

Attribute-Based Access Control (ABAC)

Prof. Ravi Sandhu
Executive Director and Endowed Chair

Lecture 10

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

**Fixed
policy**



**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control
(MAC), 1970**

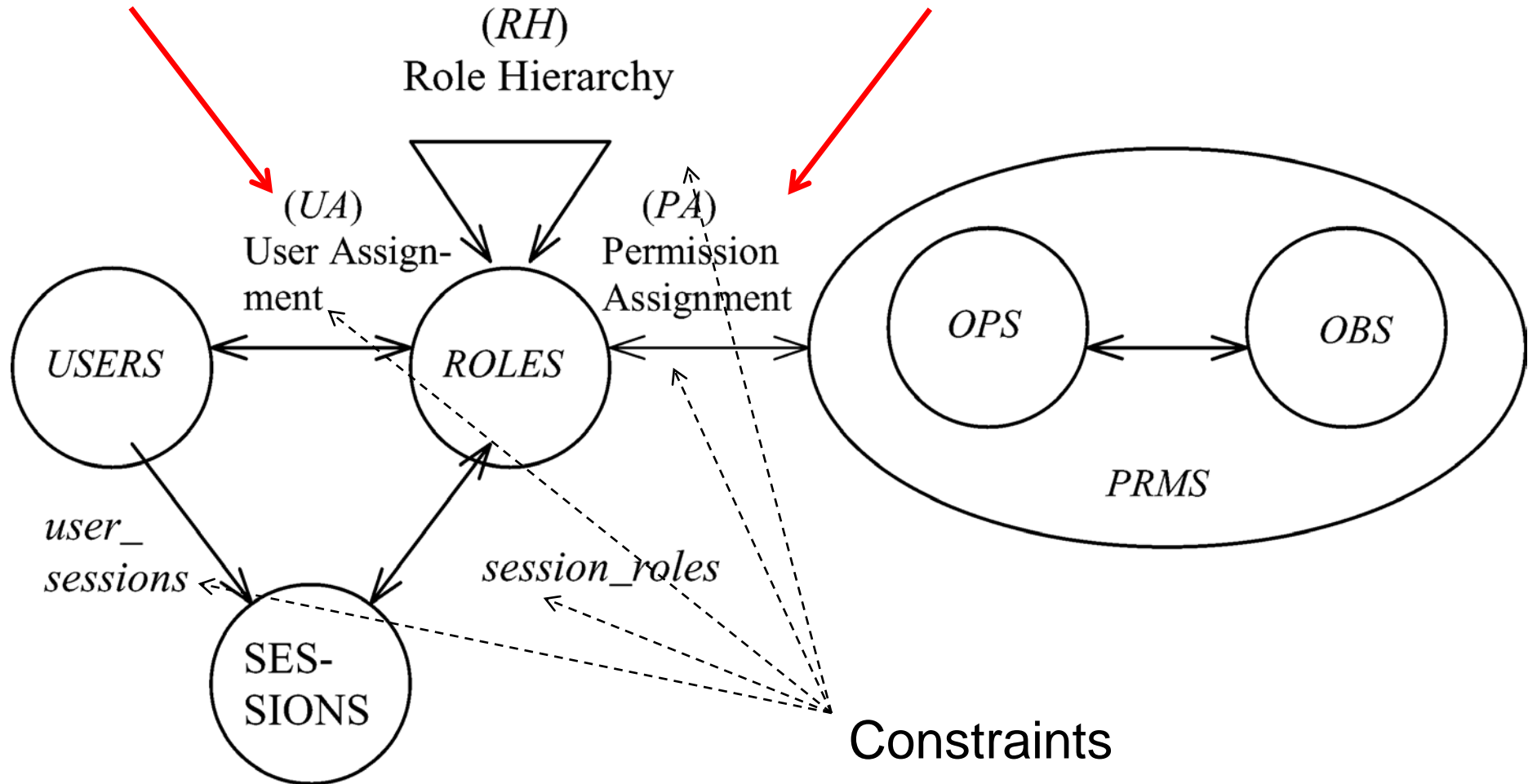
**Role Based Access Control
(RBAC), 1995**

