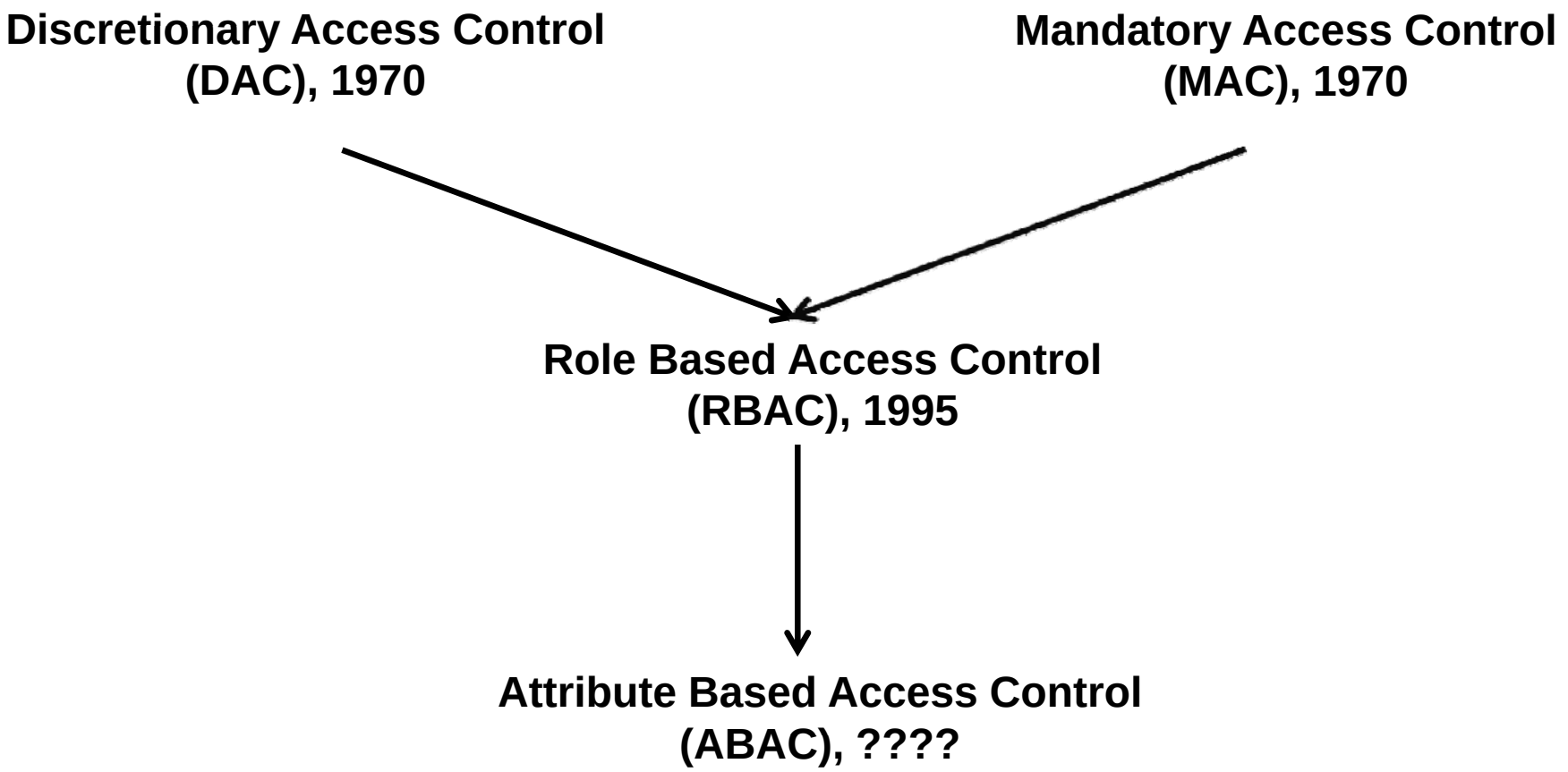
Numerous other models but only 3 successes

- What's next?
  - Attribute-Based Access Control (ABAC)
  - Relationship-Based Access Control (ReBAC)
  - Usage Control (UCON)

