Attribute-Based Access Control Models and Beyond

Prof. Ravi Sandhu

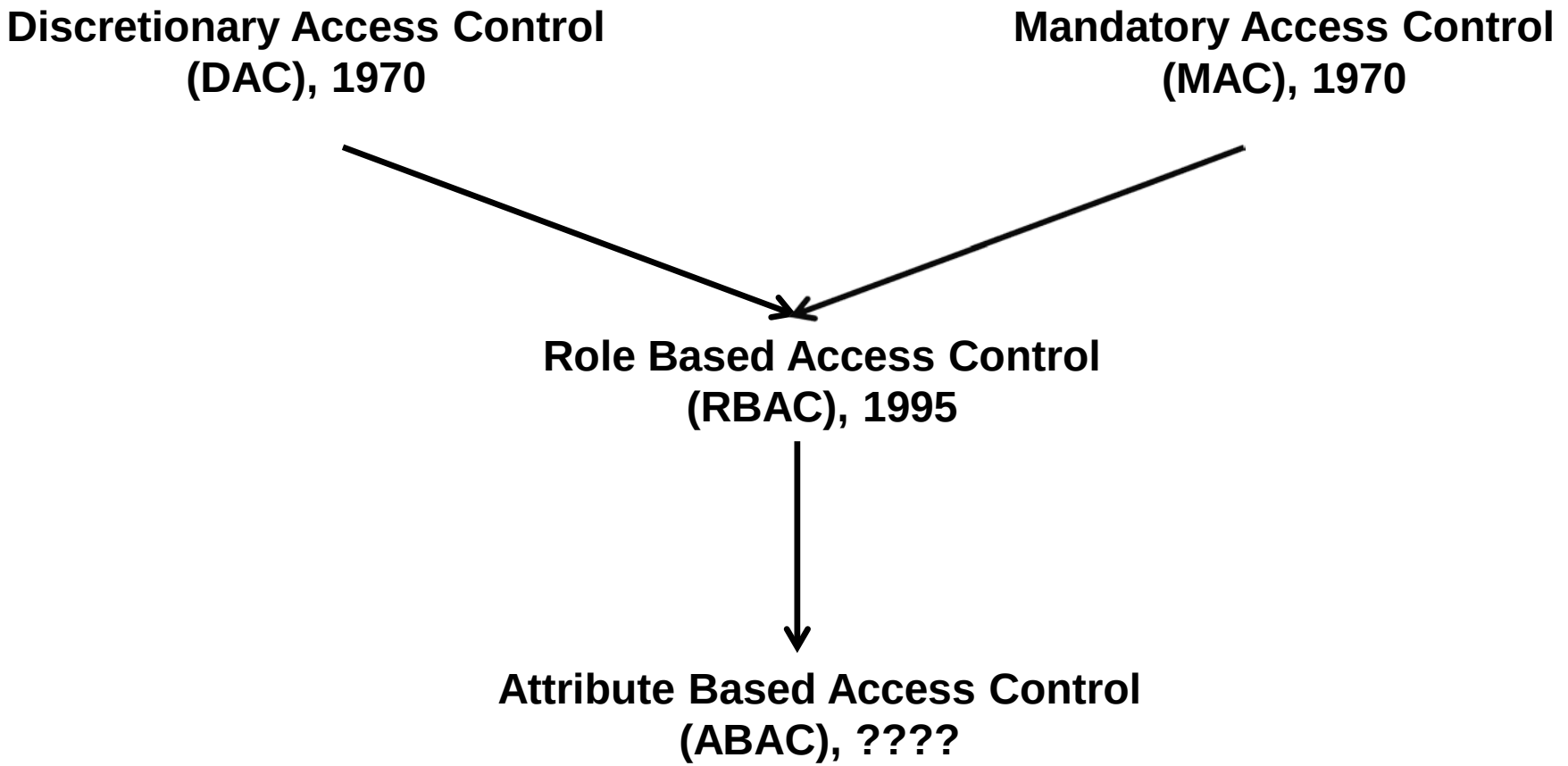
Executive Director, Institute for Cyber Security
Lutcher Brown Endowed Chair in Cyber Security
University of Texas at San Antonio

Cybersecurity Lecture Series
Austrian Institute of Technology (AIT) and TU Vienna
June 3, 2015

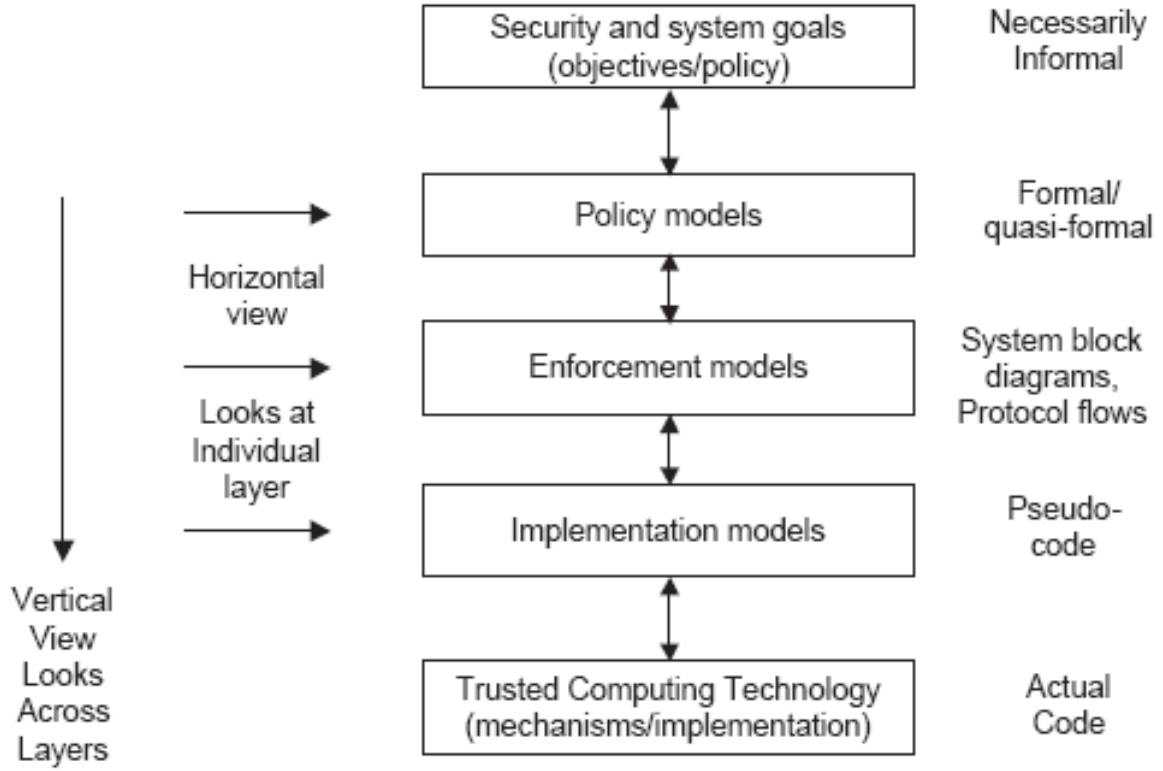
ravi.sandhu@utsa.edu, www.profsandhu.com, www.ics.utsa.edu