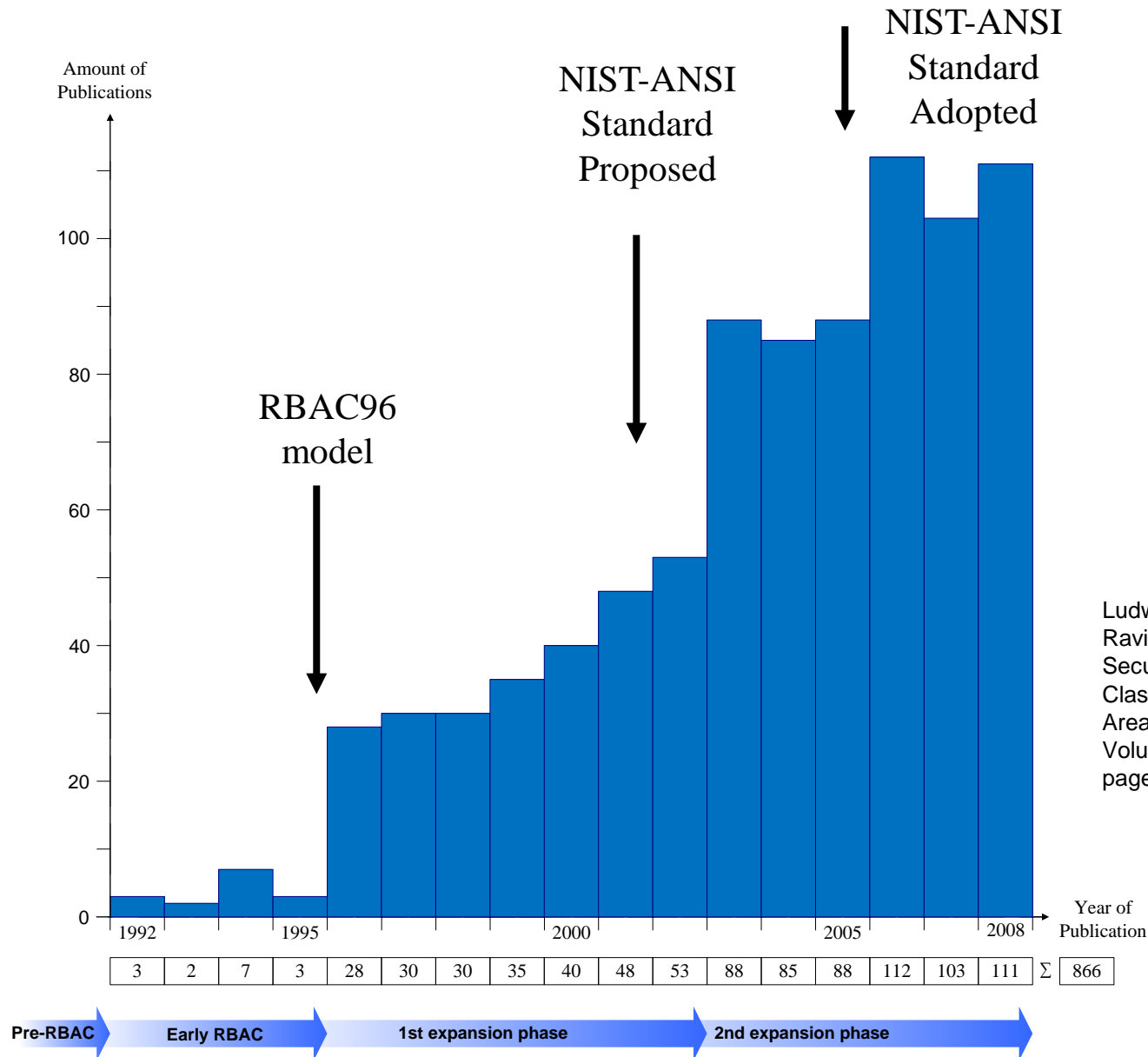
**Attribute Based Access Control
(ABAC), ????**

