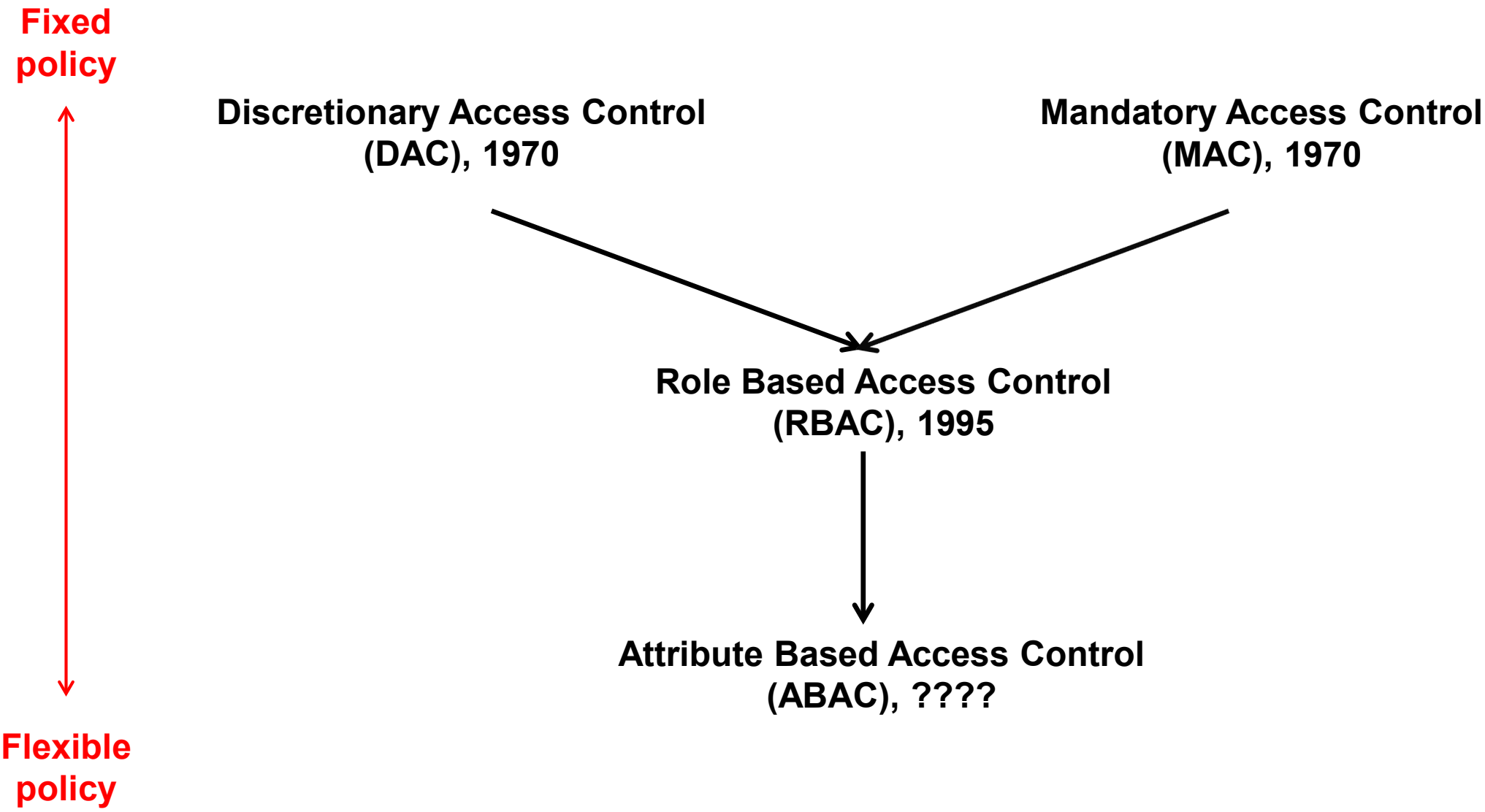
Attribute-Based Access Control (ABAC)