v2.0

Access Control



PEI Models

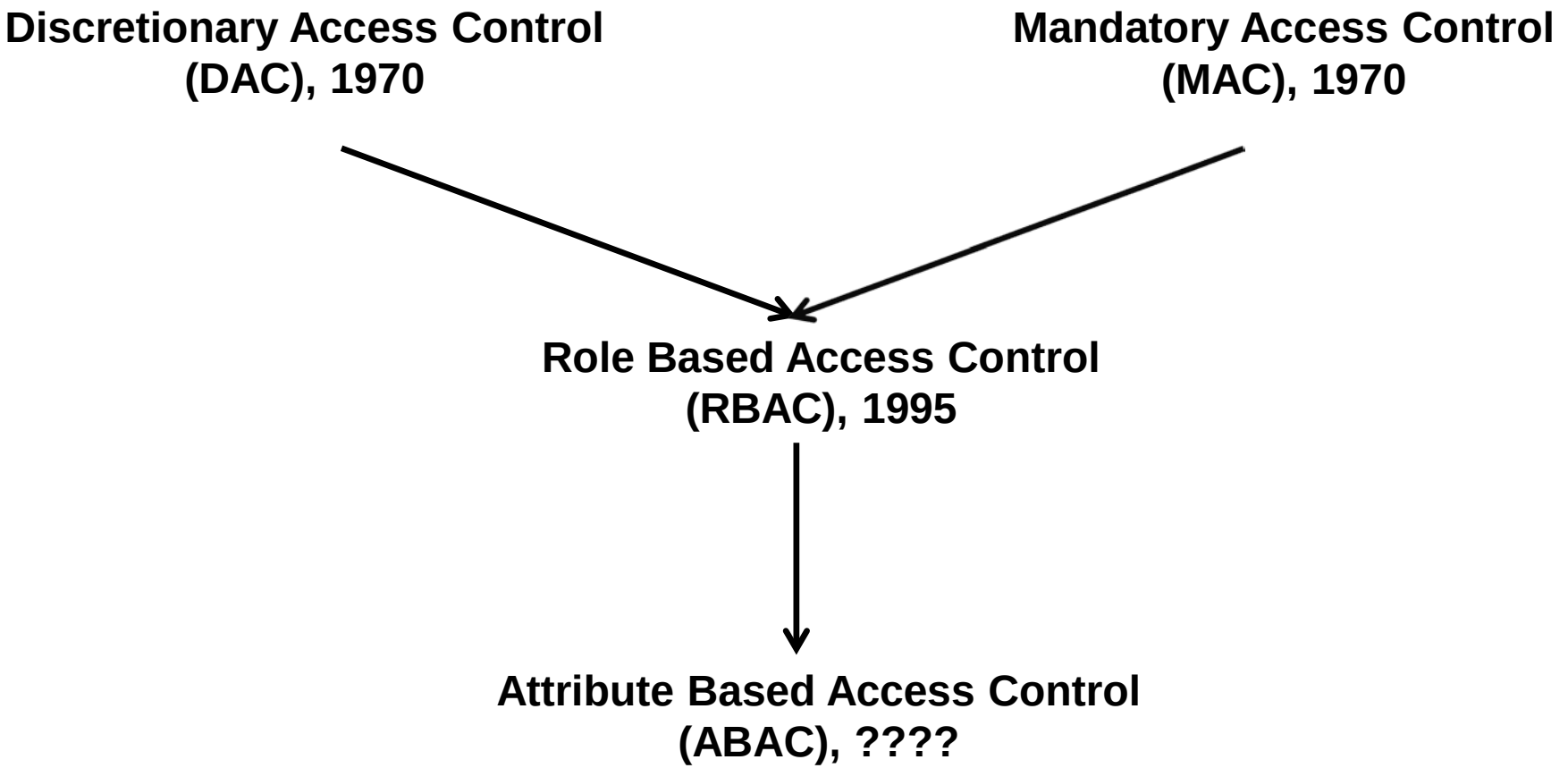


Idealized

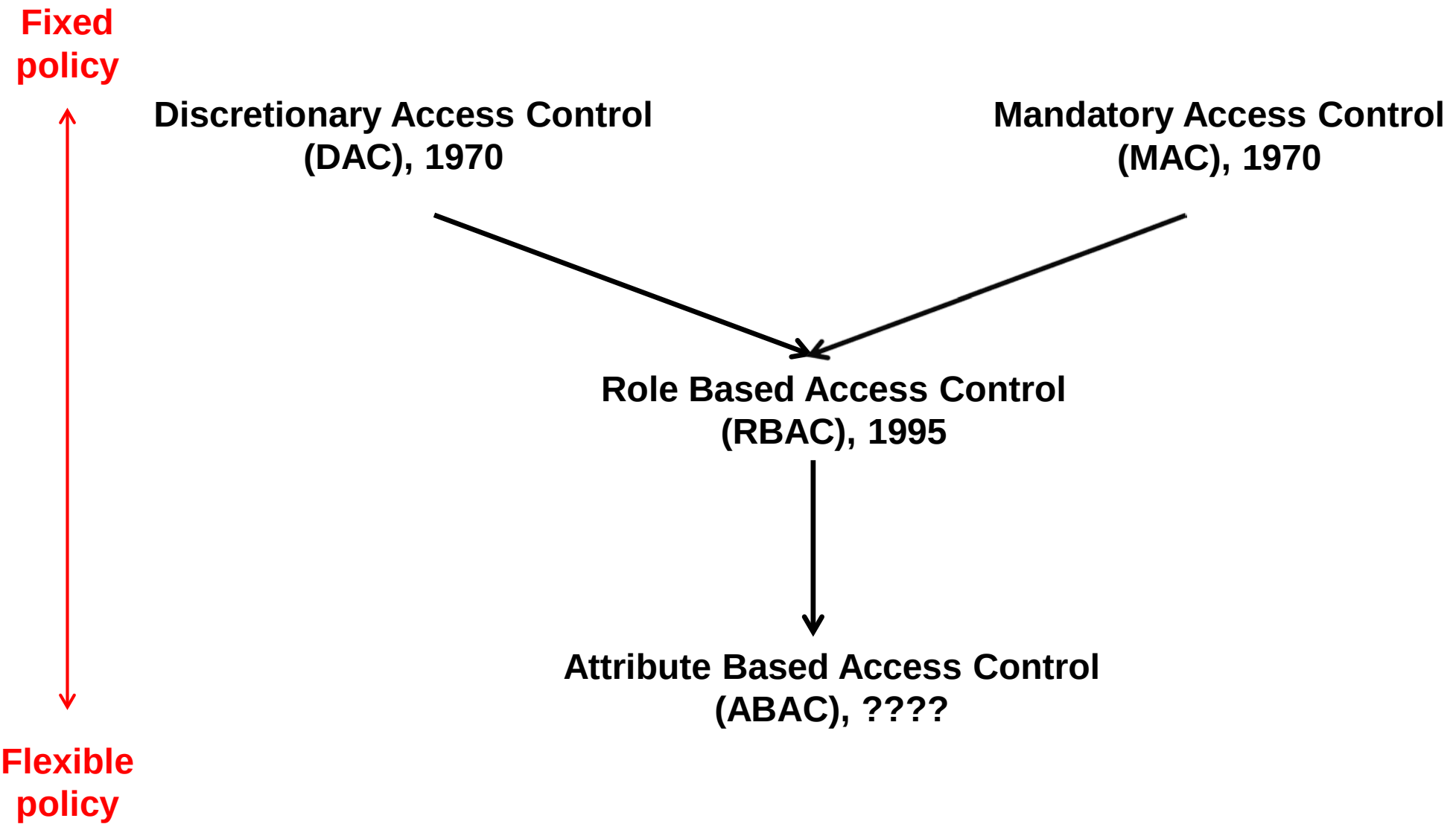
Enforceable (Approximate)