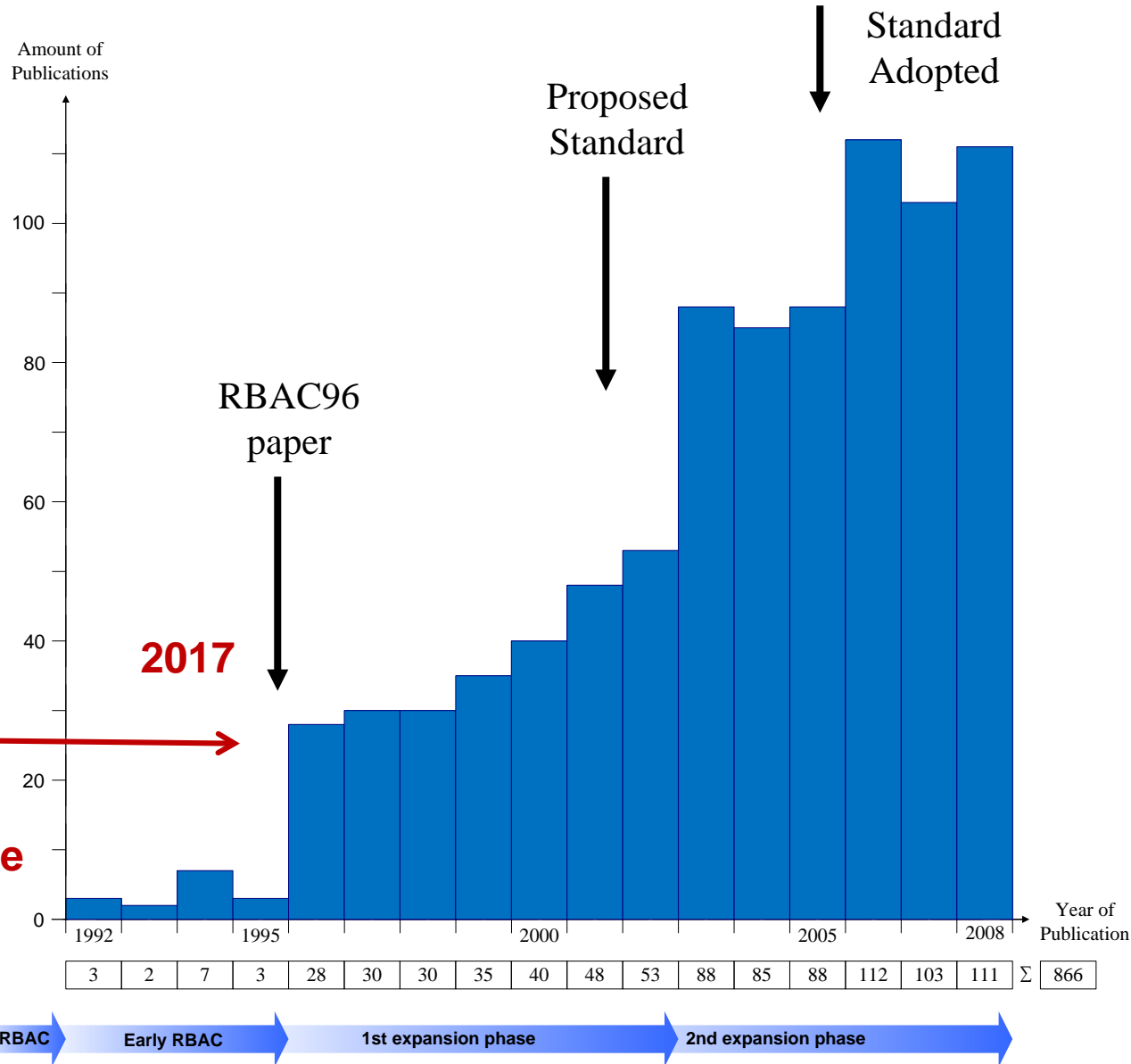
**Flexible
policy**