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 4

ravi.utsa@gmail.com
www.profsandhu.com

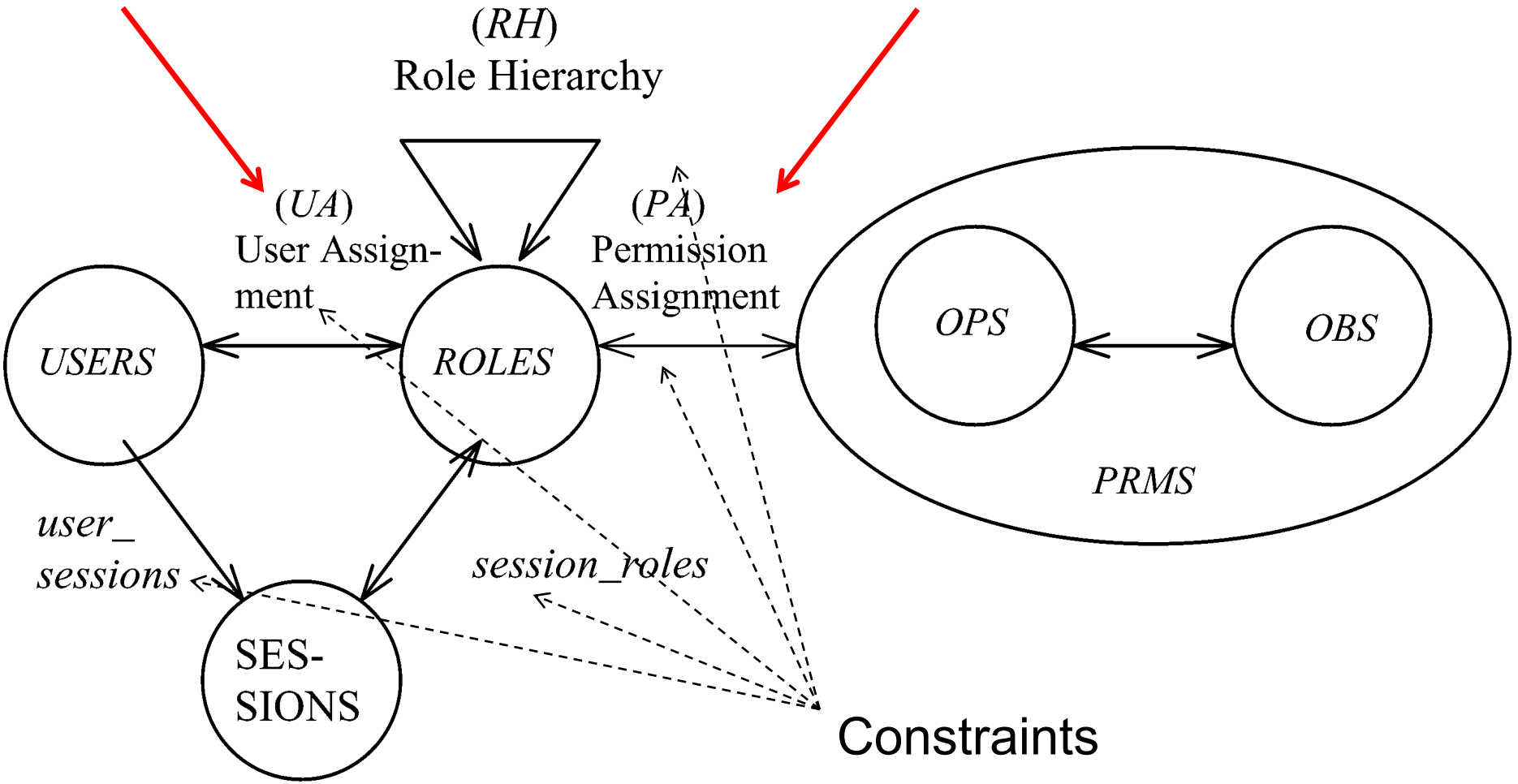
Access Control



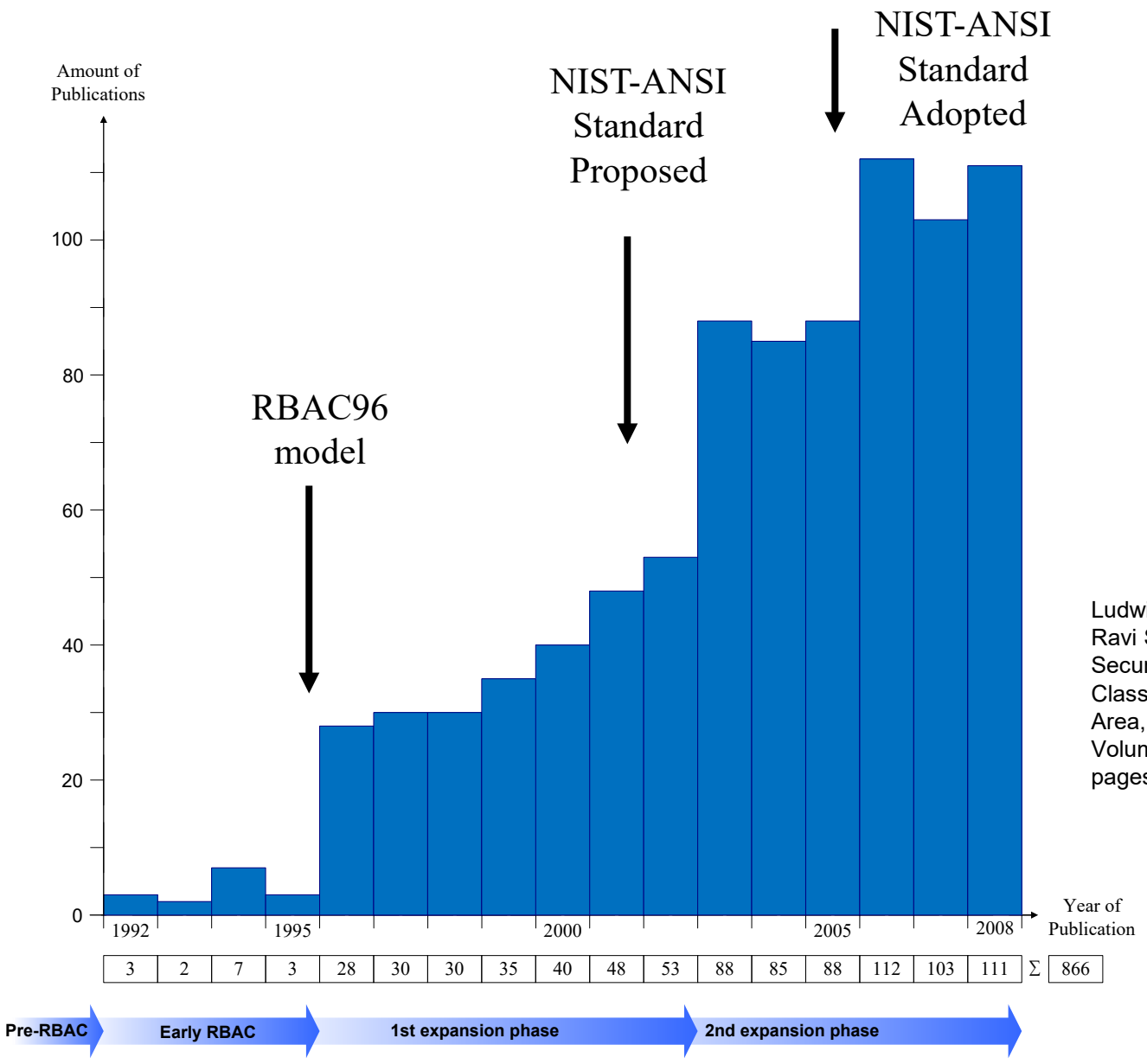
RBAC Shortcomings

Hard Enough

Impossible

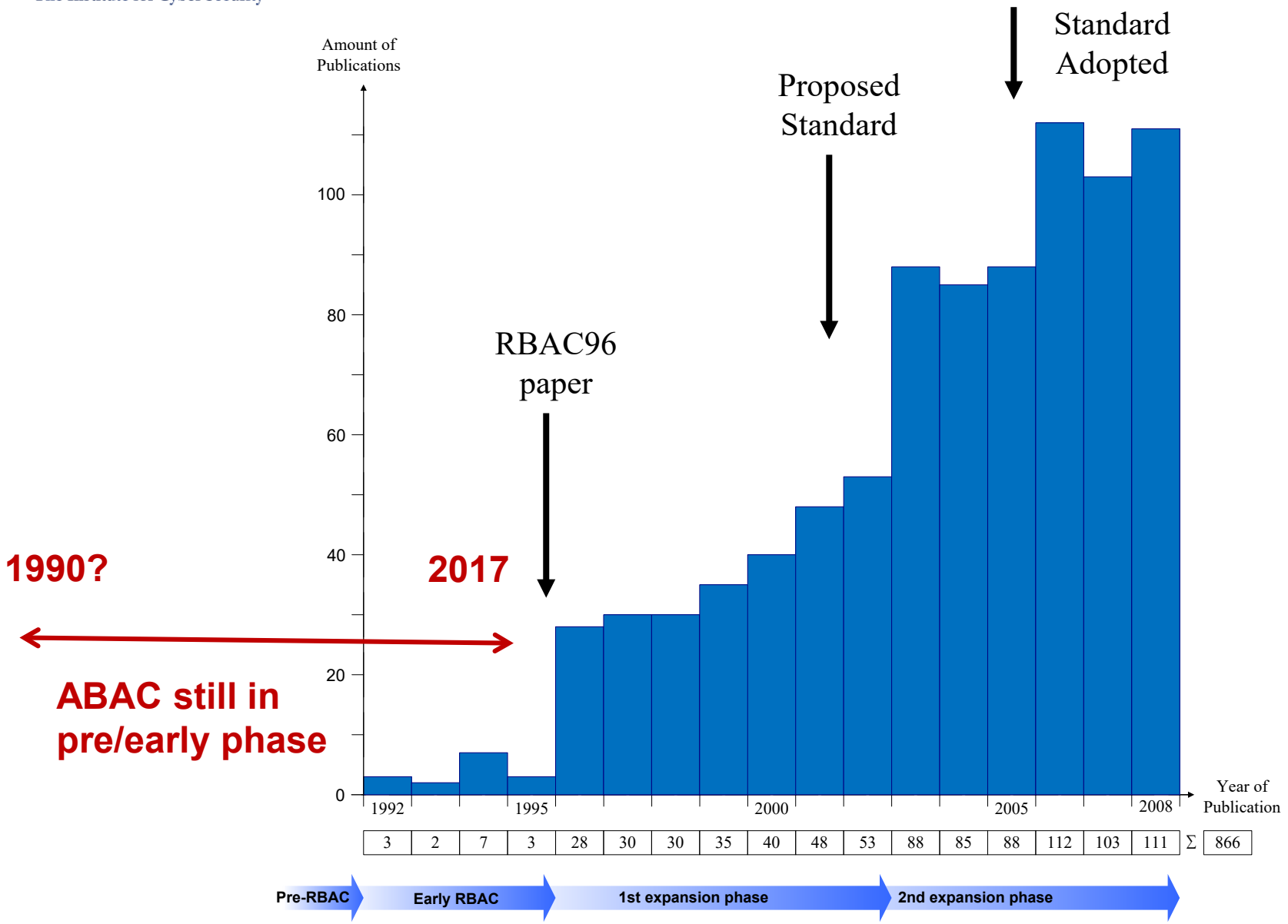


The RBAC Story

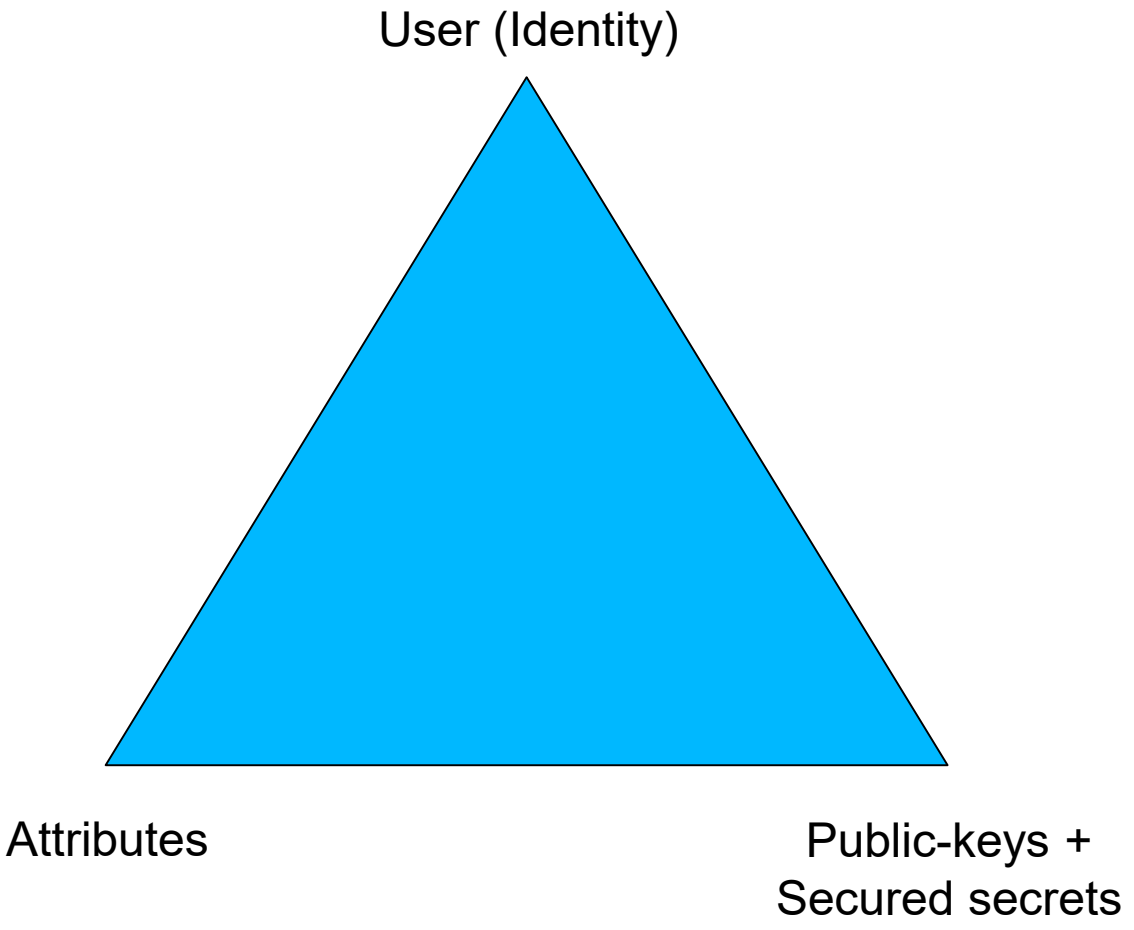