Codeable

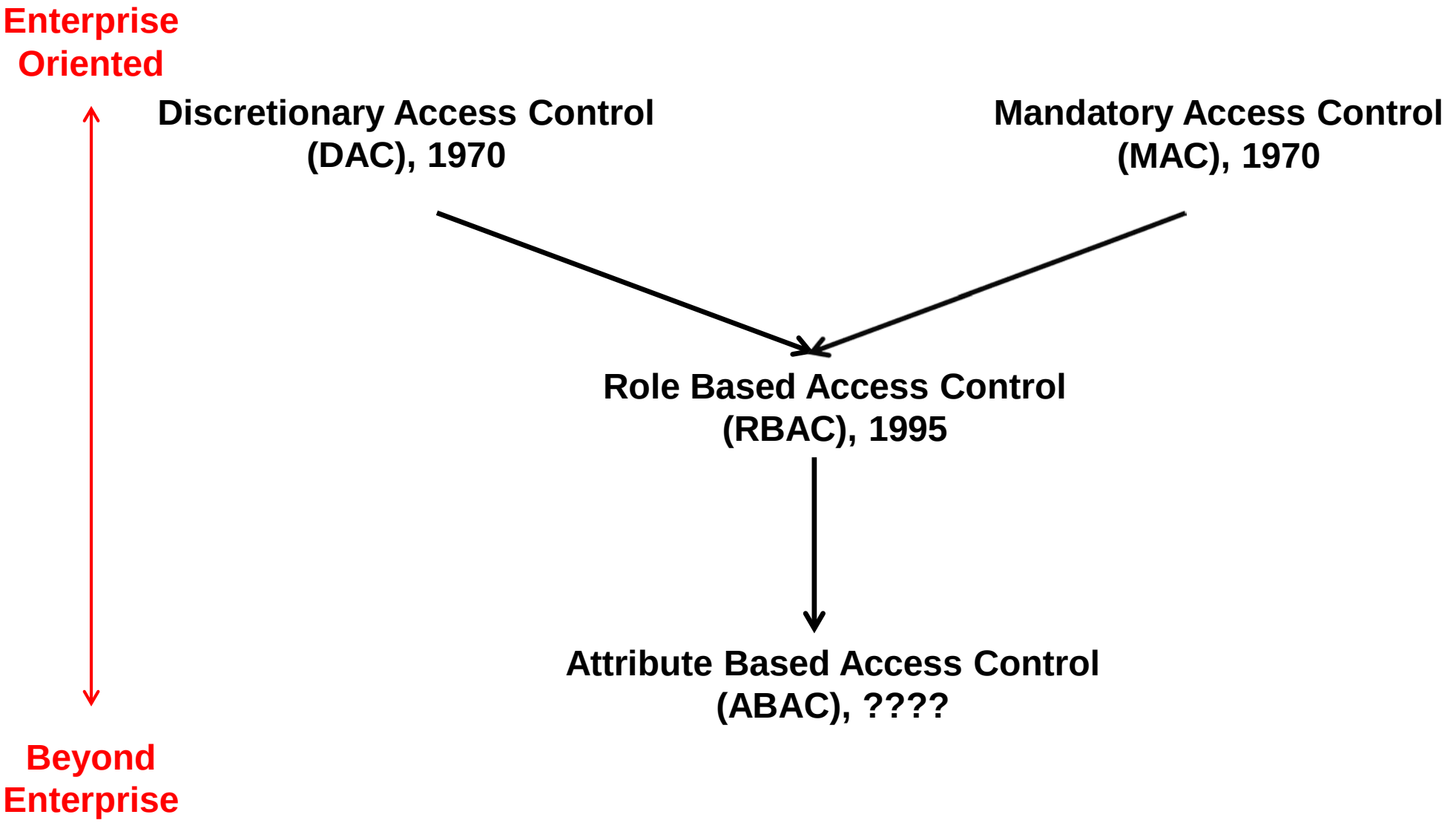
Access Control



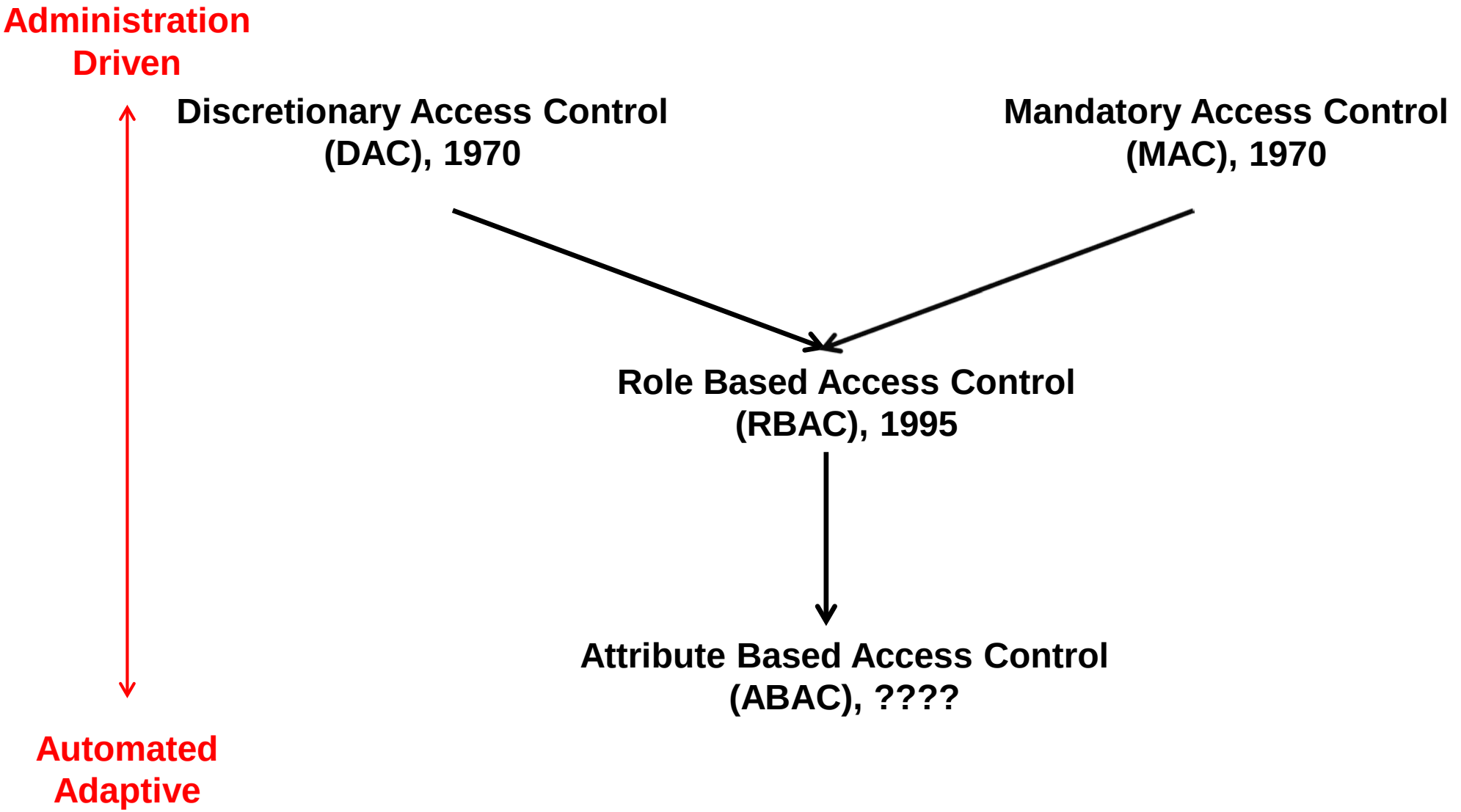
Access Control



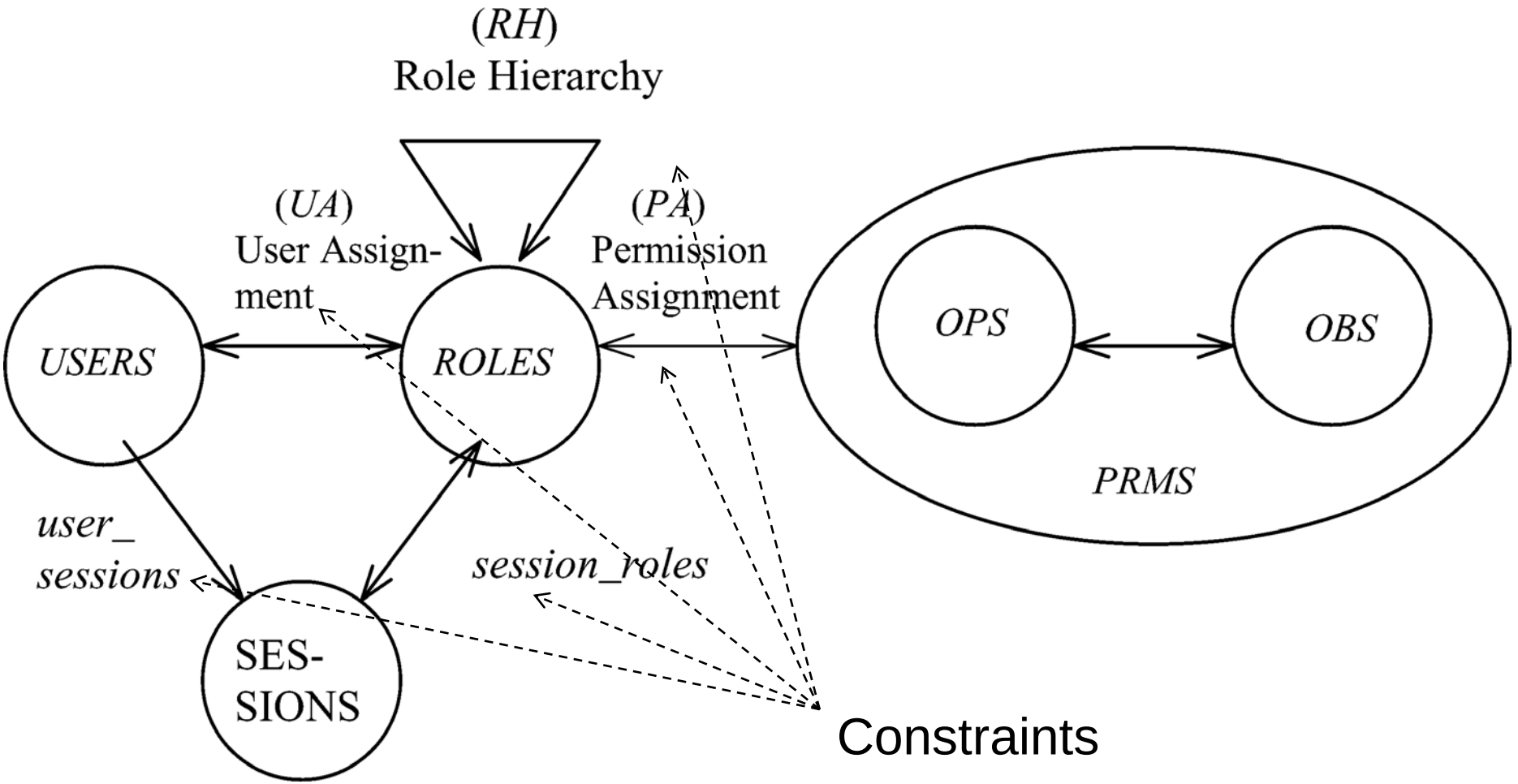
Access Control



Access Control



RBAC96 Model



Fundamental Theorem of RBAC

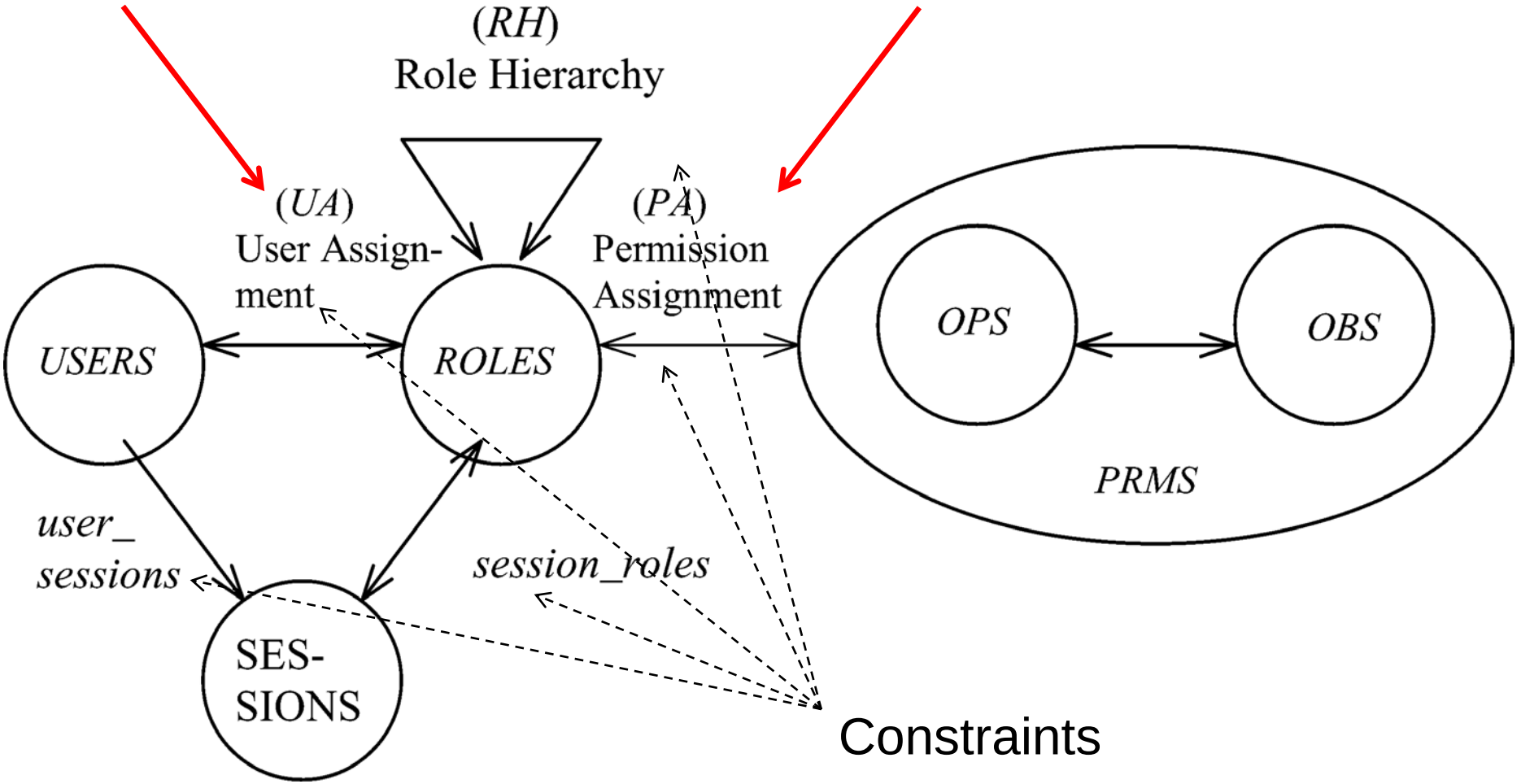
- RBAC can be configured to do MAC
- RBAC can be configured to do DAC
- RBAC is policy neutral

RBAC is neither MAC nor DAC!