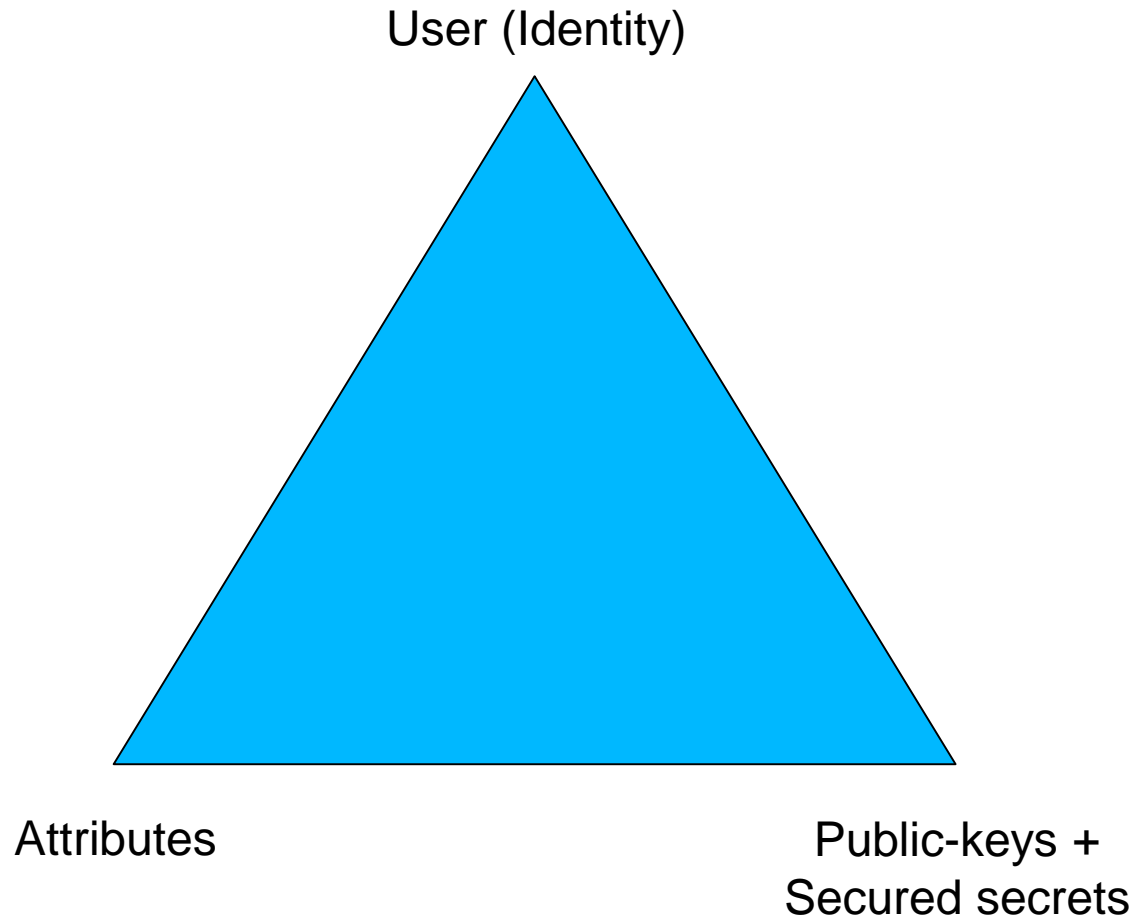