Ludwig Fuchs, Gunther Pernul and Ravi Sandhu, Roles in Information Security-A Survey and Classification of the Research Area, Computers & Security, Volume 30, Number 8, Nov. 2011, pages 748-76

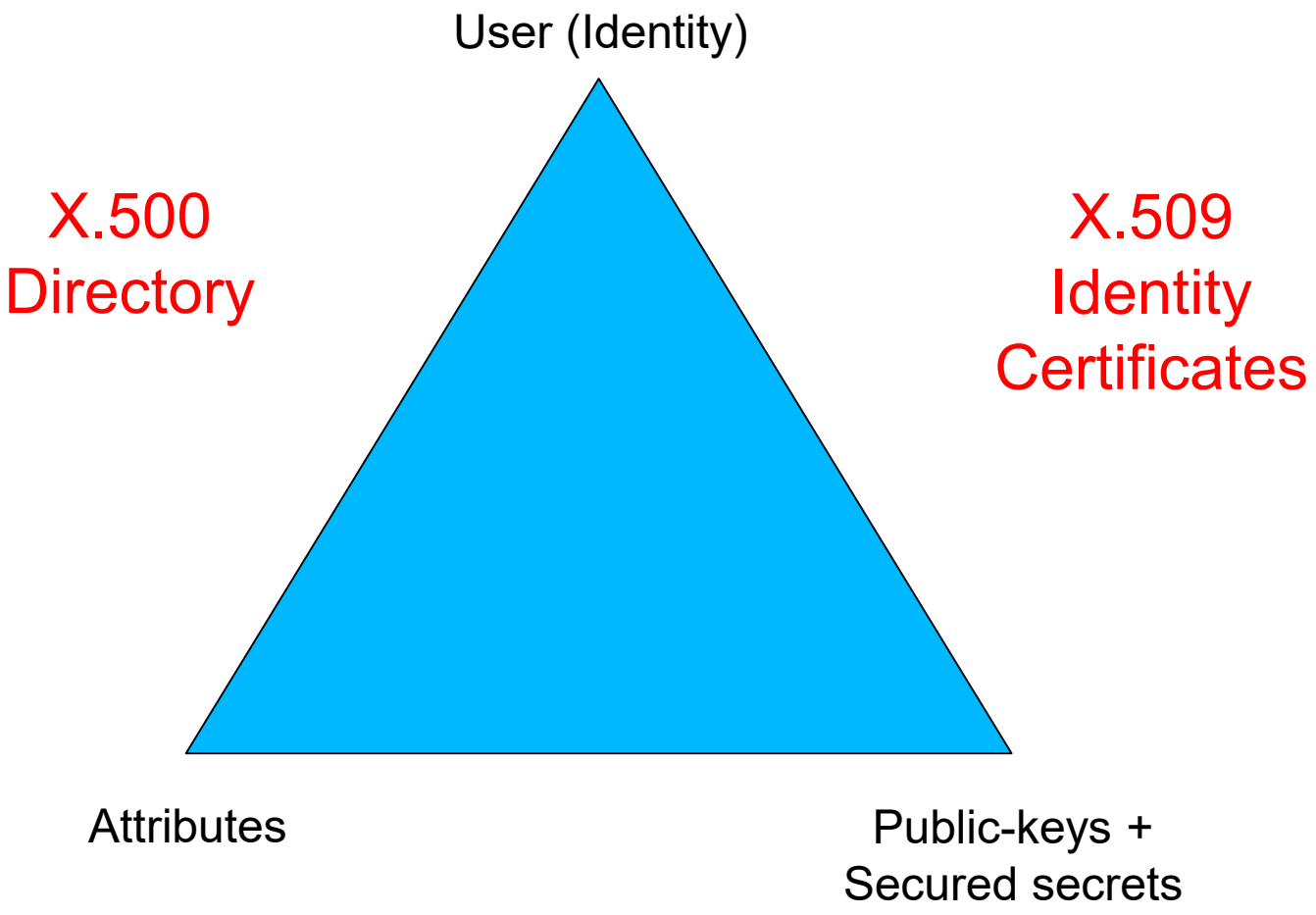
ABAC Status


Amount of Publications
Standard Adopted
Proposed Standard
RBAC96 paper
1990?
2017
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