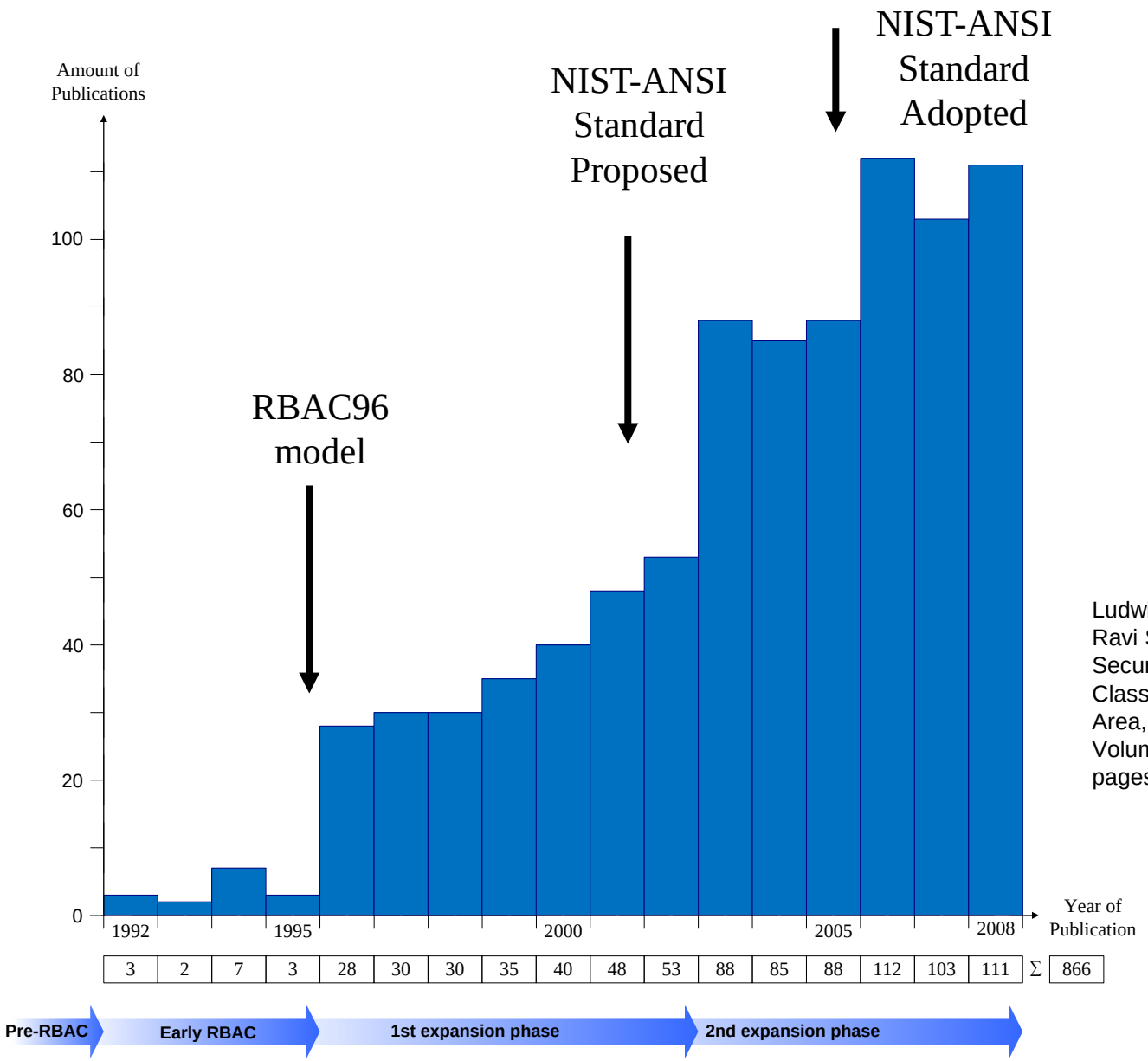
RBAC Shortcomings

Hard Enough

Impossible

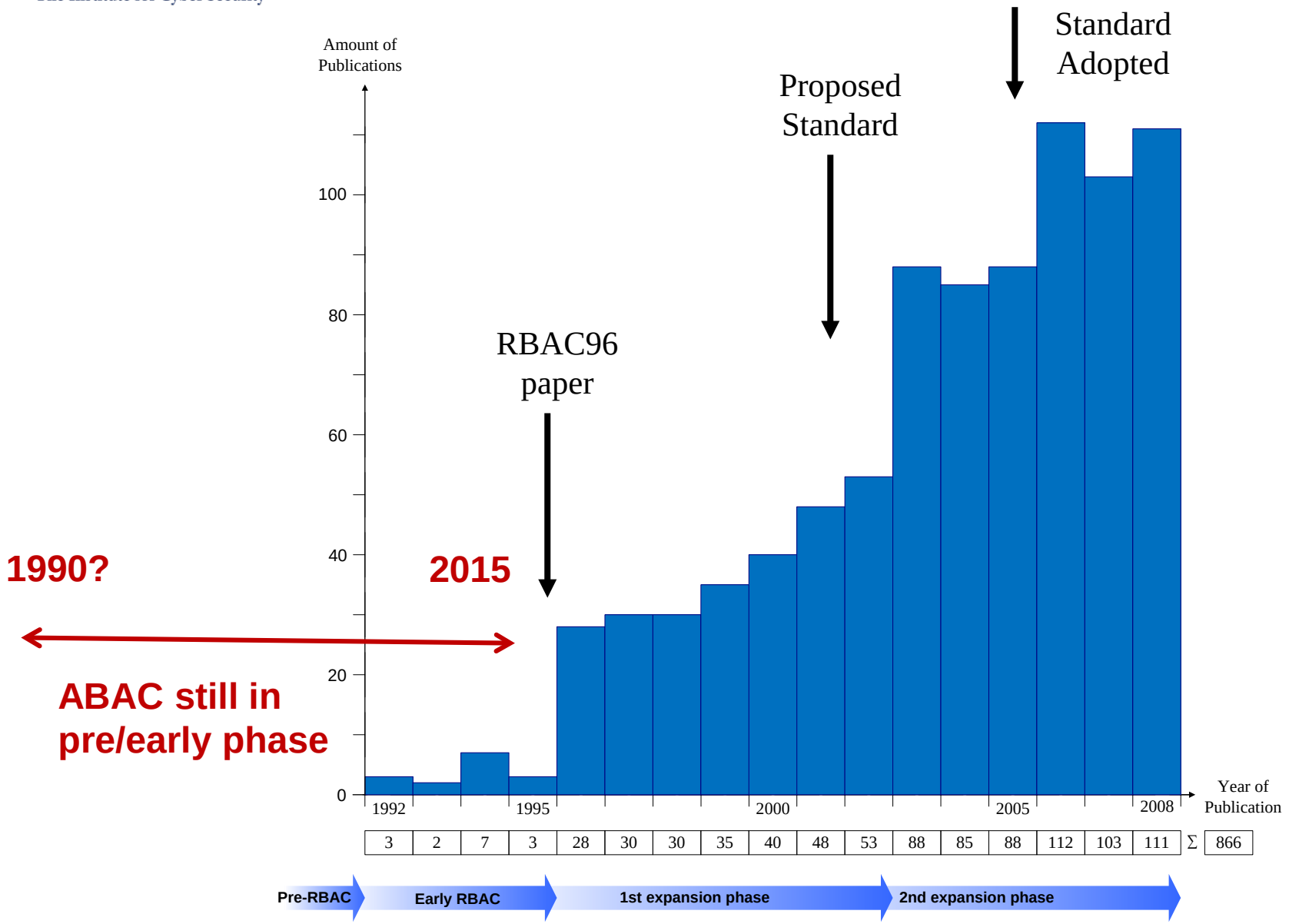


The RBAC Story

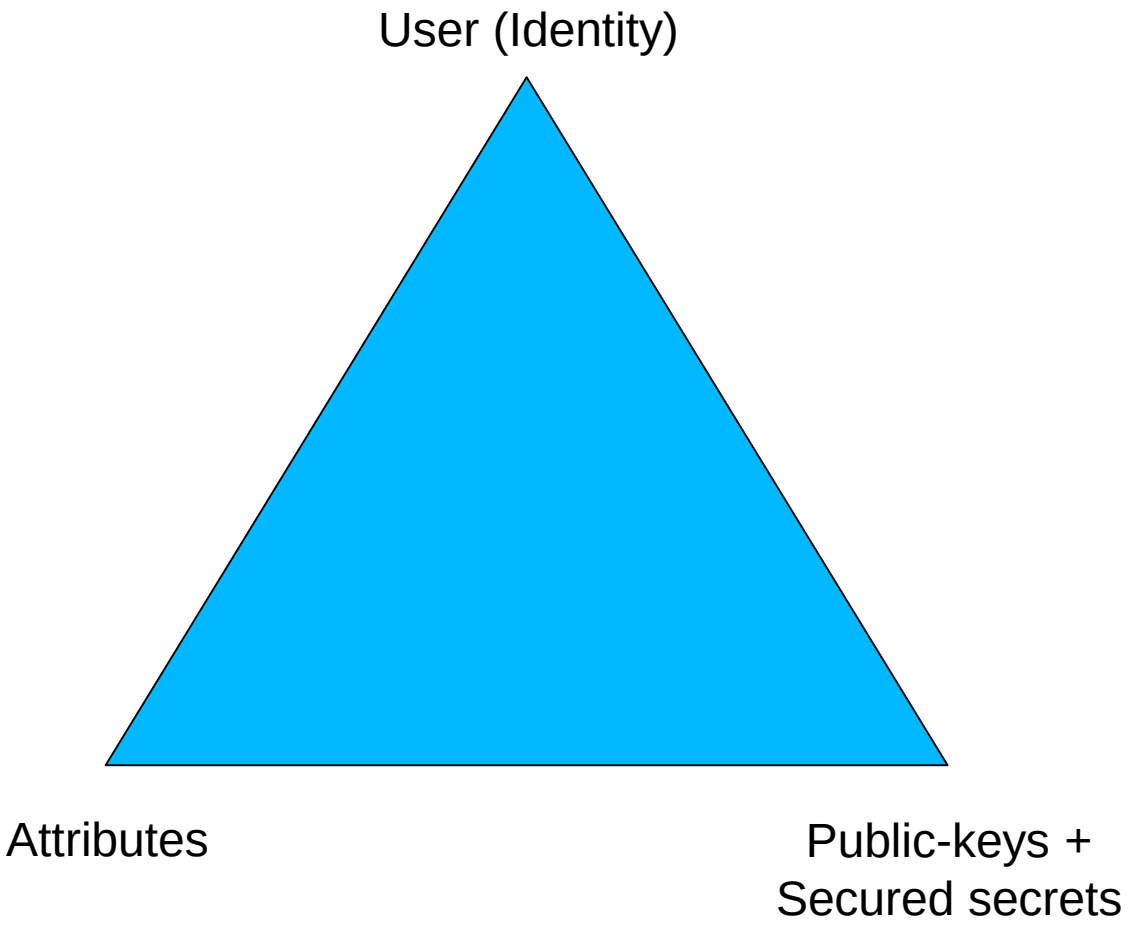


Ludwig Fuchs, Gunther Pernul and Ravi Sandhu, Roles in Information Security-A Survey and Classification of the Research Area, Computers & Security, Volume 30, Number 8, Nov. 2011, pages 748-76

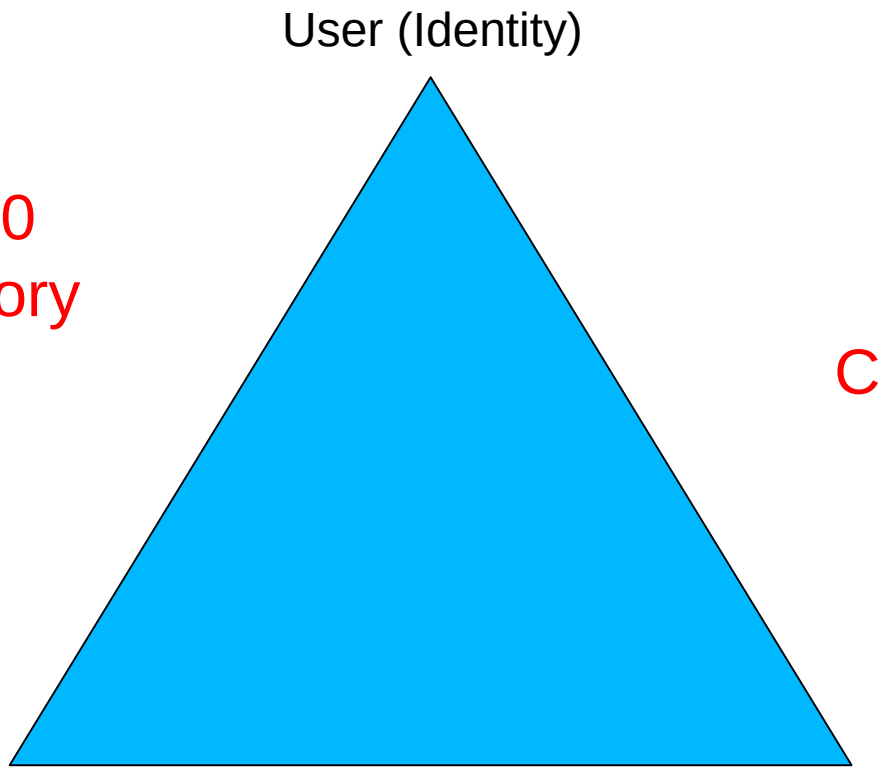
ABAC Status


Amount of Publications
Standard Adopted
Proposed Standard
RBAC96 paper
1990?
2015
ABAC still in pre/early phase
100
80
60
40
20
0
1992
1995
2000
2005
2008
Year of Publication
3 2 7 3 28 30 30 35 40 48 53 88 85 88 112 103 111 Σ 866
Pre-RBAC
Early RBAC
1st expansion phase
2nd expansion phase