Hard Enough

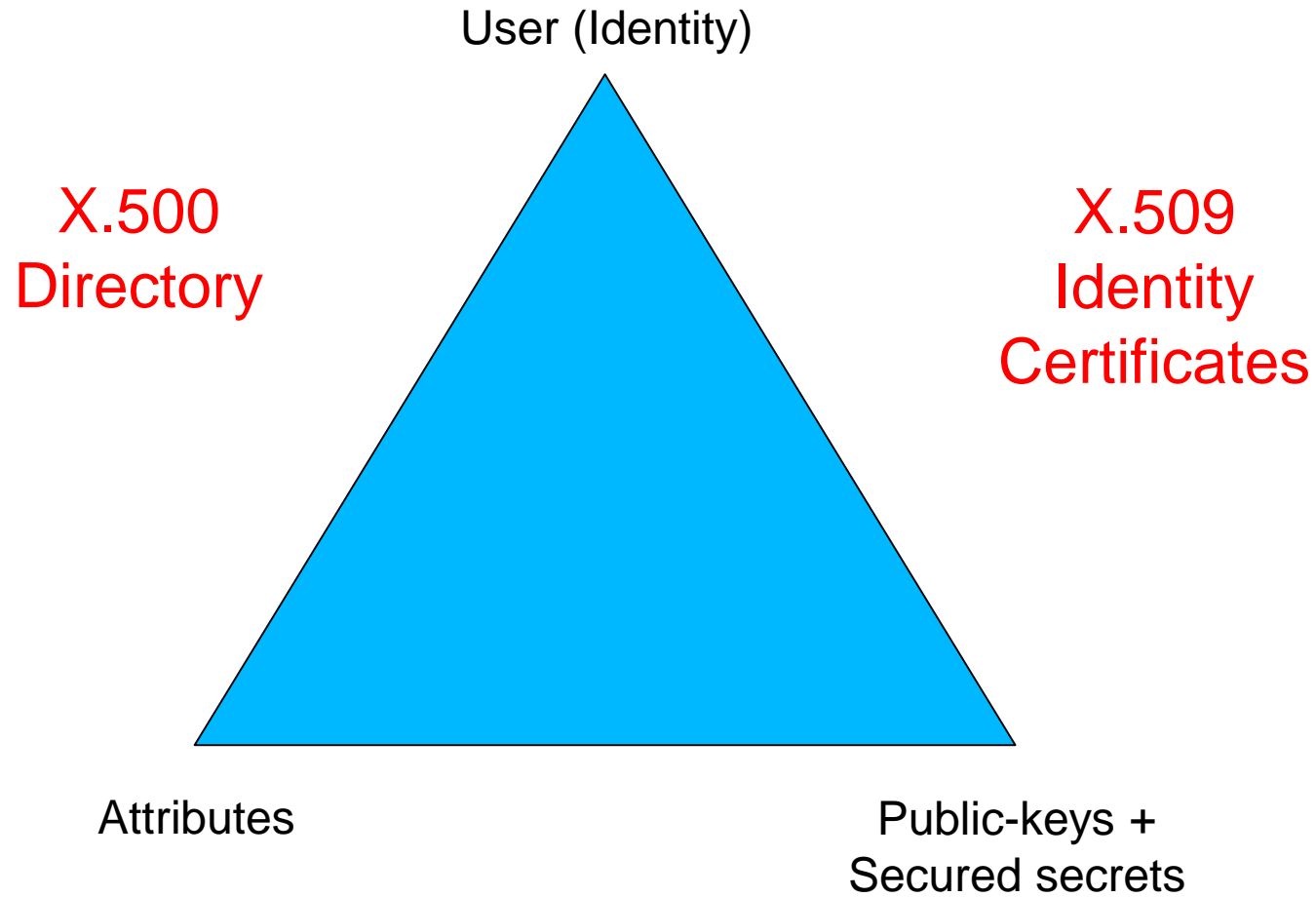