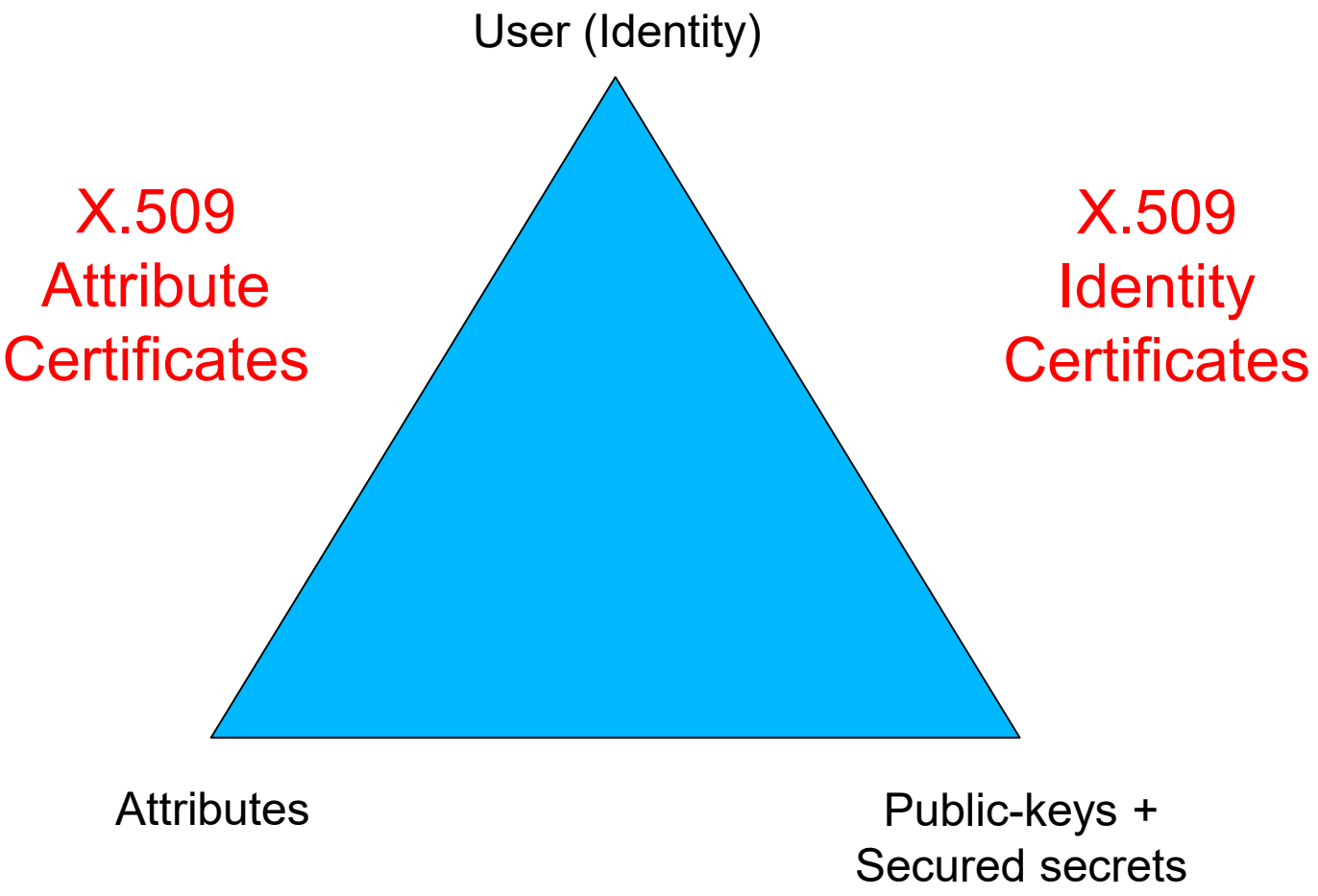


ABAC is not New



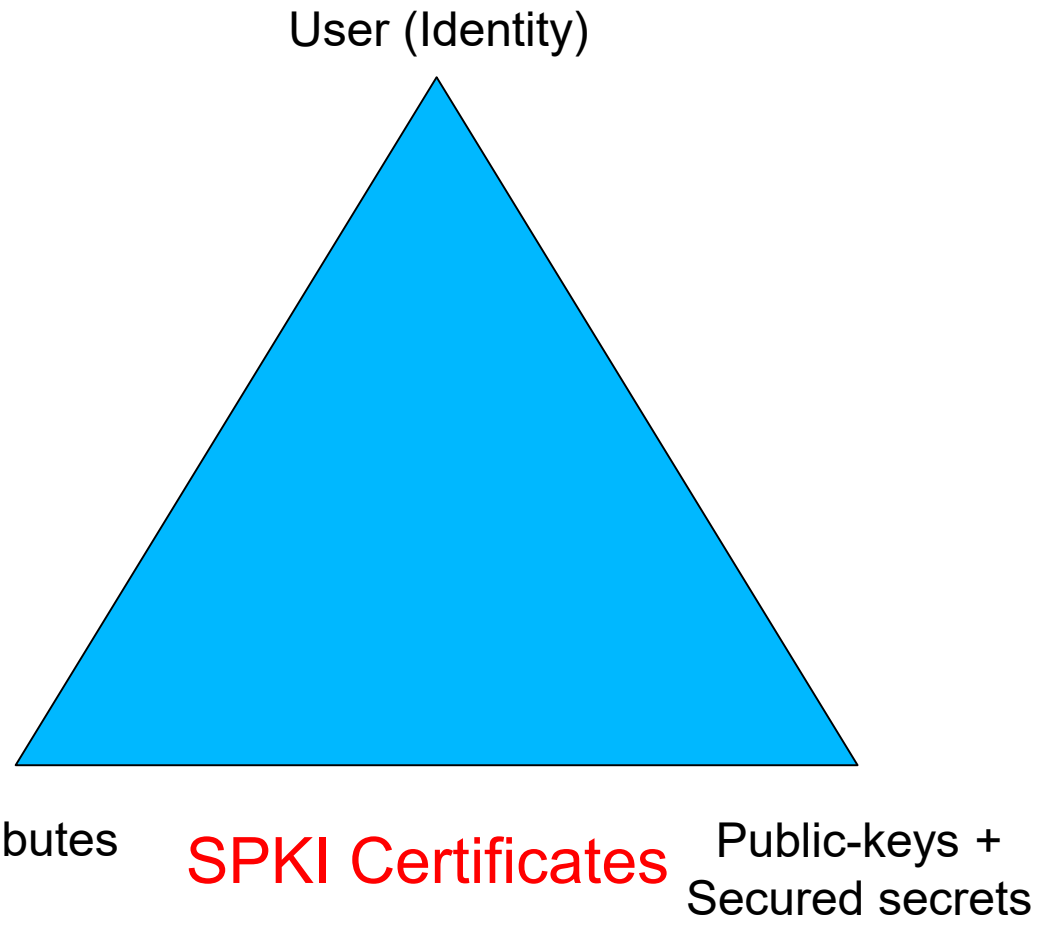
Pre Internet, early 1990s

ABAC is not New



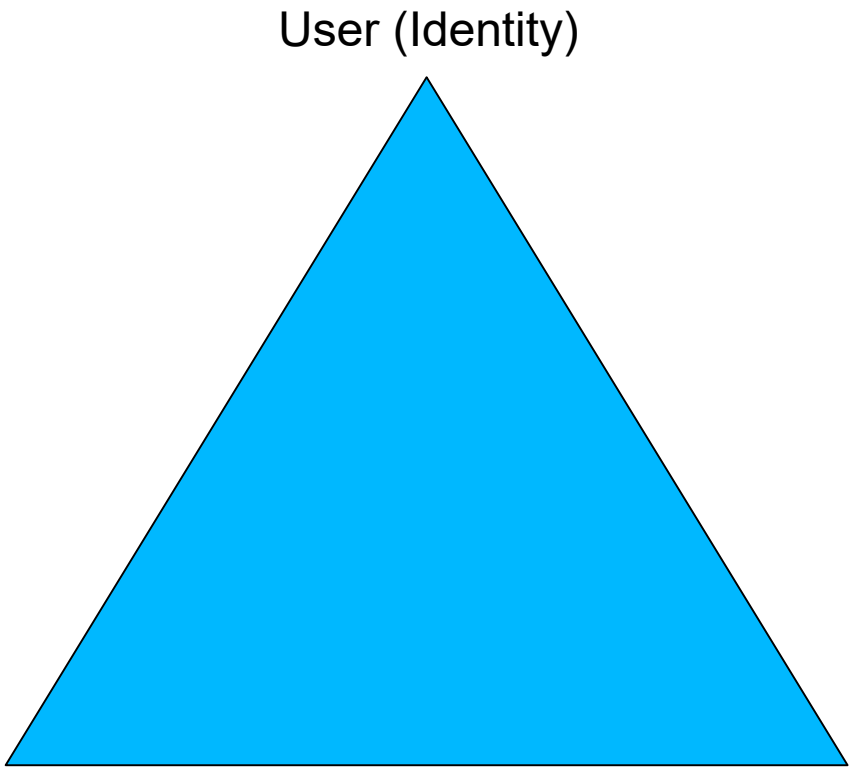
Post Internet, late 1990s

ABAC is not New



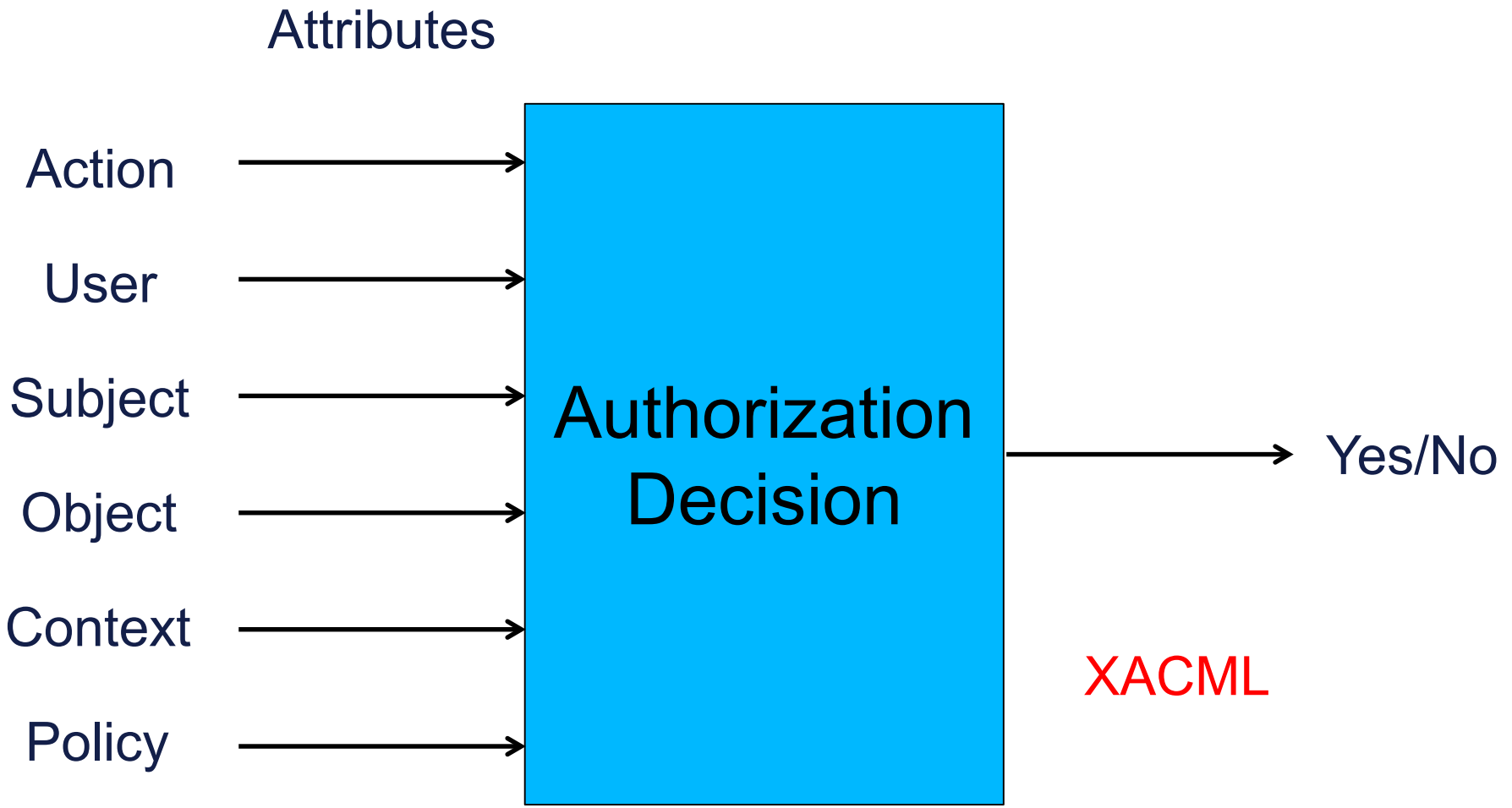
Post Internet, late 1990s

ABAC is not New



Mature Internet, 2000s

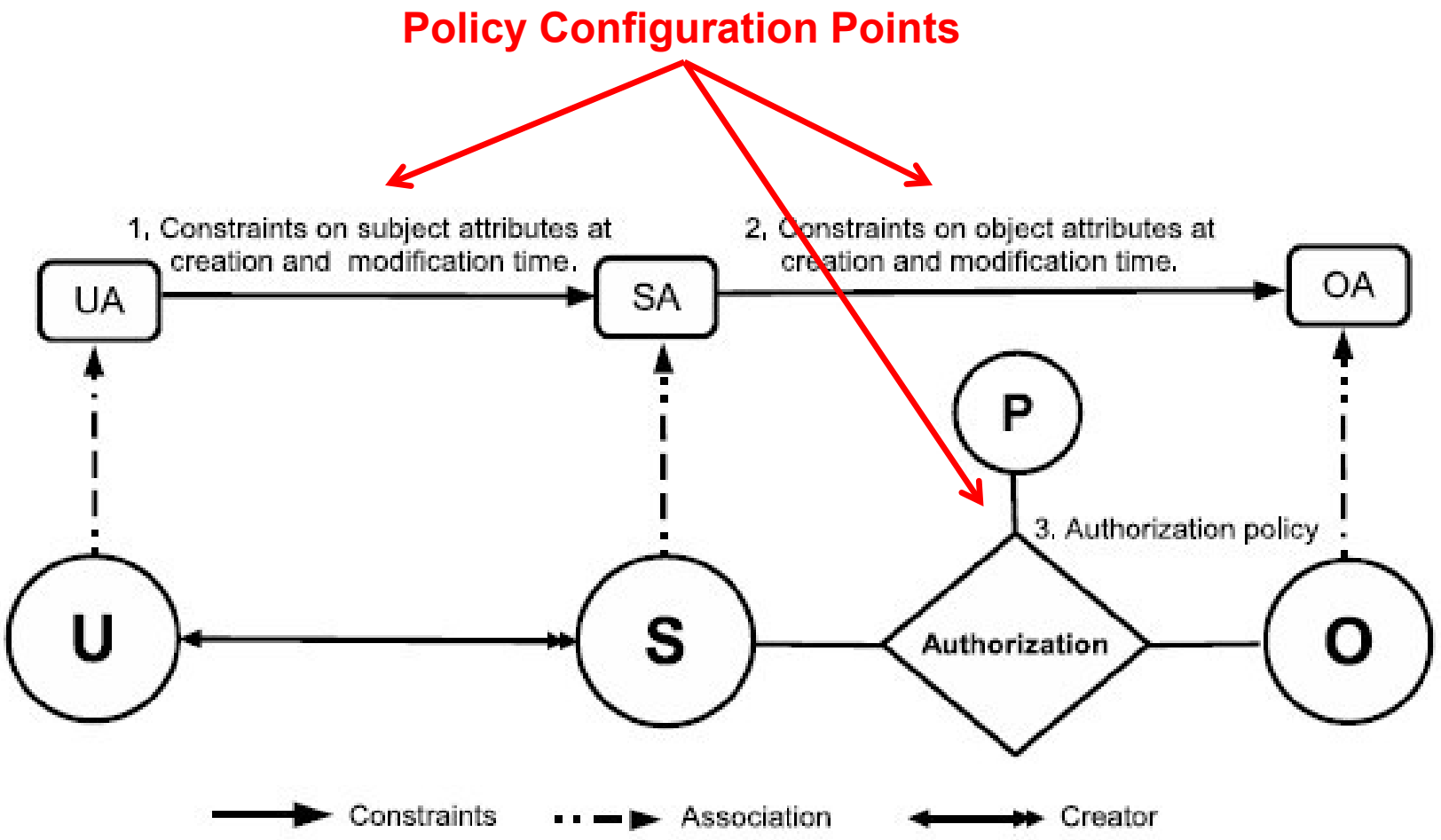
ABAC is not New



Mature Internet, 2000s

ABACα and ABACβ Models

ABACα Model Structure



Just sufficient mechanism to do simple forms of DAC, MAC, RBAC

ABACα Authorization Policy

- DAC

$$Authorization_{read}(s,o) \equiv SubCreator(s) \in reader(o)$$
$$Authorization_{write}(s,o) \equiv SubCreator(s) \in writer(o)$$

- MAC

$$Authorization_{read}(s,o) \equiv sensitivity(o) \leq sclearance(s)$$

Liberal star : $Aauthorization_{write}(s,o) \equiv sclearance(s) \leq sensitivity(o)$

Strict star : $Aauthorization_{write}(s,o) \equiv sensitivity(o) = sclearance(s)$

- RBAC0

$$Authorization_{read}(s,o) \equiv \exists r \in srole(s).r \in rrole(o)$$

- RBAC1

$$Authorization_{read}(s,o) \equiv \exists r1 \in srole(s).\exists r2 \in rrole(o).r2 \leq r1$$

ABACα Subject Attribute Constraints

- MAC creation $ConstrSub(u, s, \{(sclearance, value)\}) \equiv value \leq uclearance(u)$

  modification FALSE

- RBAC0 $ConstrSub(u, s, \{srole, value\}) \equiv value \subseteq urole(u)$

- RBAC1 $ConstrSub(u, s, \{srole, value\}) \equiv \forall r1 \in value. \exists r2 \in urole(u). r1 \leq r2$