ABAC is not New

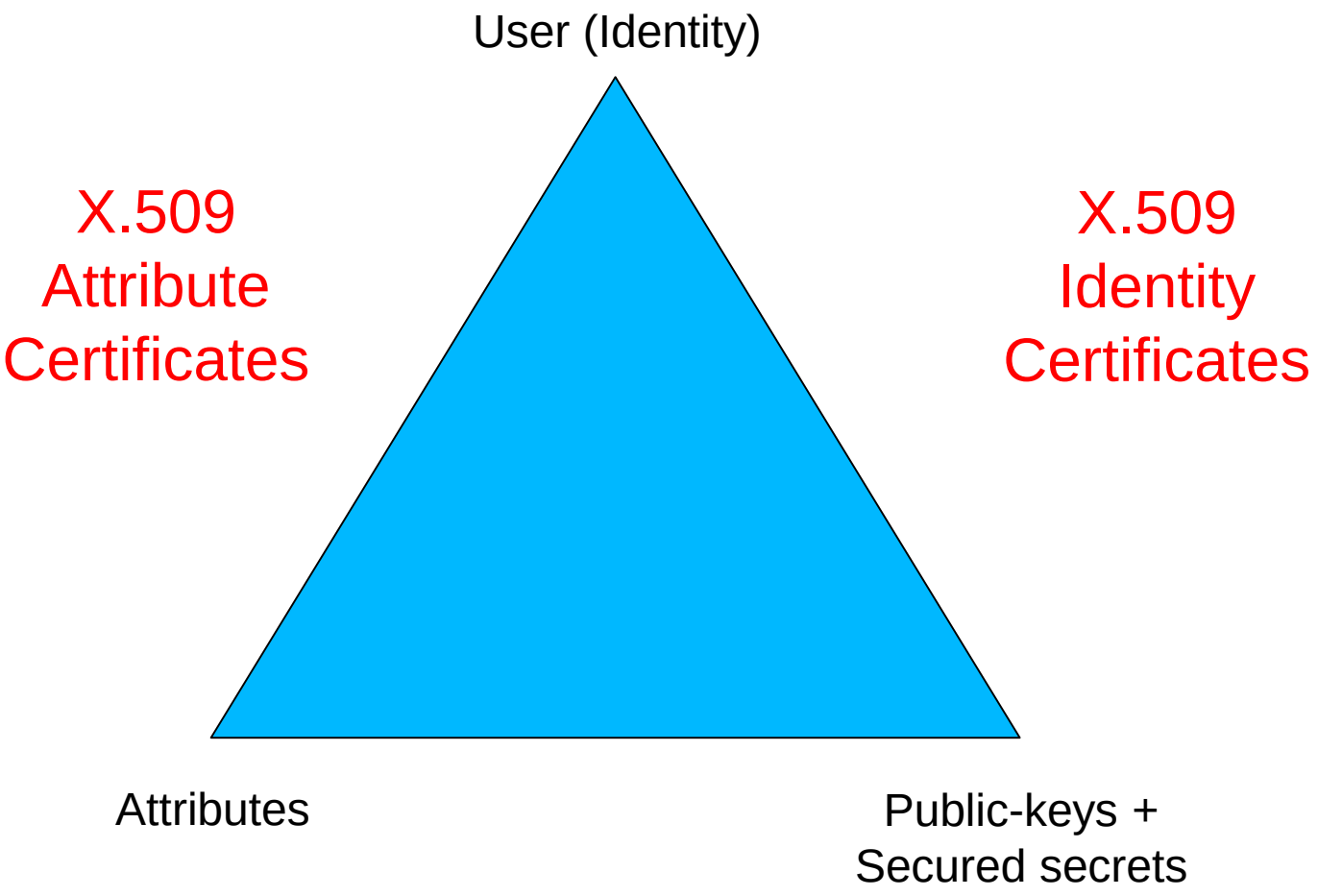


ABAC is not New



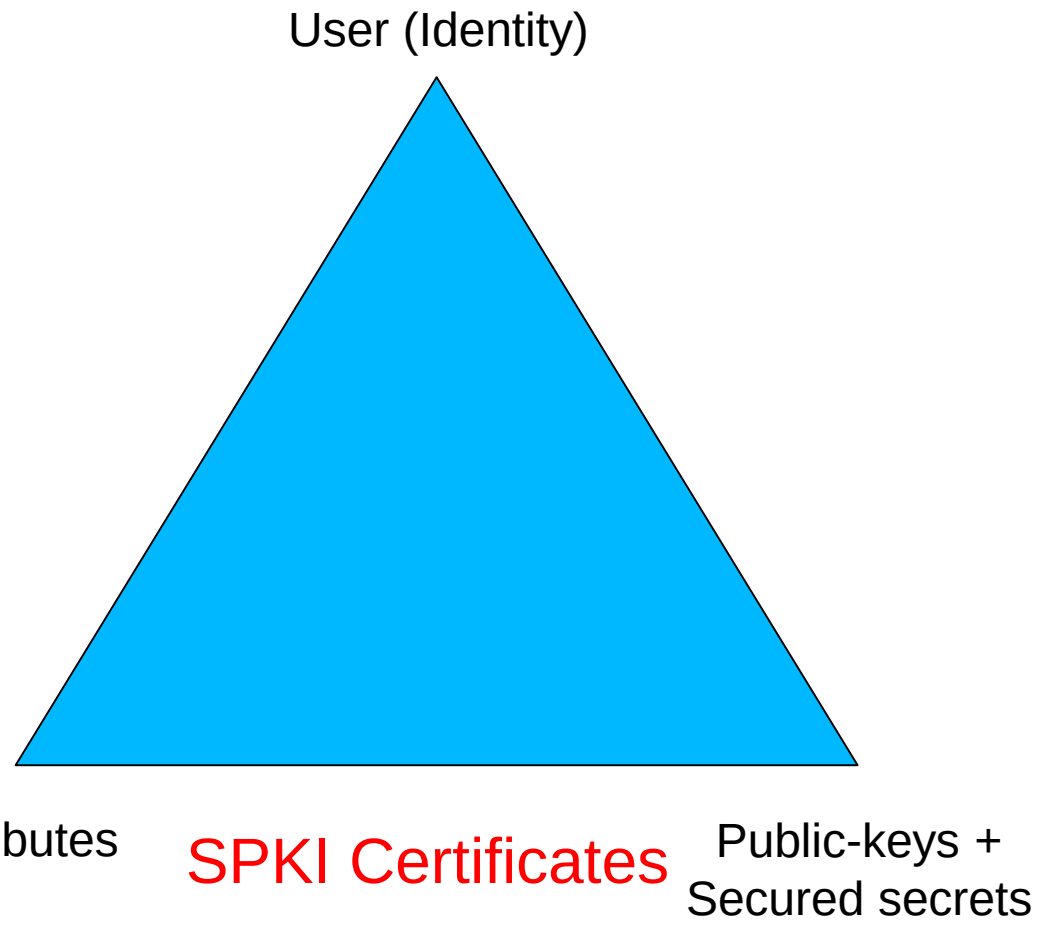
Pre Internet, early 1990s

ABAC is not New



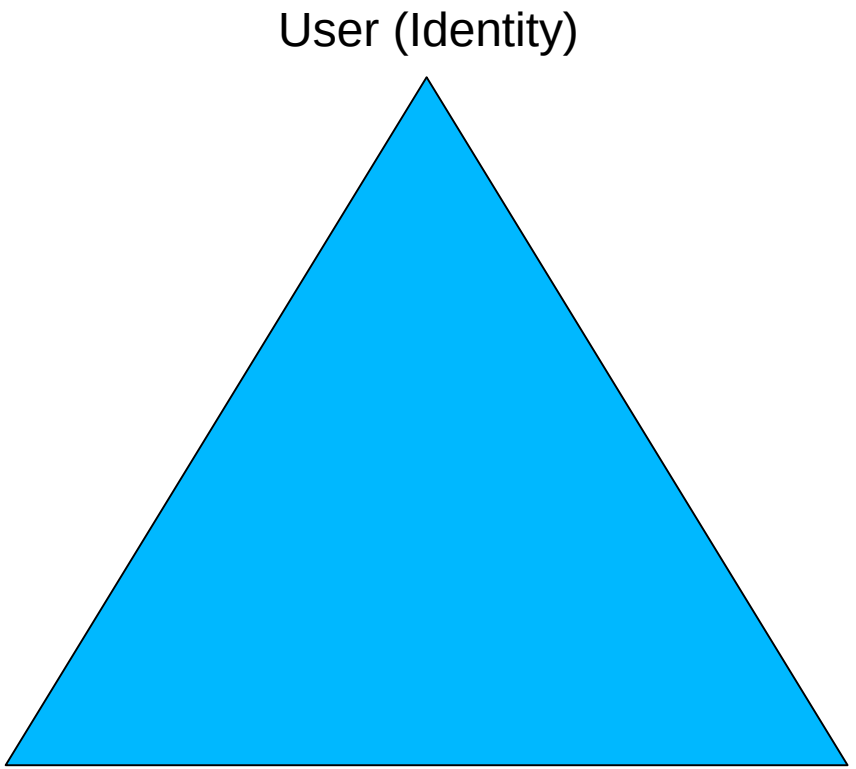
Post Internet, late 1990s

ABAC is not New



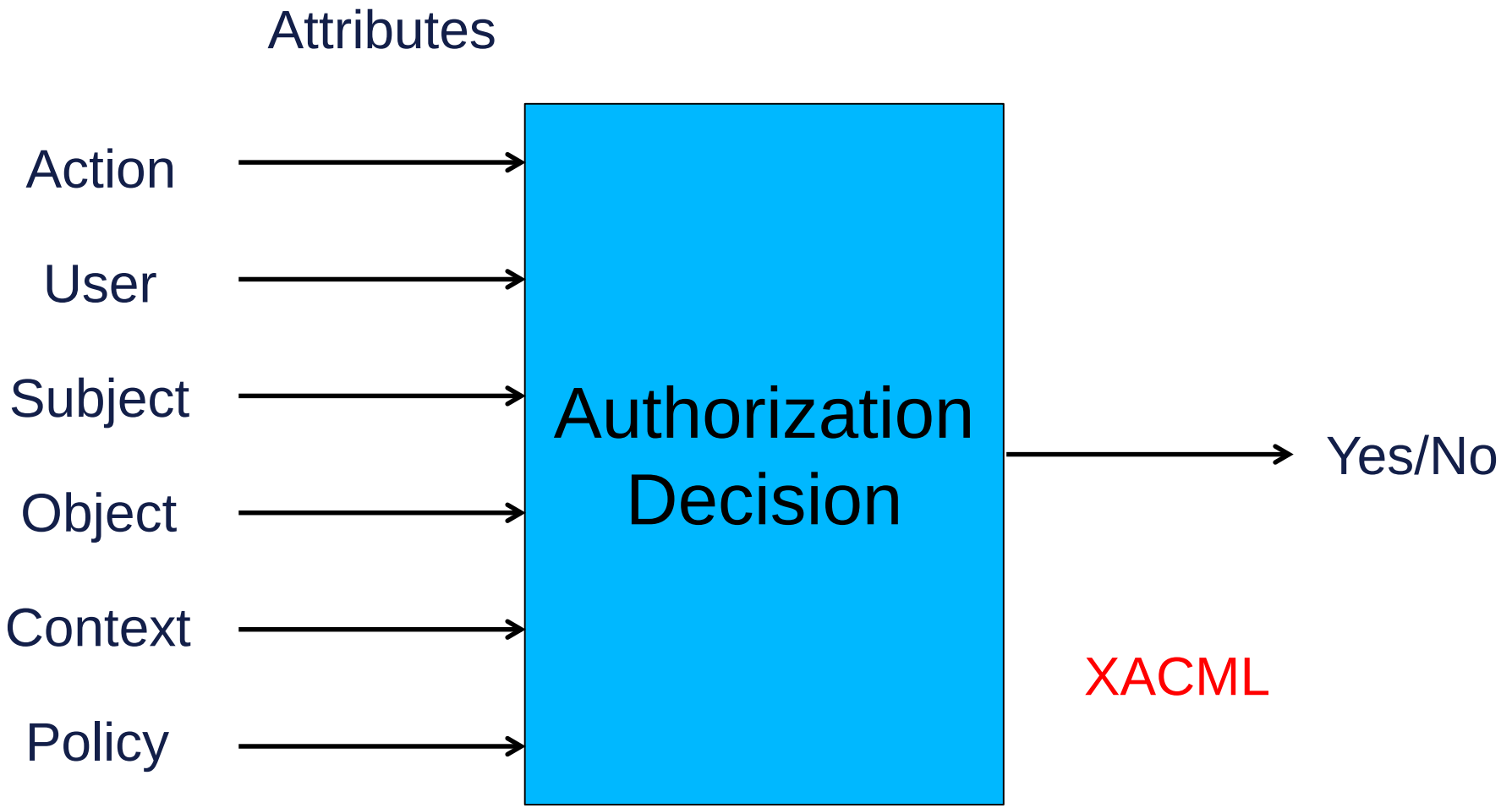
Post Internet, late 1990s

ABAC is not New



Mature Internet, 2000s

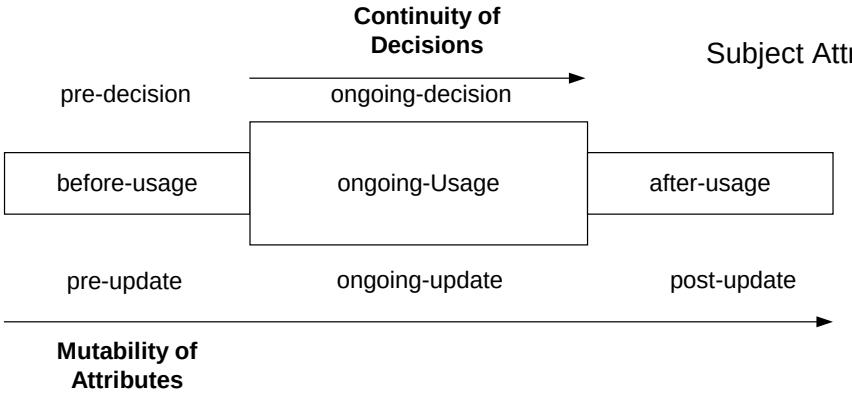