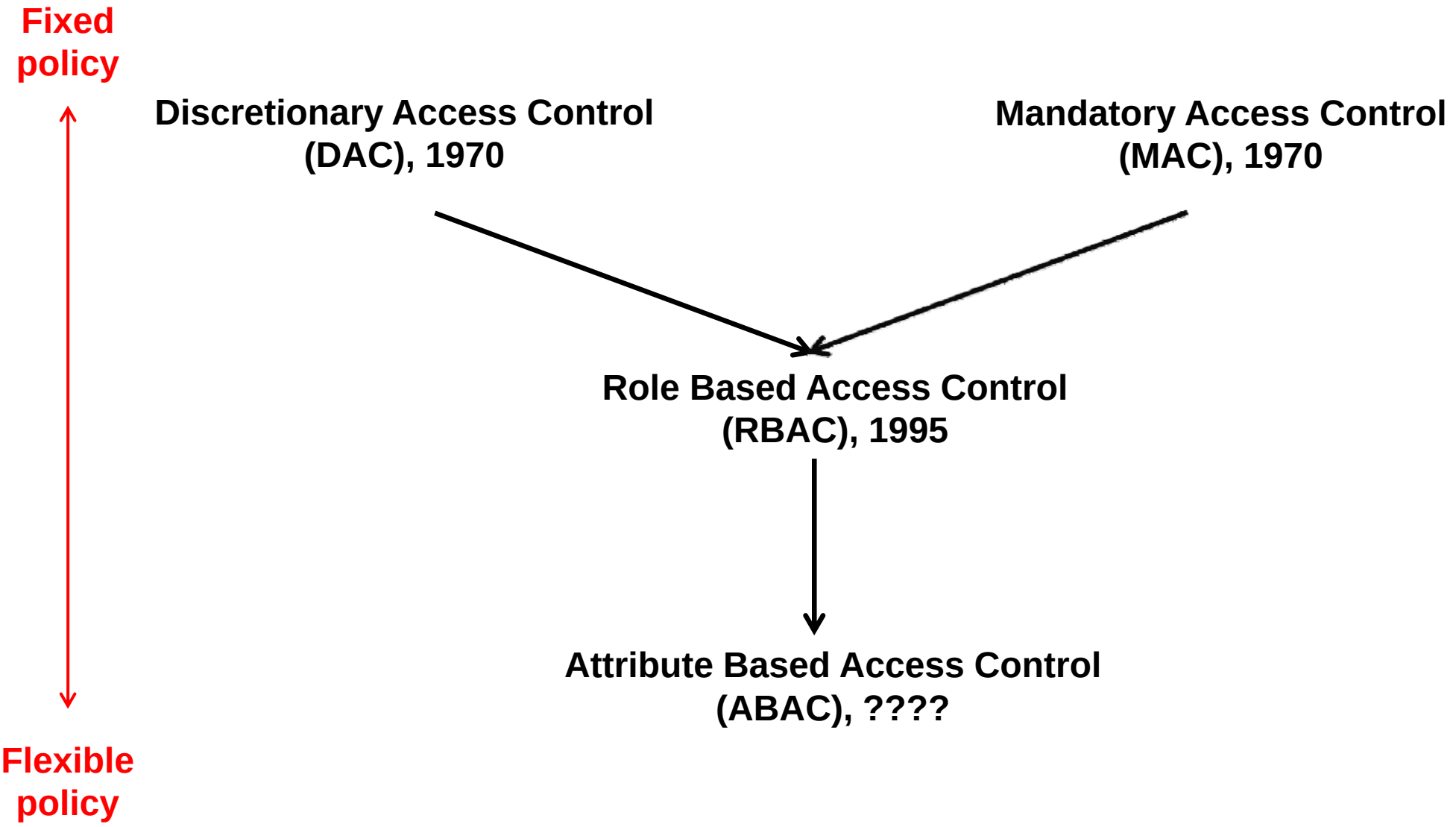
PEI Models


Security and system goals (objectives/policy)
Necessarily Informal
Policy models
Formal/ quasi-formal
Enforcement models
System block diagrams, Protocol flows
Implementation models
Pseudo-code
Trusted Computing Technology (mechanisms/implementation)
Actual Code
Horizontal view
Looks at Individual layer
Vertical View Looks Across Layers
Idealized
Enforceable (Approximate)
Codeable