ABACα Object Attribute Constraints

- DAC Creation

$$ConstrObj(s,o,\{(reader,val1),(writer,val2),(createdby,val3)\}) \equiv val3 = SubCreator(s)$$

  Modification

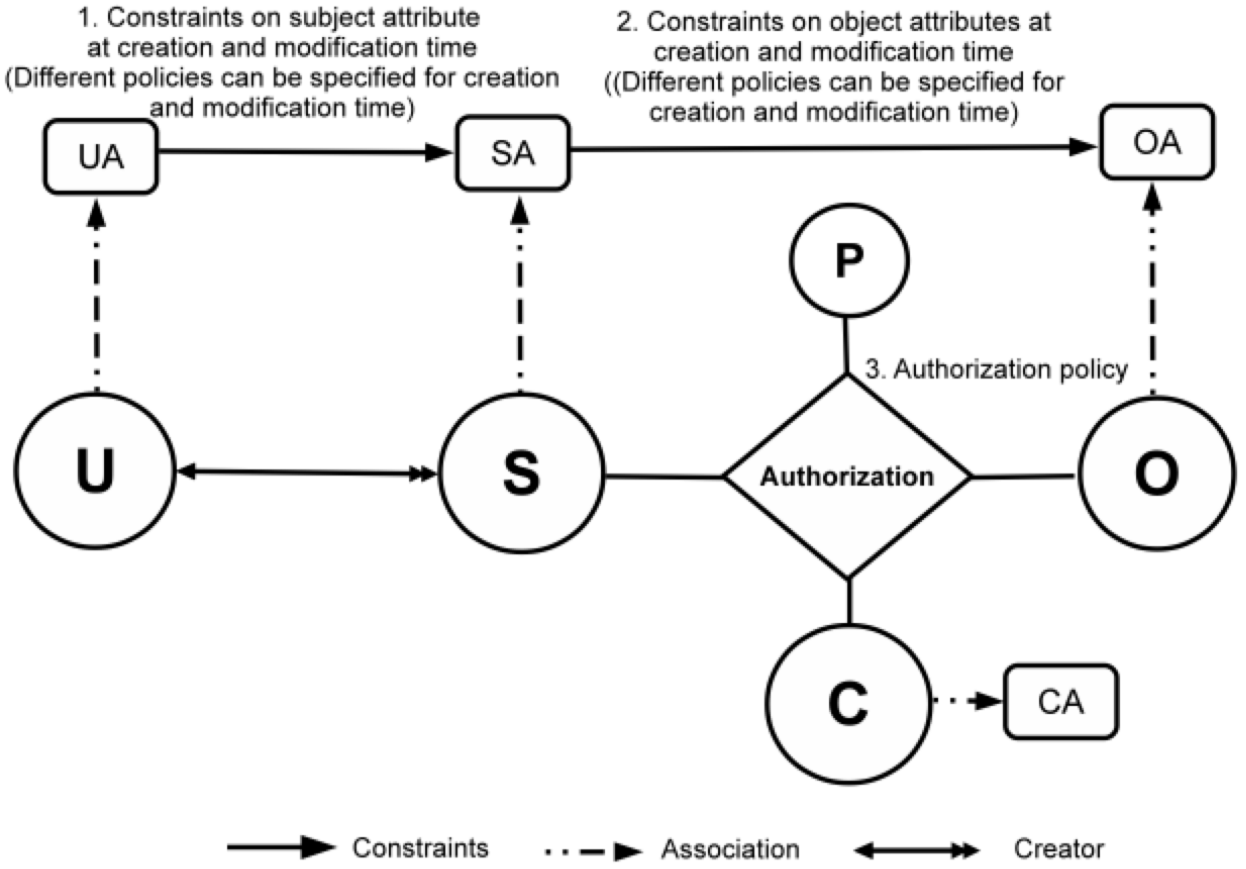
$$ConstrObj(s,o,\{(reader,val1),(writer,val2),(createdby,val3)\}) \equiv createdby(o) = SubCreator(s)$$

- MAC Creation

$$ConstrObj(s,o,\{sensitivity,value\}) \equiv sclearance(s) \leq value$$

  Modification FALSE

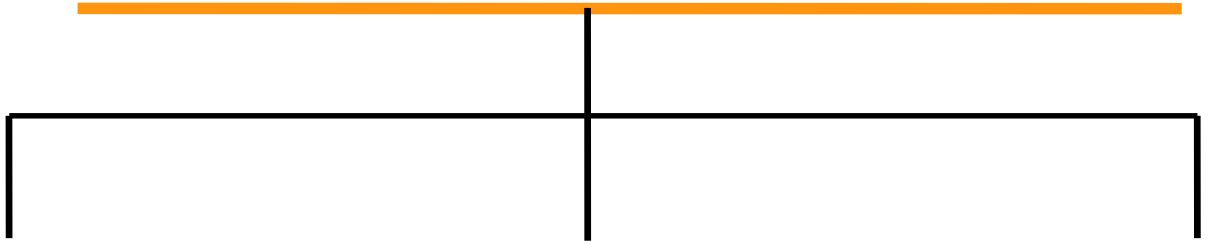
ABAC$_\beta$ Model



Can be configured to do many but not all RBAC extensions

Roles and Attributes

Roles and Attributes



Attribute-Centric

Role is just another attribute. Nothing special about it.