ABAC is not New

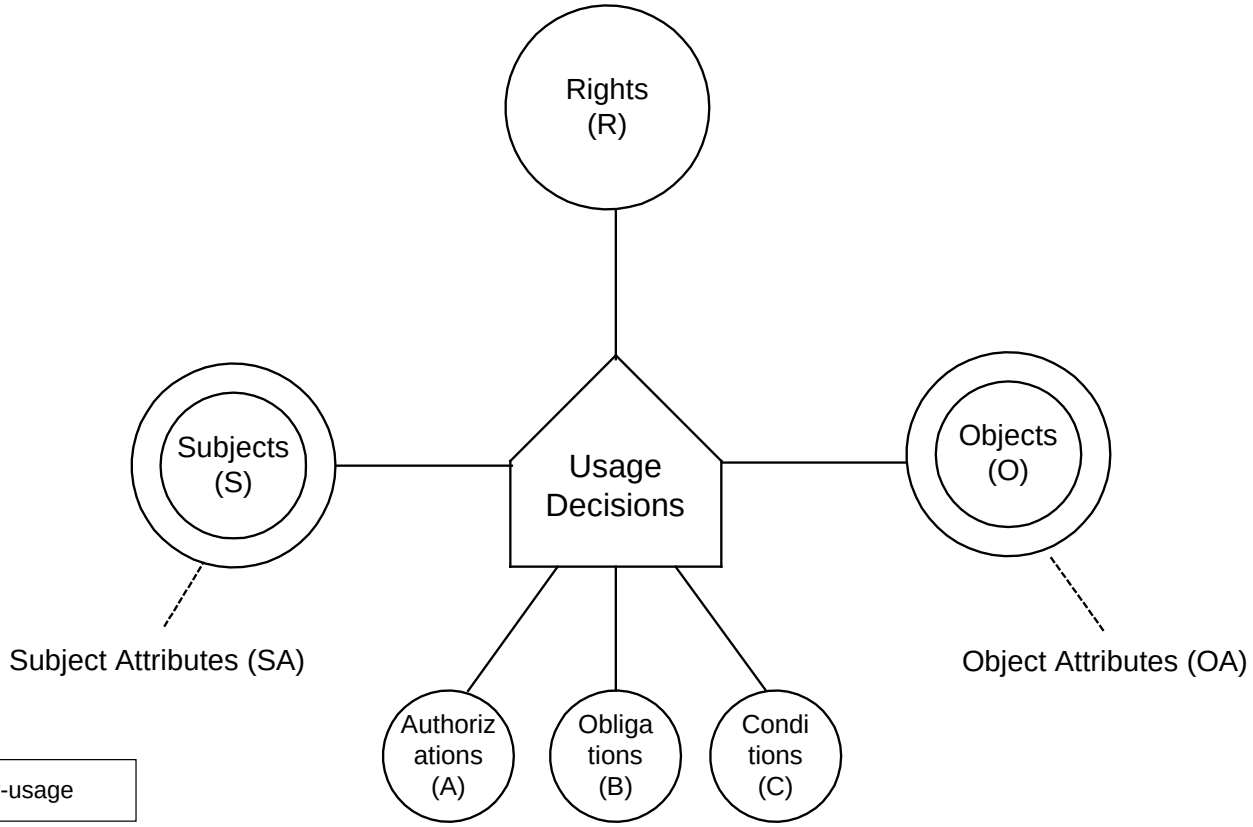


Mature Internet, 2000s

ABAC is not New

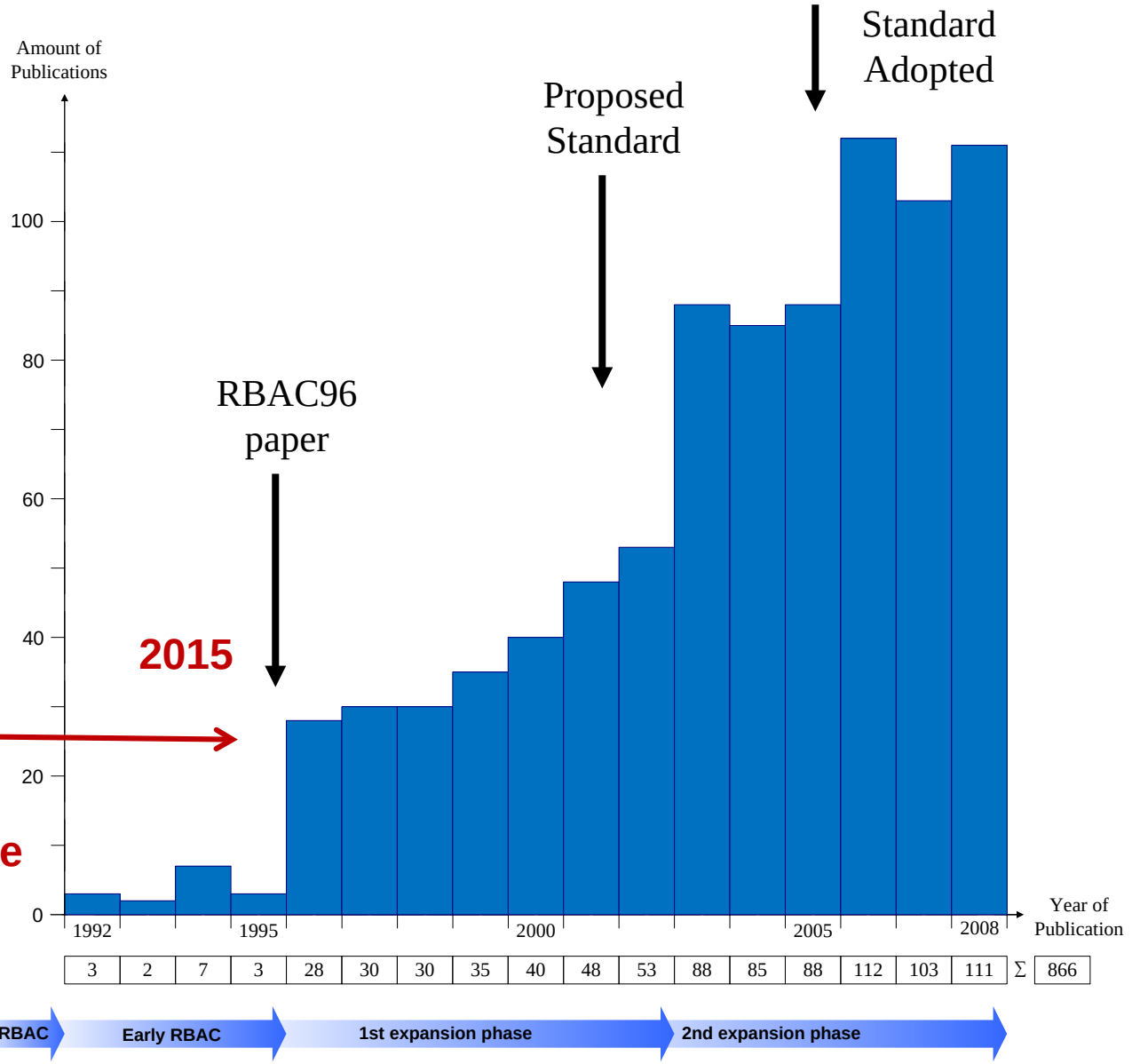
- unified model integrating
  - authorization
  - obligation
  - conditions
- and incorporating
  - continuity of decisions
  - mutability of attributes





Usage Control Models, early 2000s

ABAC Status

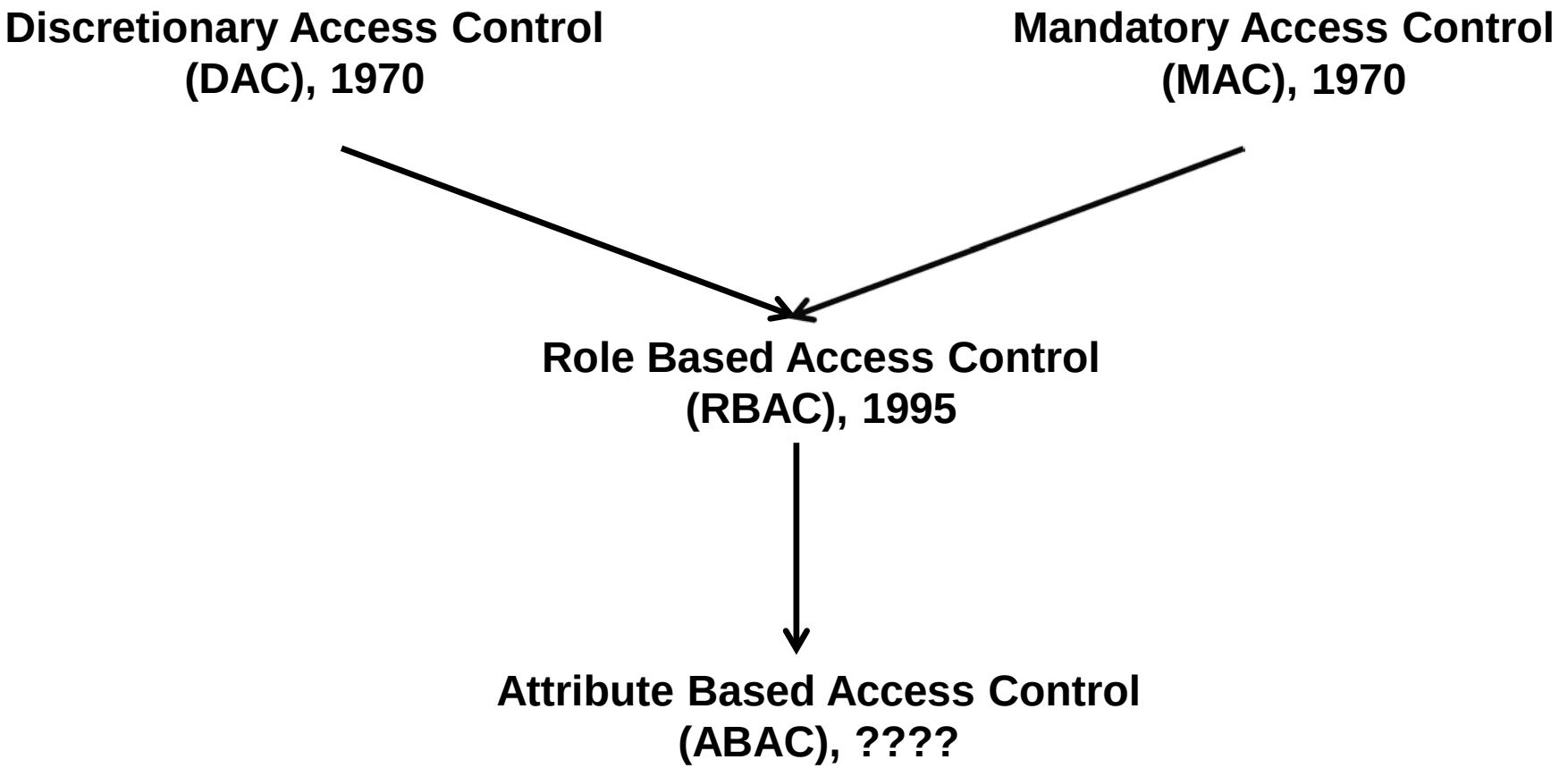


1990?