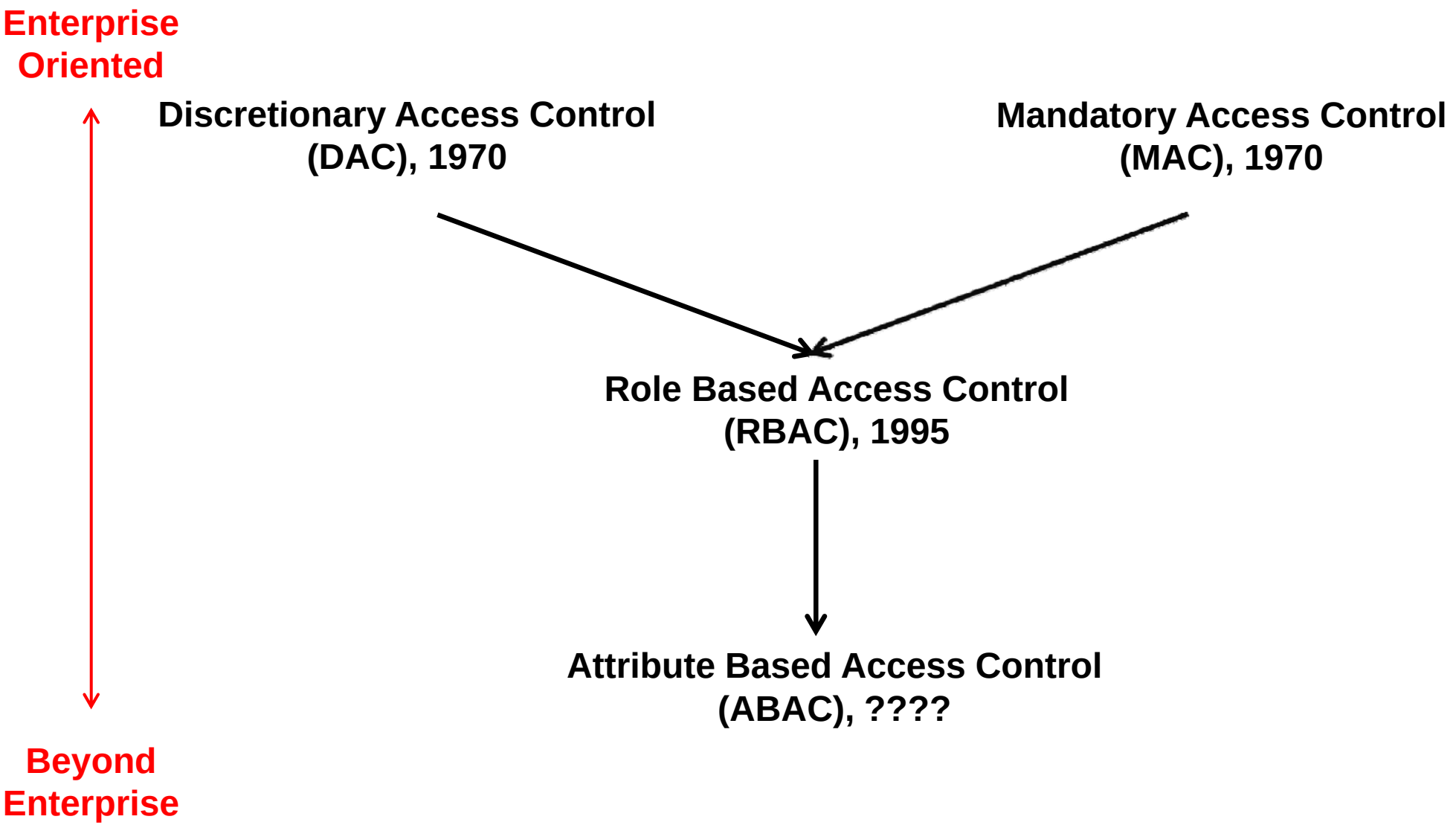
Access Control



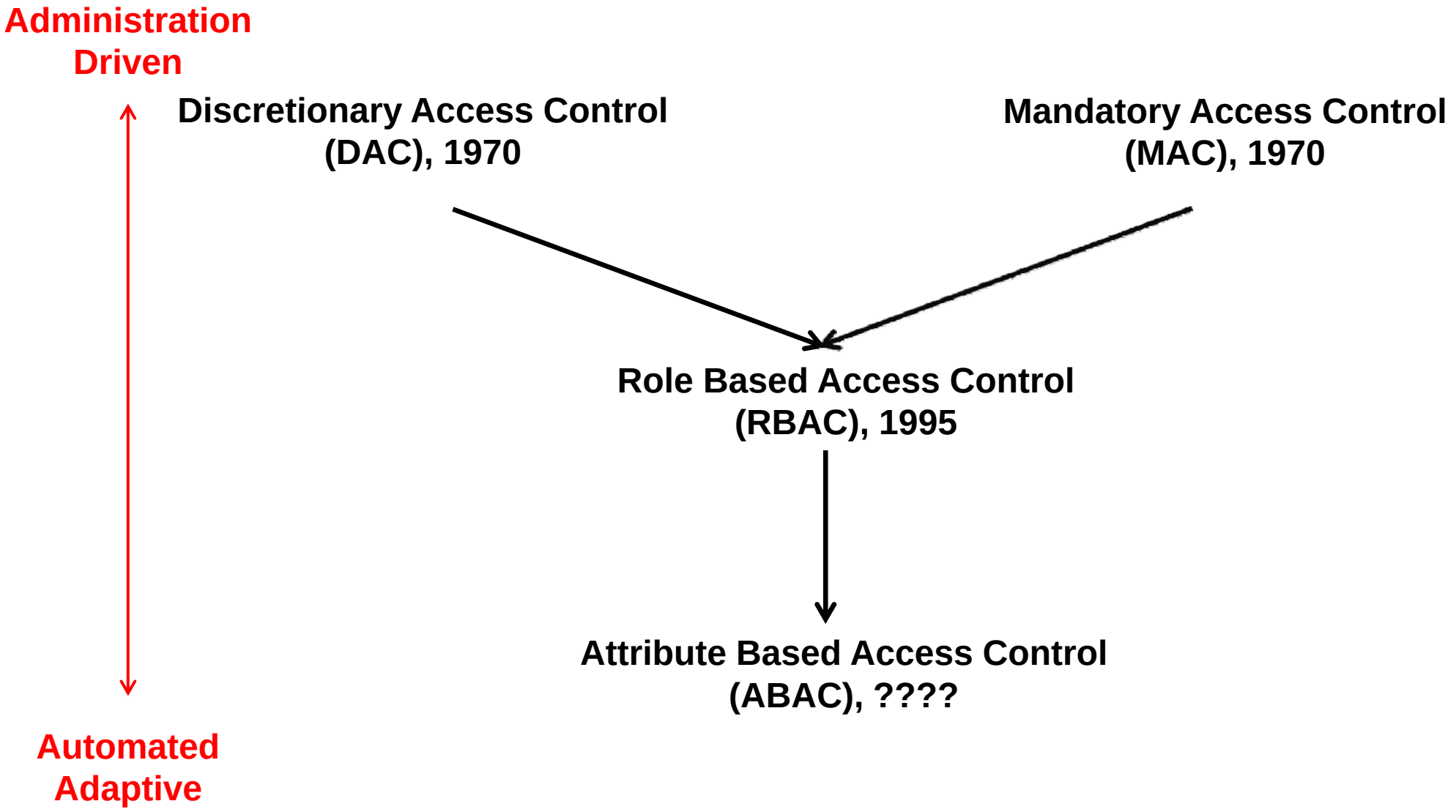
Access Control



Access Control

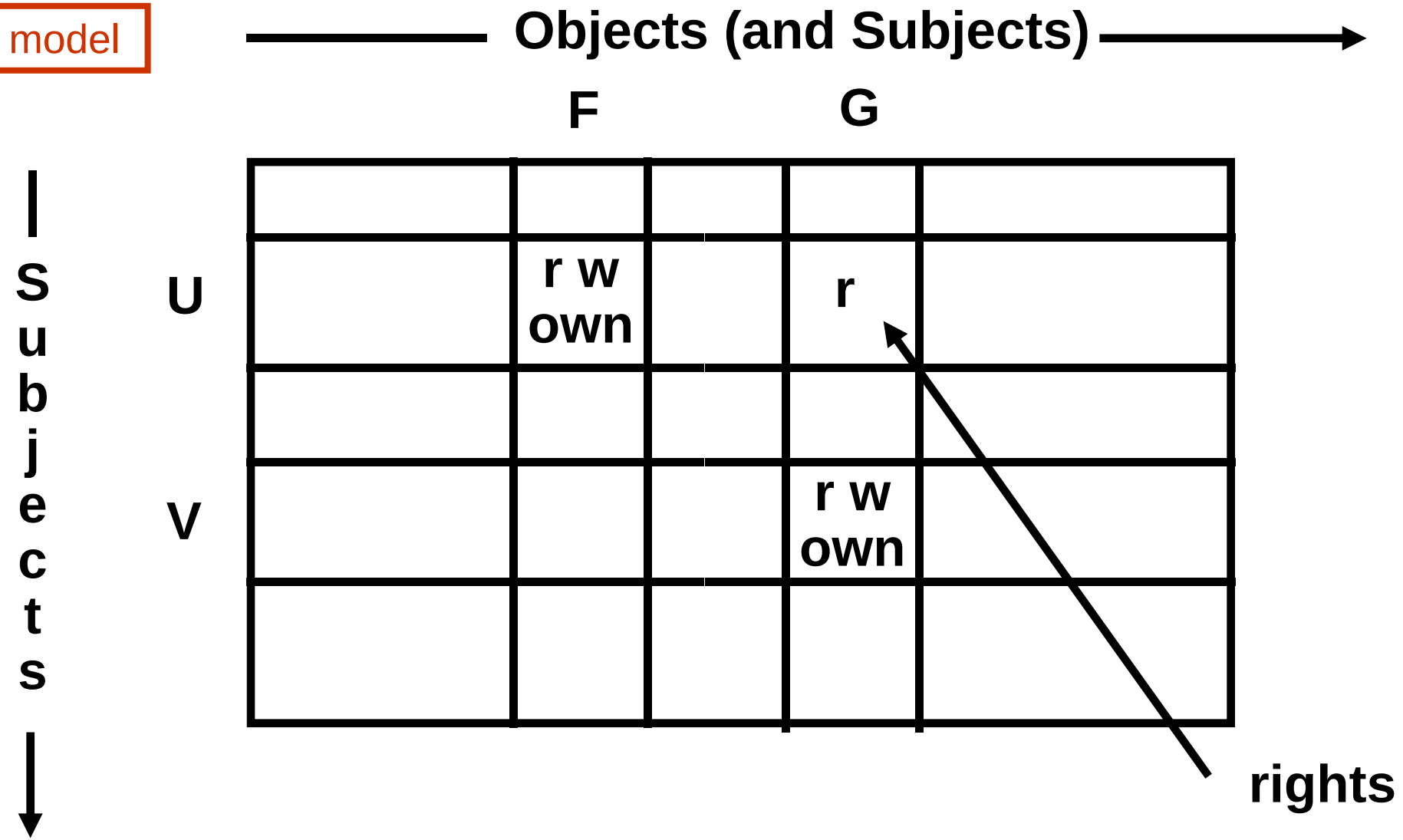


Access Control



DAC: ACCESS MATRIX MODEL

P model



ACCESS CONTROL LISTS (ACLs)

E model

F

U:r

U:w

U:own

G

U:r

V:r

V:w

V:own

each column of the access matrix is stored with the object corresponding to that column

CAPABILITY LISTS

E model

U **F/r, F/w, F/own, G/r**

V **G/r, G/w, G/own**

each row of the access matrix is stored with the subject corresponding to that row