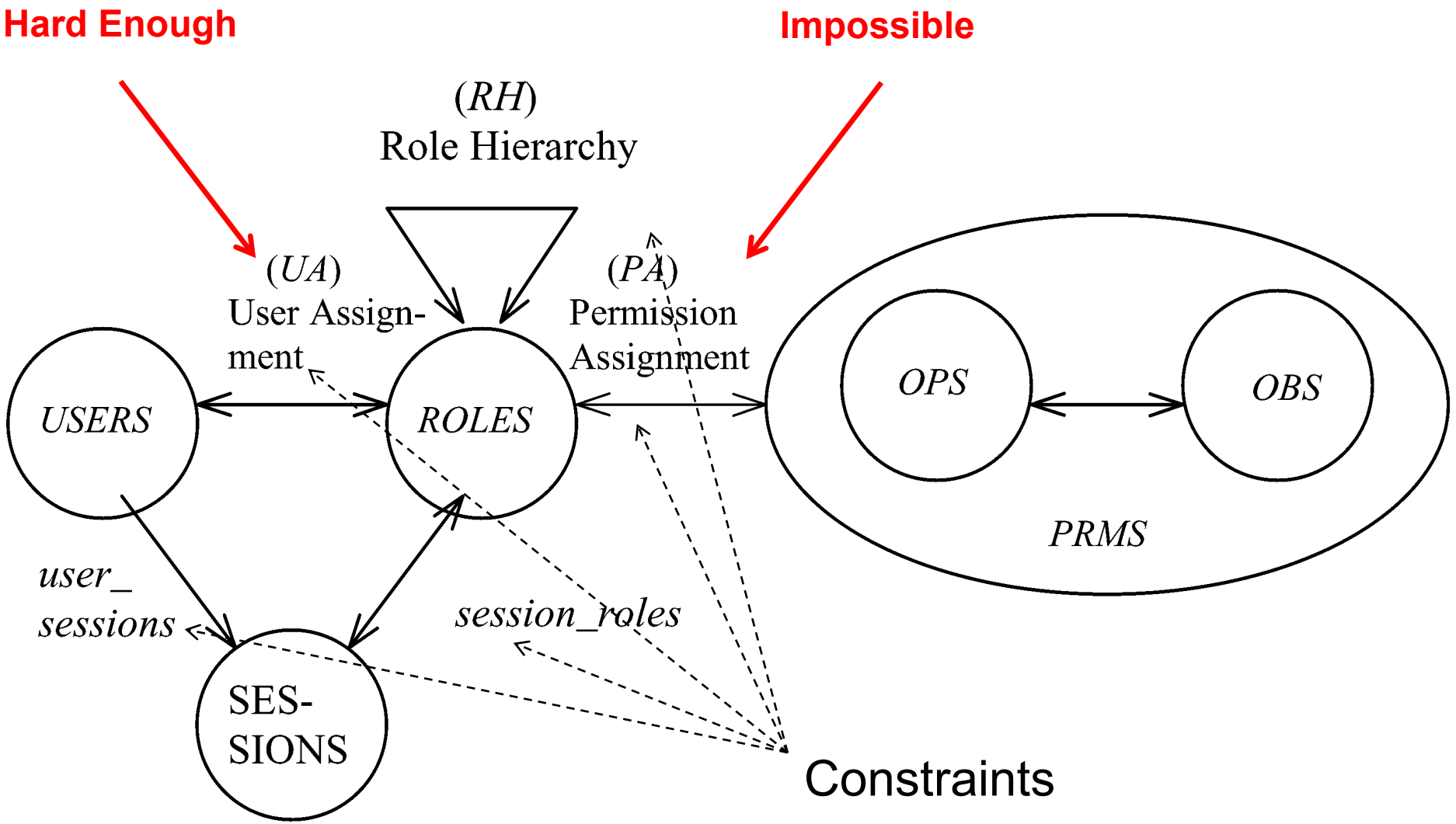
Dynamic Roles

Compute user roles from user attributes

Role-Centric

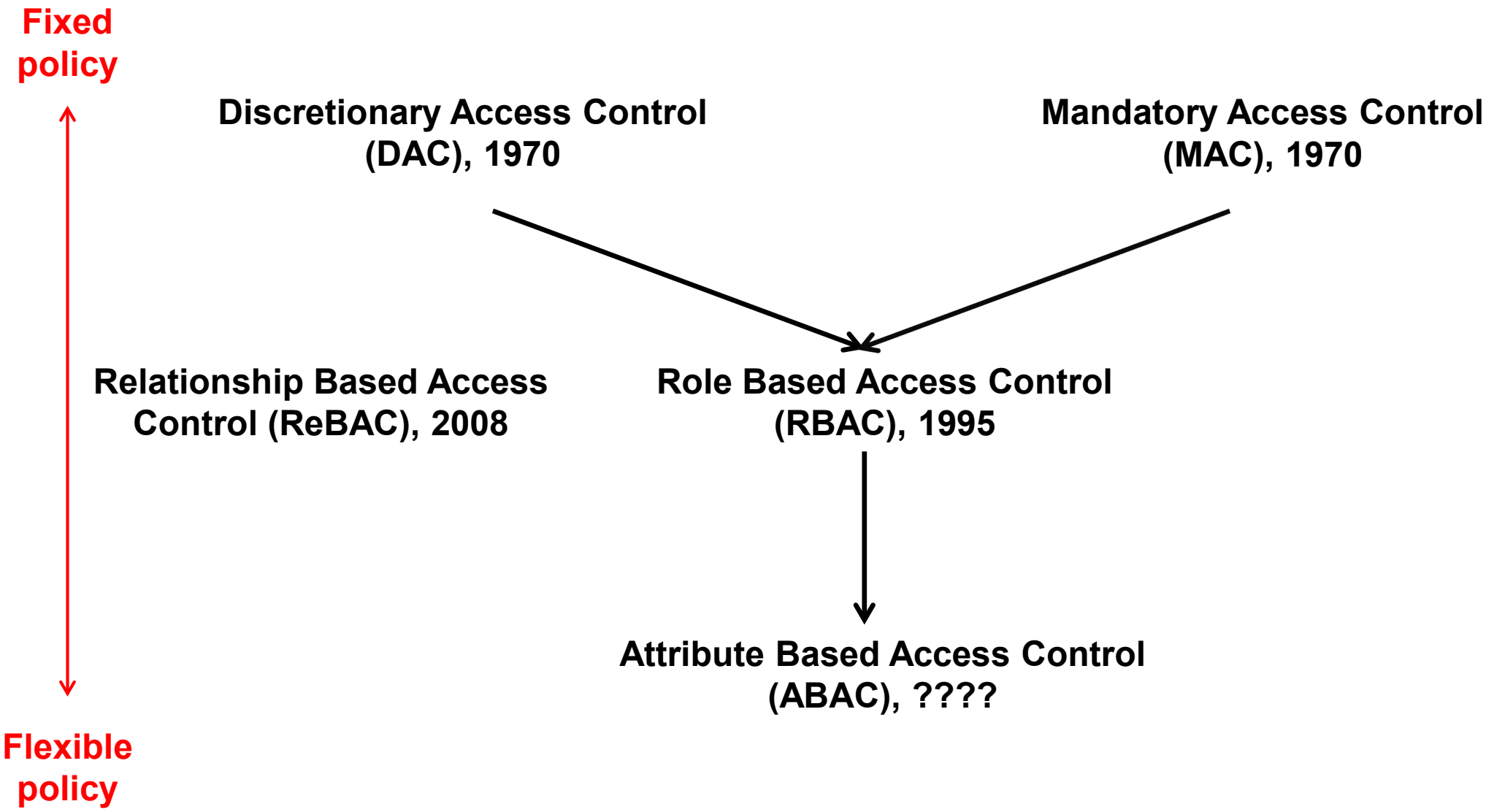
Attributes constrain permissions of roles for each user