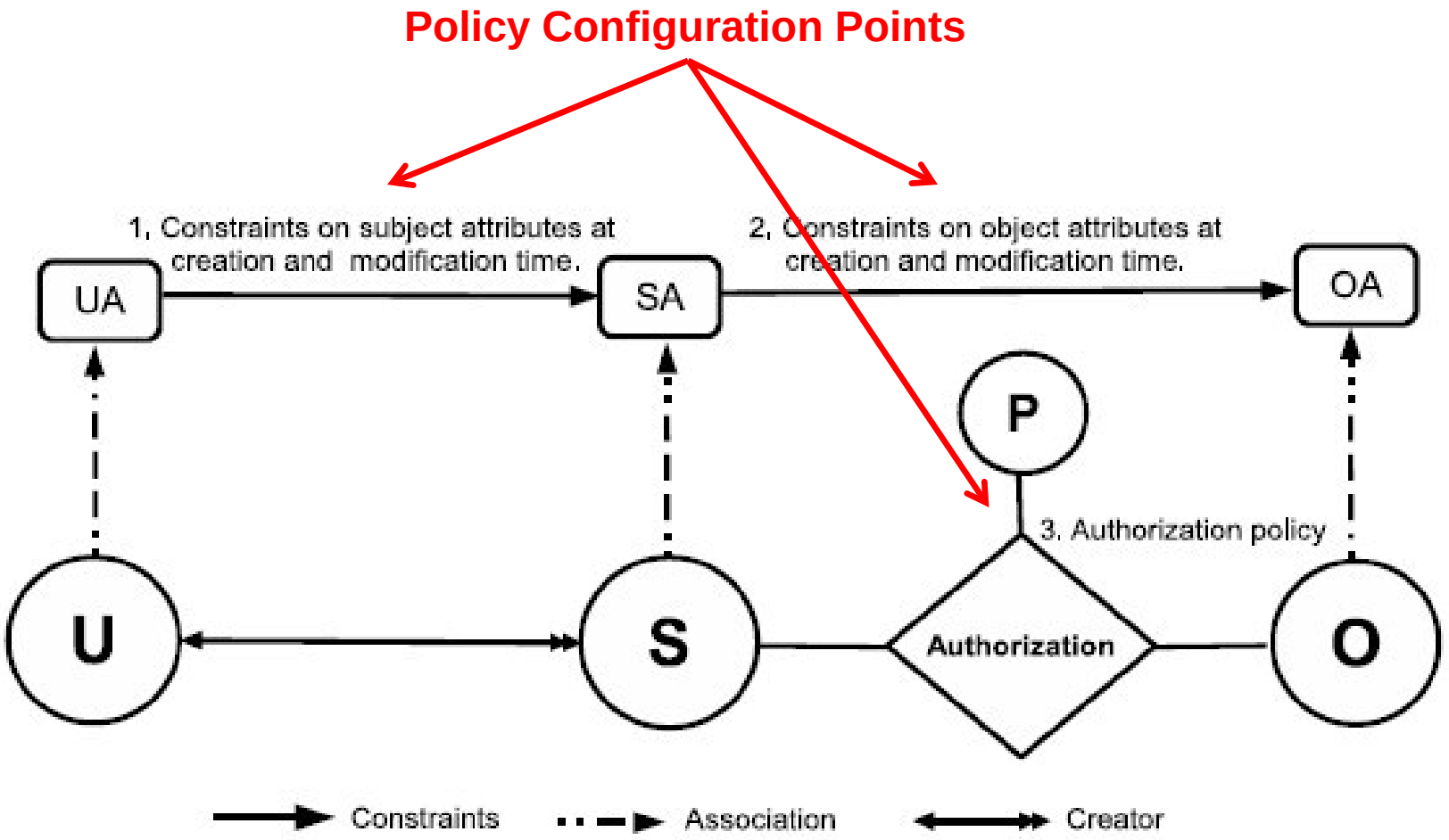
2015

ABAC still in pre/early phase

Access Control

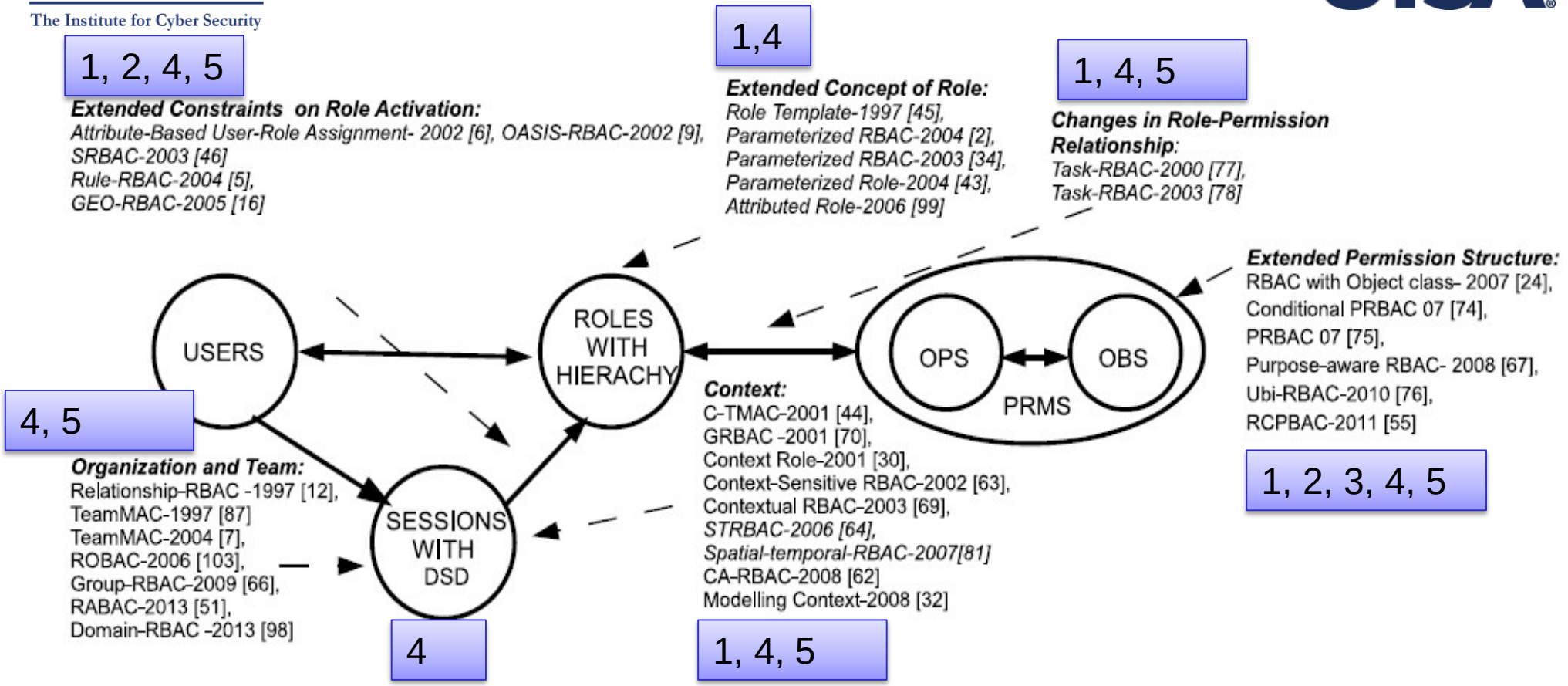


ABACα Model Structure



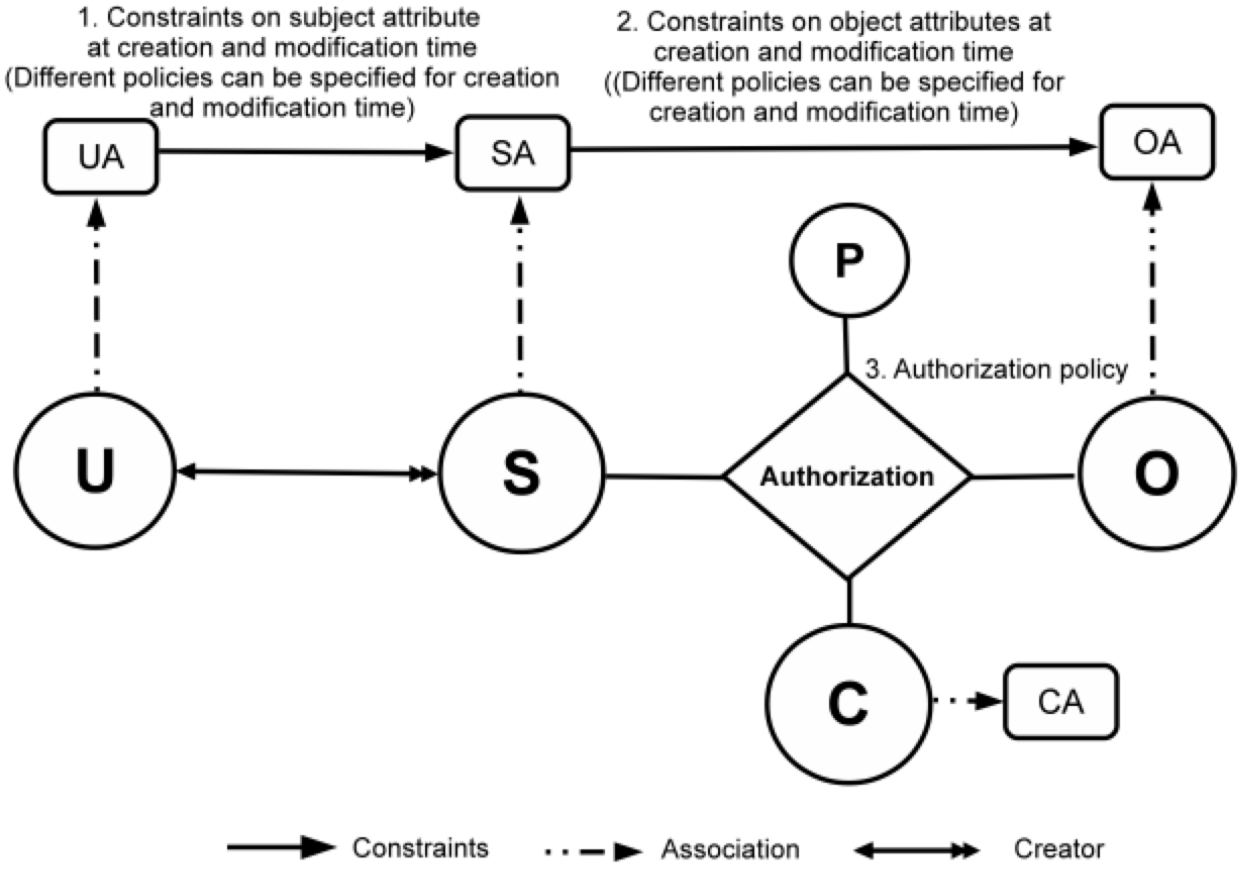
Can be configured to do simple forms of DAC, MAC, RBAC

RBAC Extensions



1. Context Attributes
2. Subject attribute constraints policy are different at creation and modification time.
3. Subject attributes constrained by attributes of subjects created by the same user.
4. Policy Language
5. Meta-Attributes