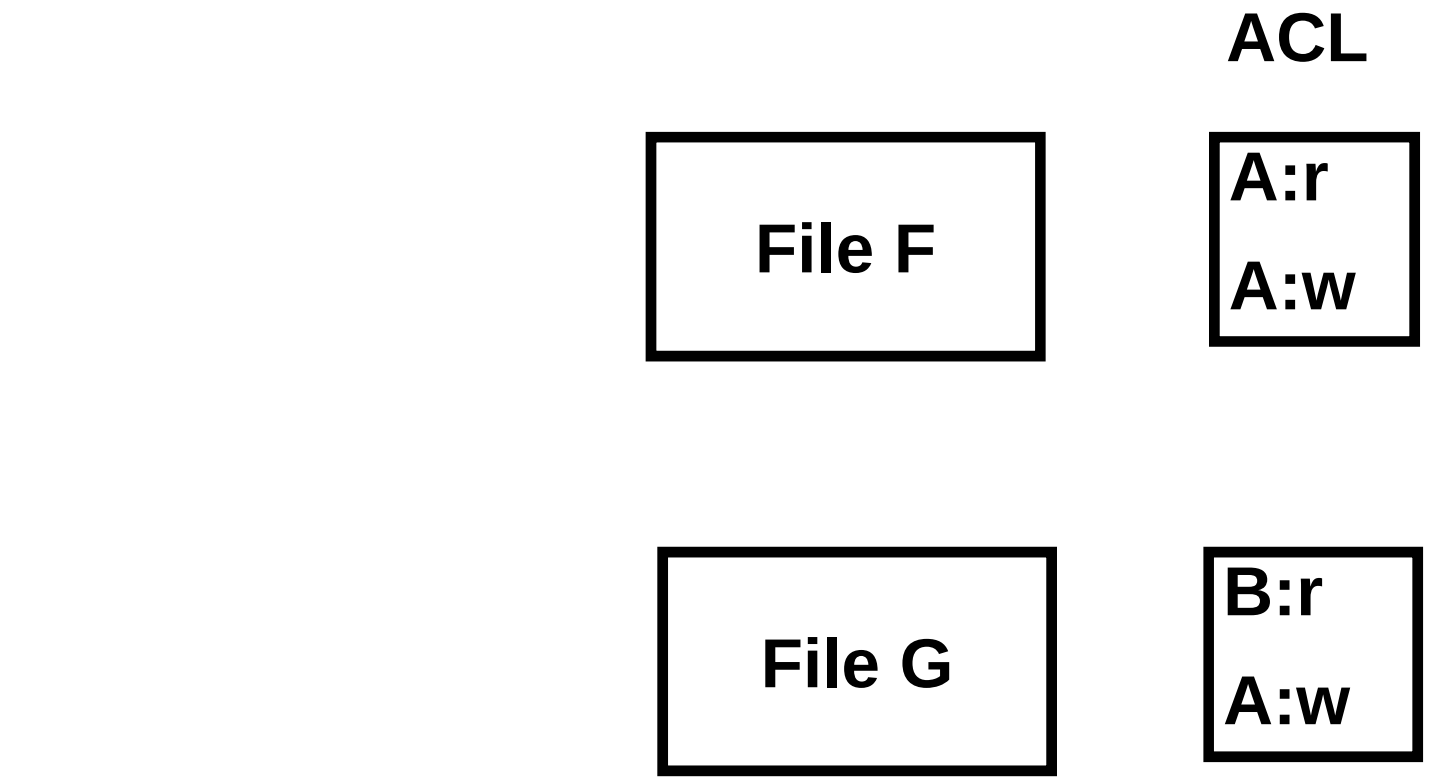
ACCESS CONTROL TRIPLES

E model

Subject	Access	Object
U	r	F
U	w	F
U	own	F
U	r	G
V	r	G
V	w	G
V	own	G

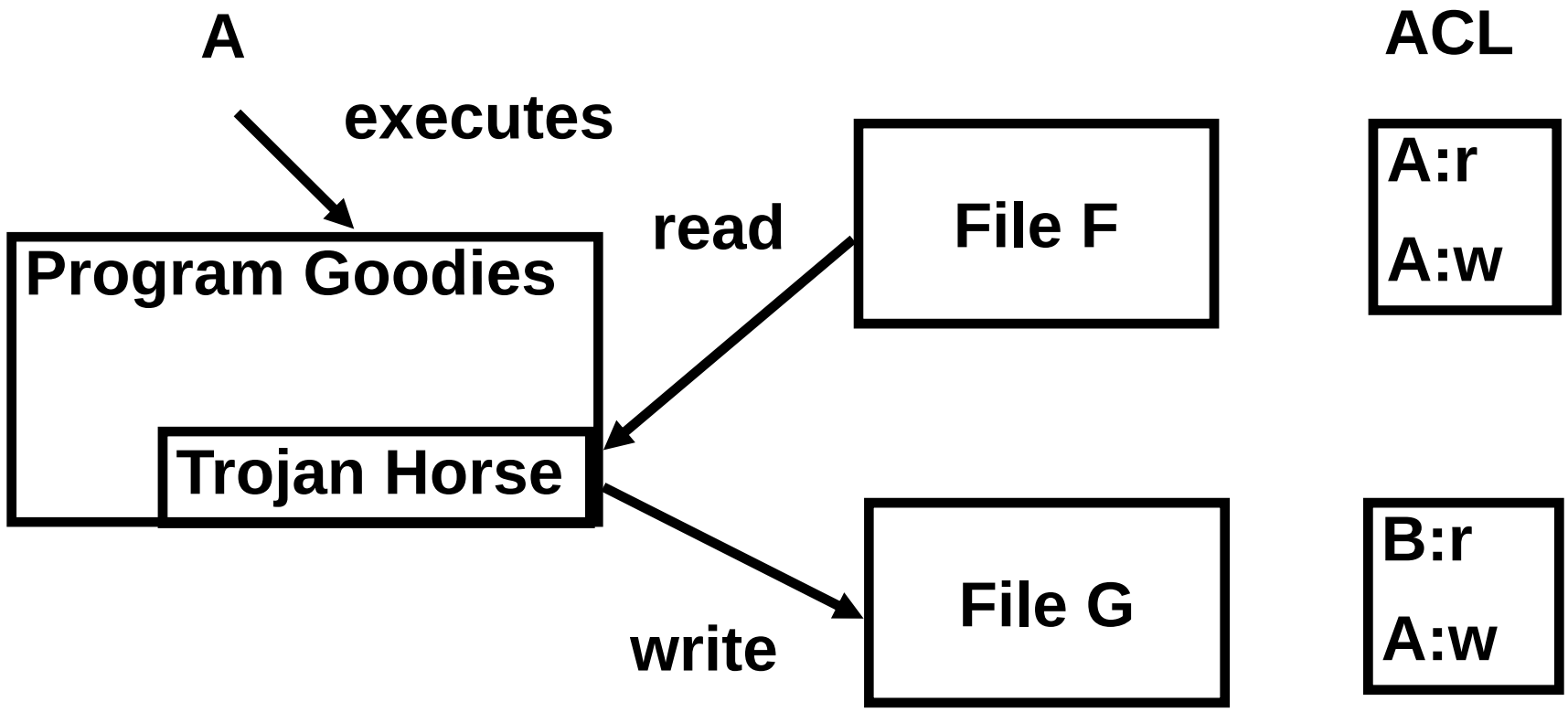
commonly used in relational database management systems