User-Role Assignment Problem

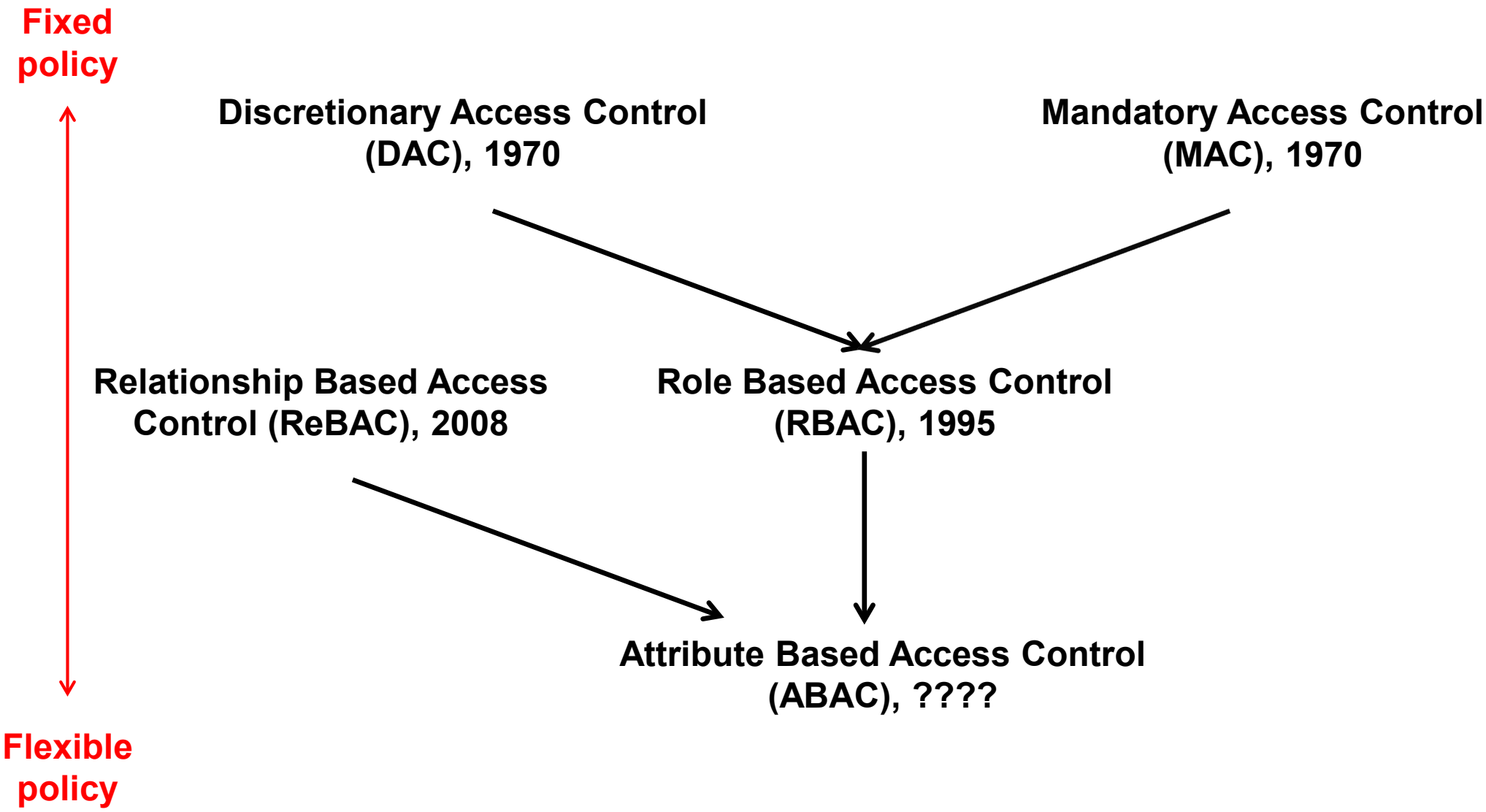


Beyond Attributes

Access Control

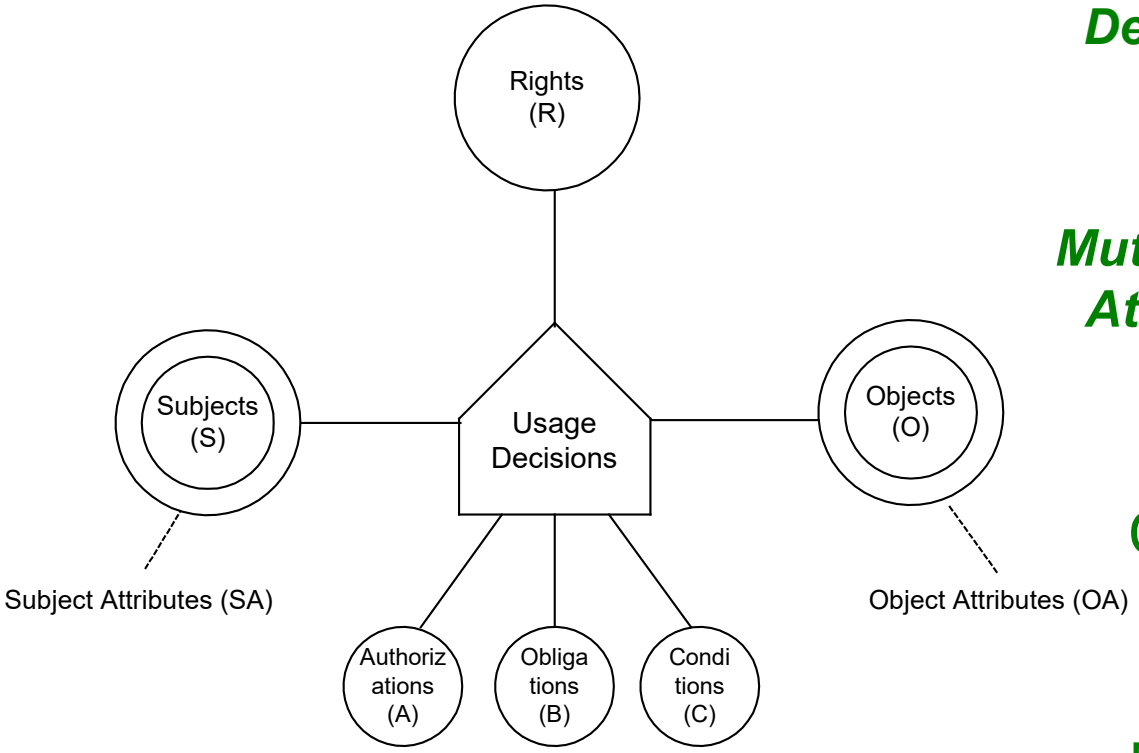


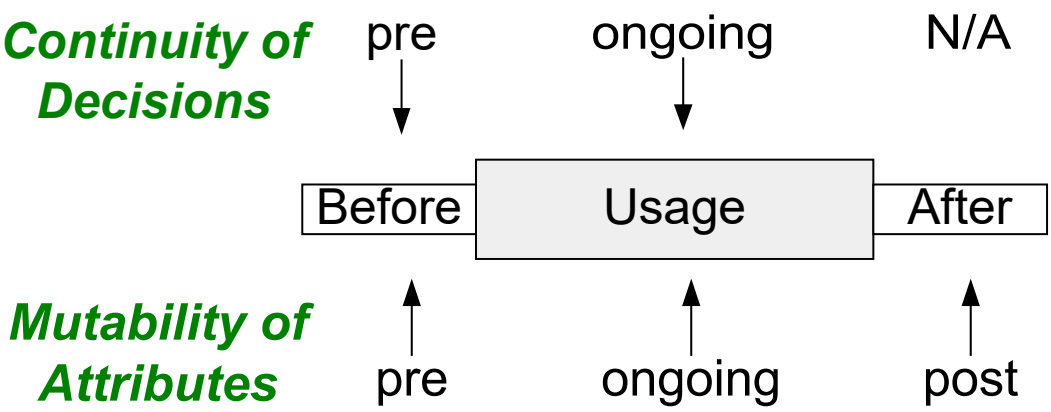
Access Control



Usage Control (UCON) Model: Attributes on Steroids

$UCON_{ABC}$ Models





Continuity

Decision can be made during usage for continuous enforcement

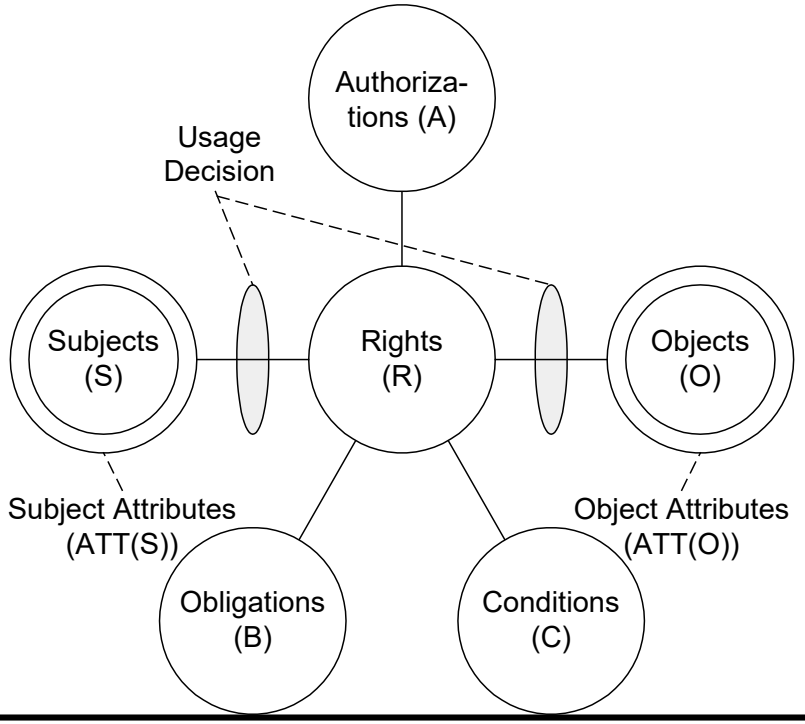
Mutability

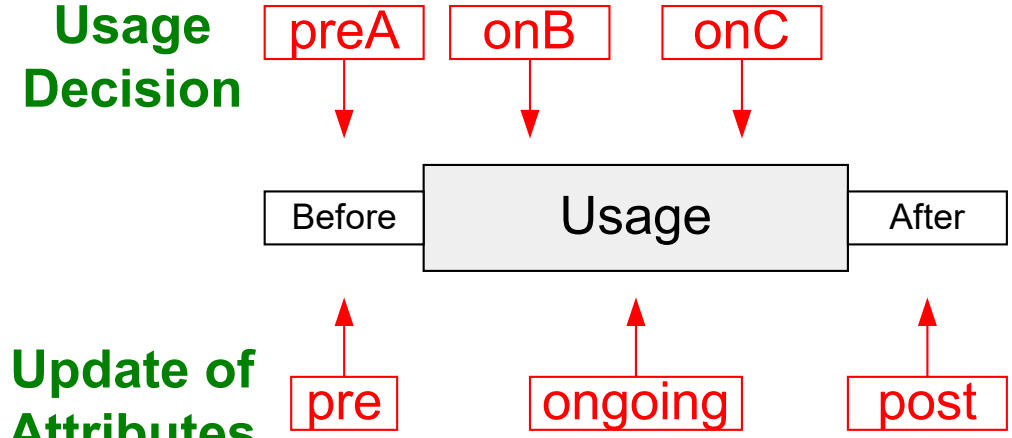
Attributes can be updated as side-effects of subjects' actions

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 every 30 minutes (ongoing-obligation with ongoing-updates)
- Business Hours (pre-/ongoing-condition)

UCON$_{ABC}$





- Free ISP
  - Membership is required (pre-authorization)
  - Have to click Ad periodically while connected (on-obligation, on-update)
  - Free member: no evening connection (on-condition), no more than 50 connections (pre-update) or 100 hours usage per month (post-updates)