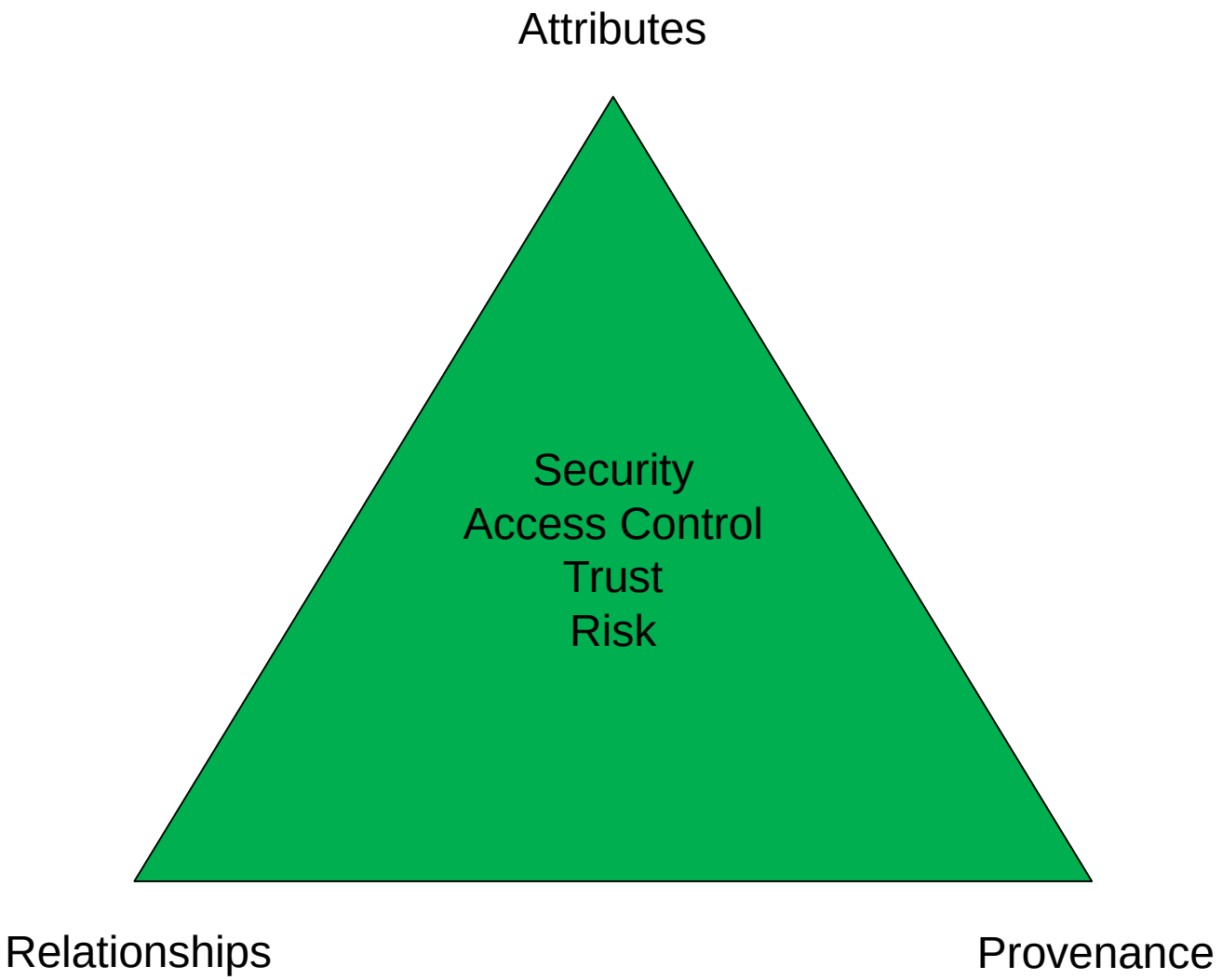
ABAC$_\beta$ Model



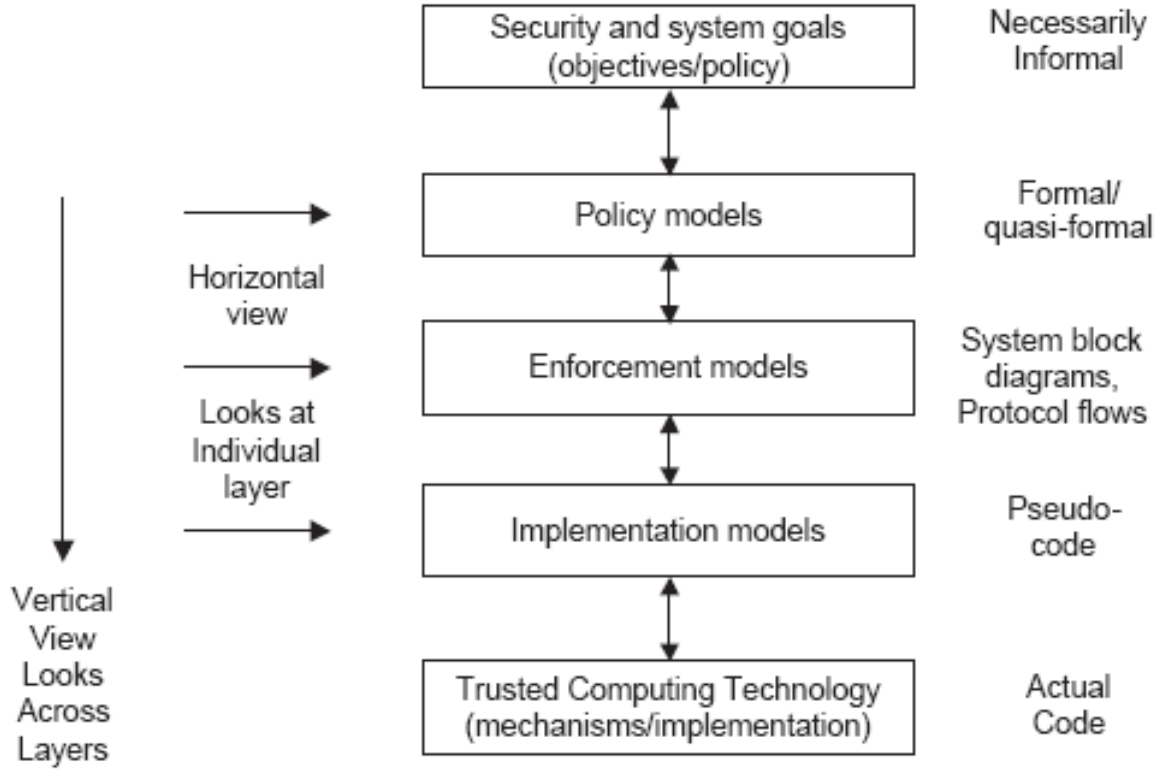
Can be configured to do many RBAC extensions

SOME RESEARCH CHALLENGES

Ultimate Unified Model



Expressive Power

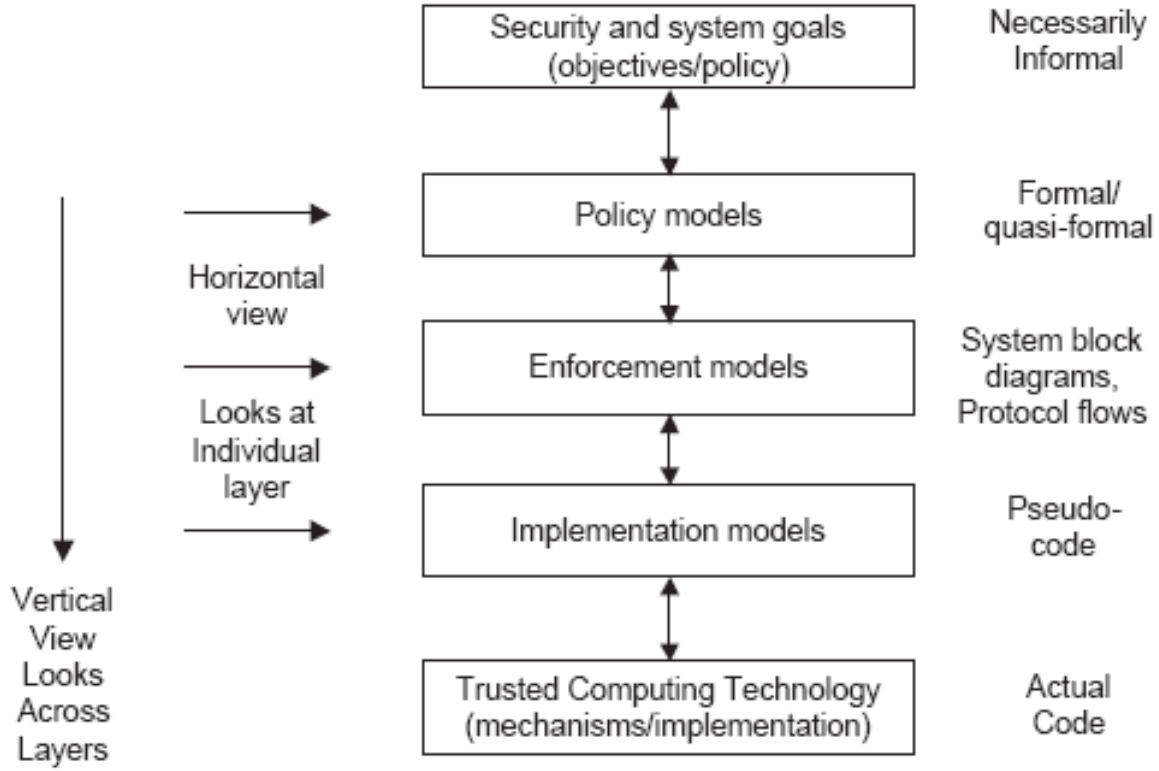


Idealized

Enforceable (Approximate)

Codeable

Safety Analysis

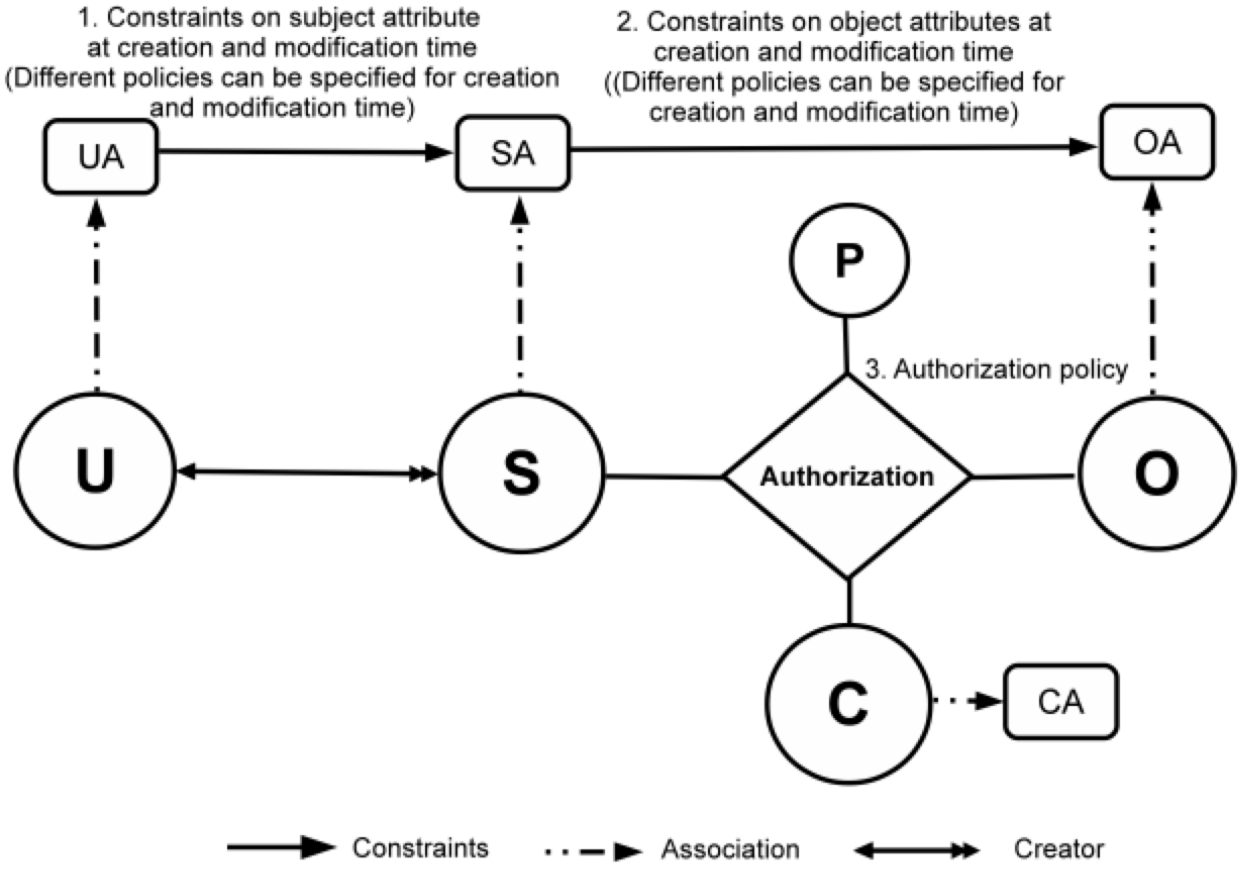


Idealized

Enforceable (Approximate)

Codeable

Attribute and Policy Engineering



Application Domains

- Cloud computing
- Internet of Things
- …….

Access Control