DAC: TROJAN HORSE VULNERABILITY



B cannot read file F

DAC: TROJAN HORSE VULNERABILITY



B can read contents of file F copied to file G

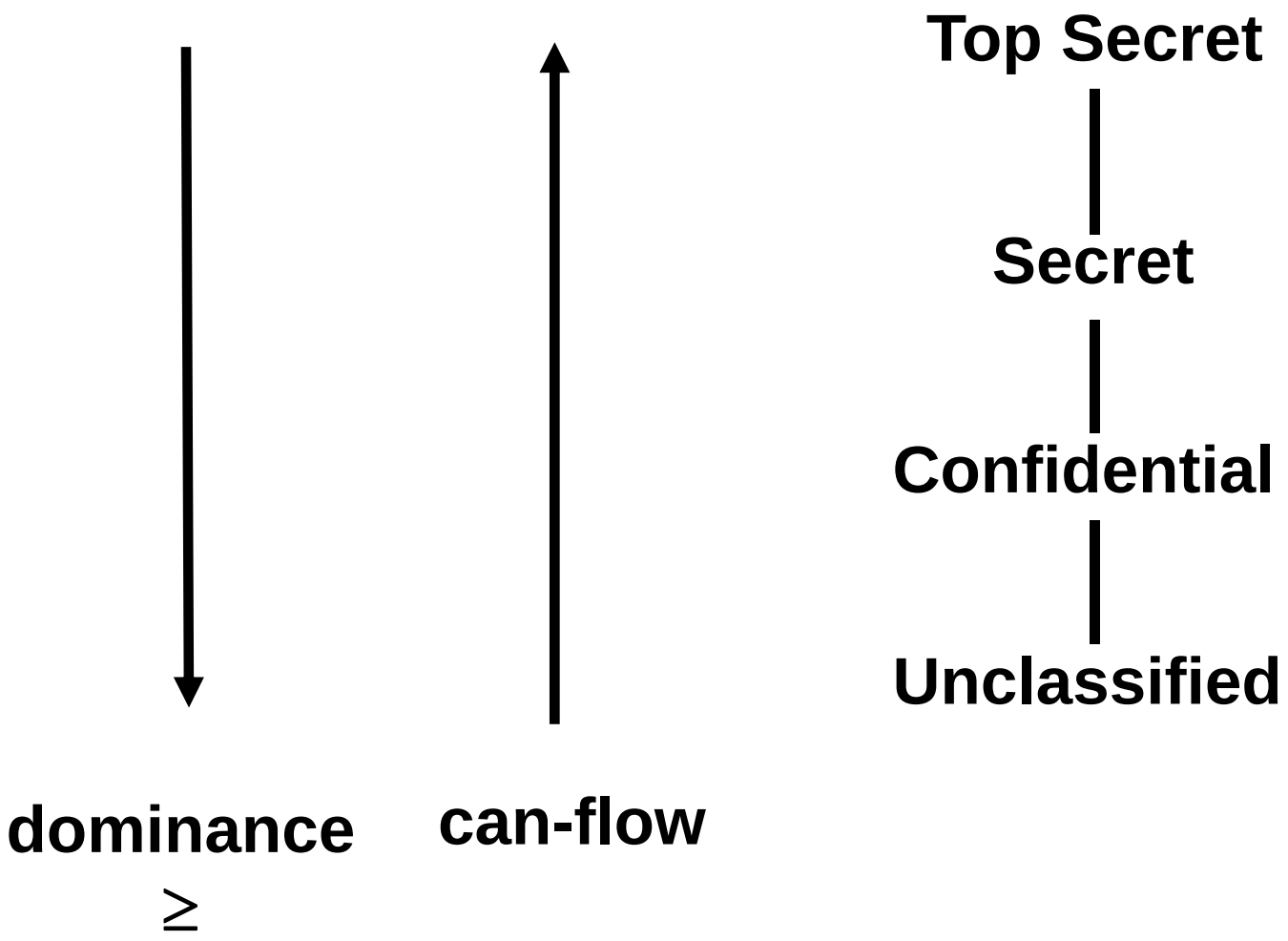
DAC CHALLENGES

- Owner unrestricted DAC versus restricted DAC
- Safety in restricted DAC
  - Undecidable
  - NP-Hard, PSpace-Hard
- Transfer of ownership
- Multiple ownership
- Cascading grants and revokes
- Negative authorizations and conflict resolution
  - Worse with groups and hierarchies
- DAC policy limits
  - You can give only what you have
  - How about user administration?
- Practical DAC deployments
  - Ownership consolidated in a single administrator
  - Can lead to inadvertent cascading revokes

© Ravi Sandhu

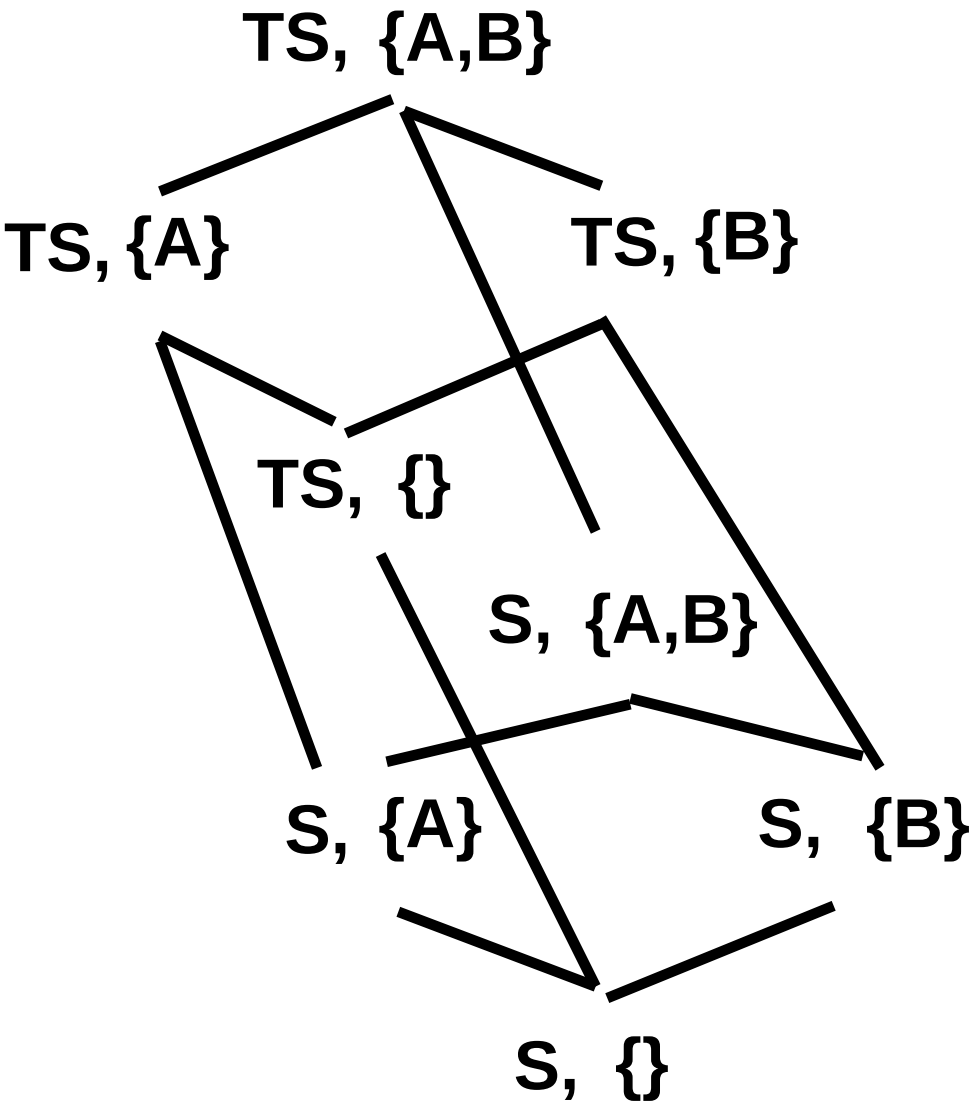
LBAC: LATTICE STRUCTURES

P model



LBAC: LATTICE STRUCTURES

P model



Hierarchical Classes with Compartments

LBAC: LATTICE STRUCTURES

SIMPLE-SECURITY

Subject S can read object O only if

- label(S) dominates label(O)

STAR-PROPERTY (LIBERAL)

Subject S can write object O only if

- label(O) dominates label(S)

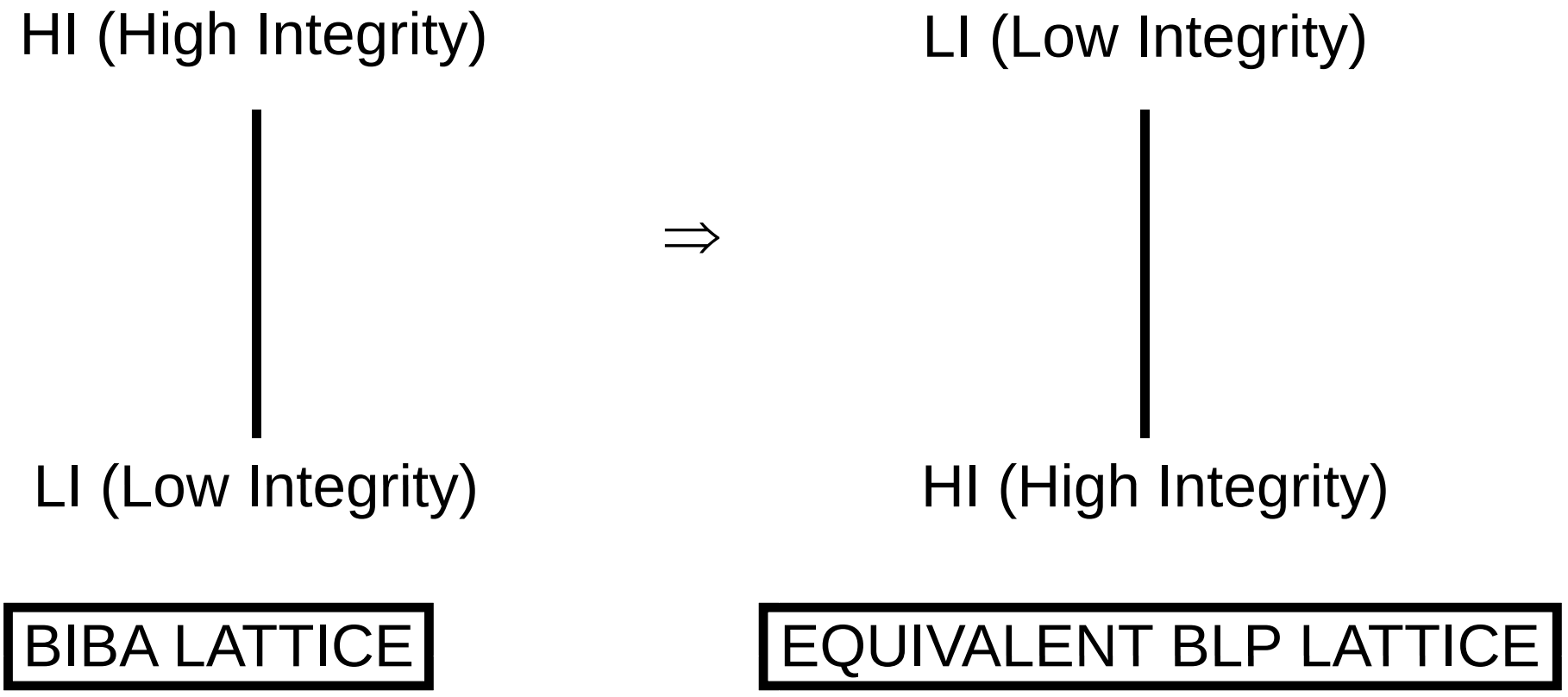
STAR-PROPERTY (STRICT)

Subject S can write object O only if

- label(O) equals label(S)

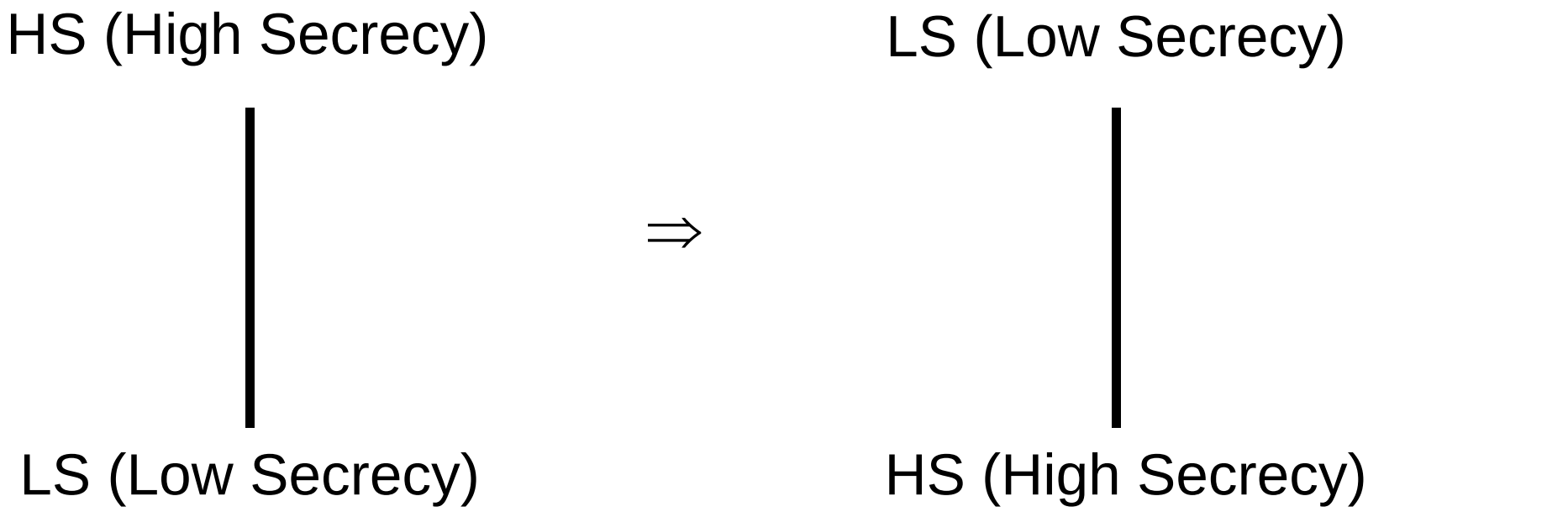
EQUIVALENCE OF BLP AND BIBA

P model



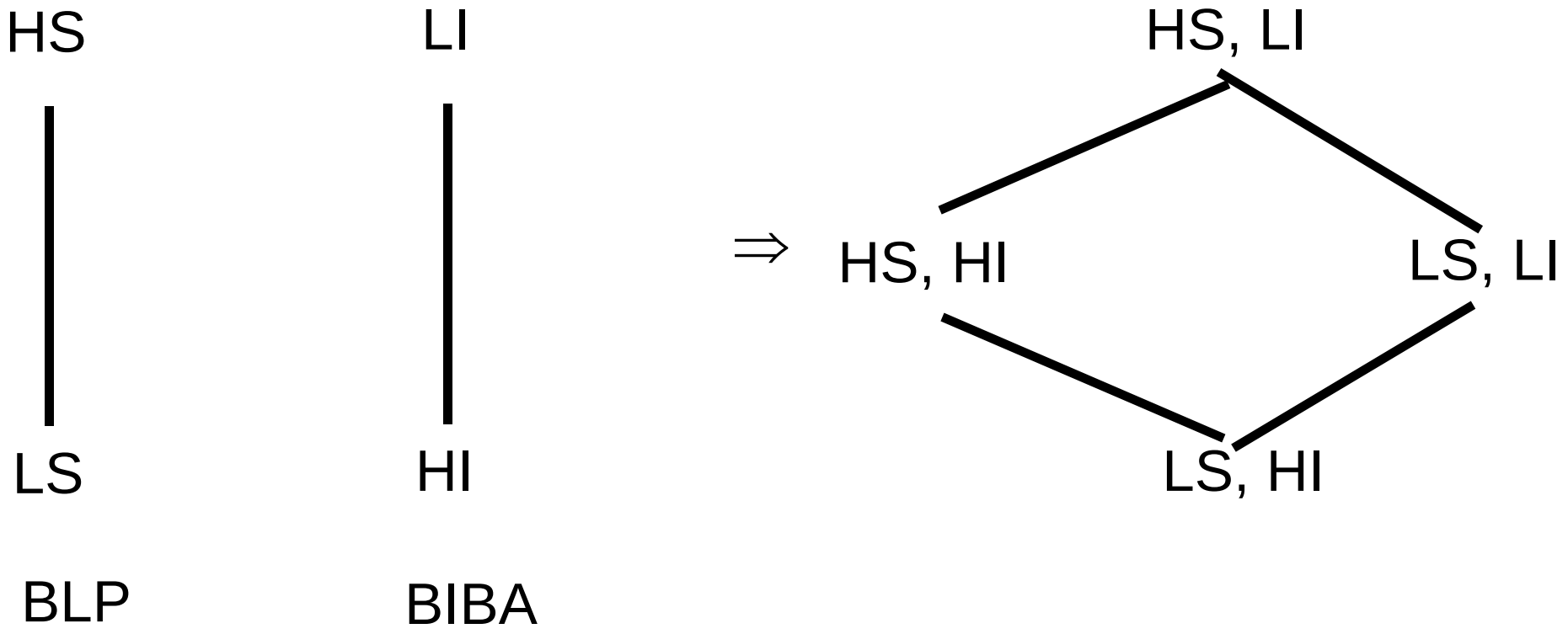
EQUIVALENCE OF BLP AND BIBA

P model



COMBINATION OF DISTINCT LATTICES

P model



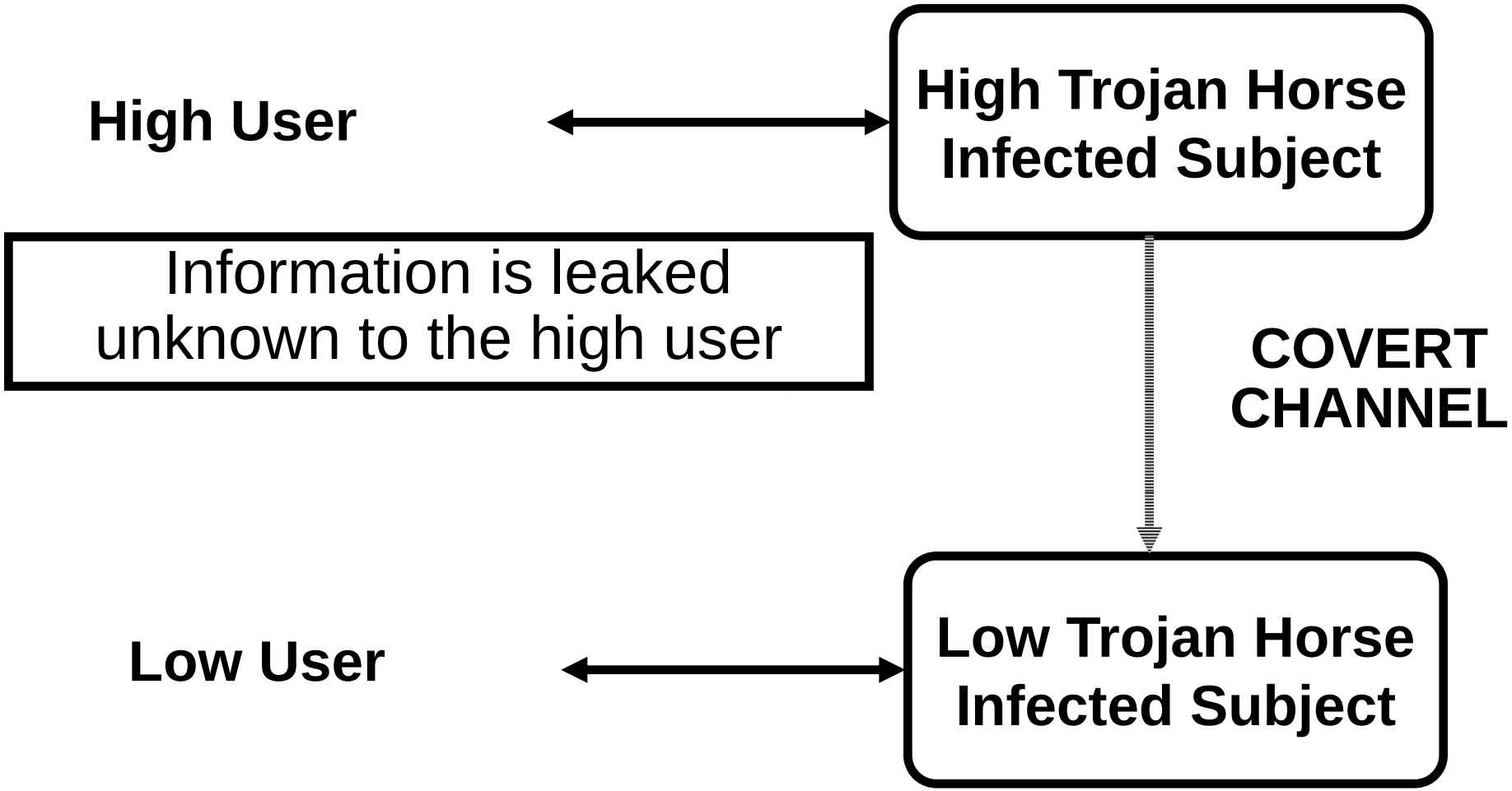
GIVEN

Information flow upwards

EQUIVALENT BLP LATTICE

Information flow upwards

LBAC: LATTICE STRUCTURES



Discuss figures from LBAC93 paper