Impossible



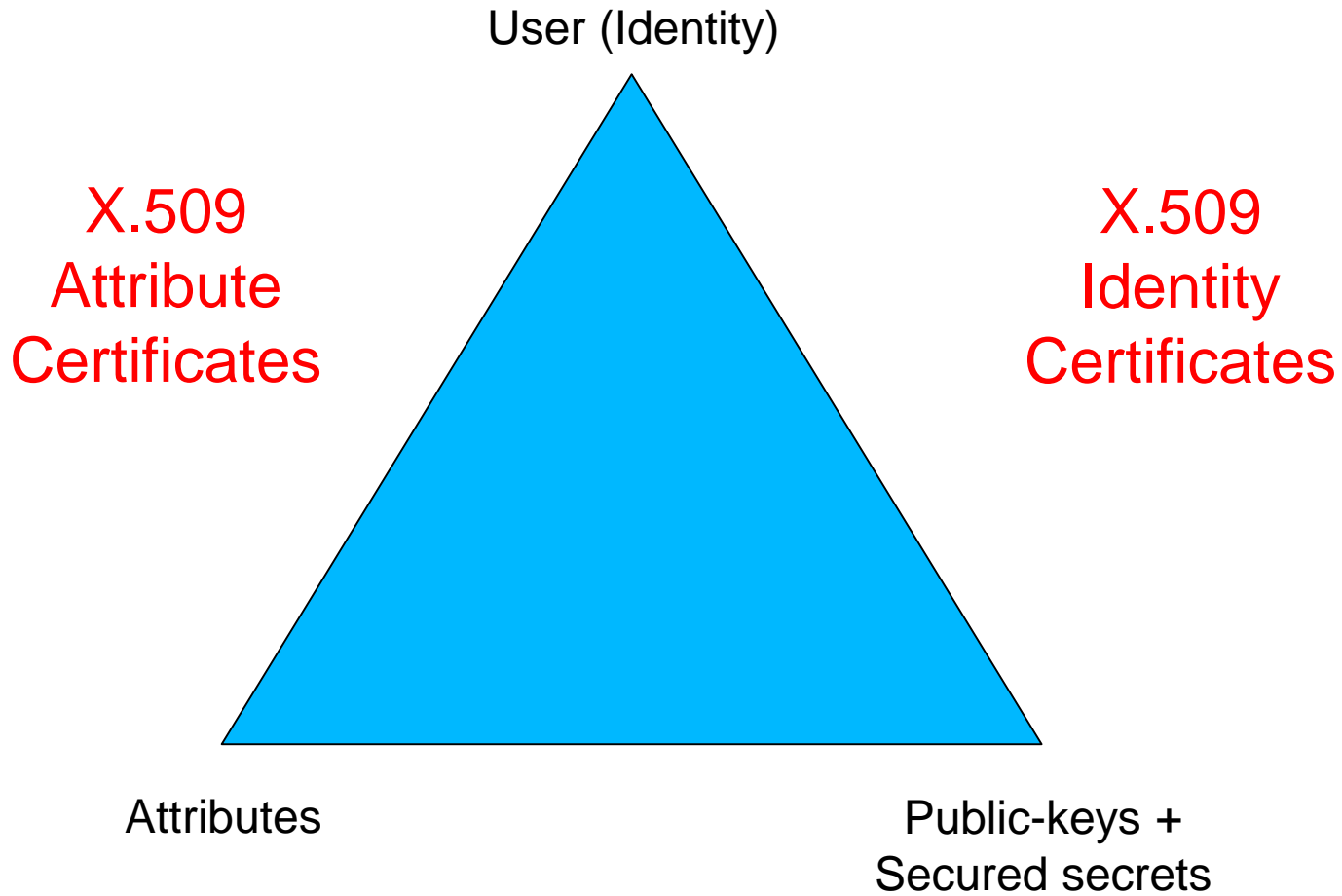




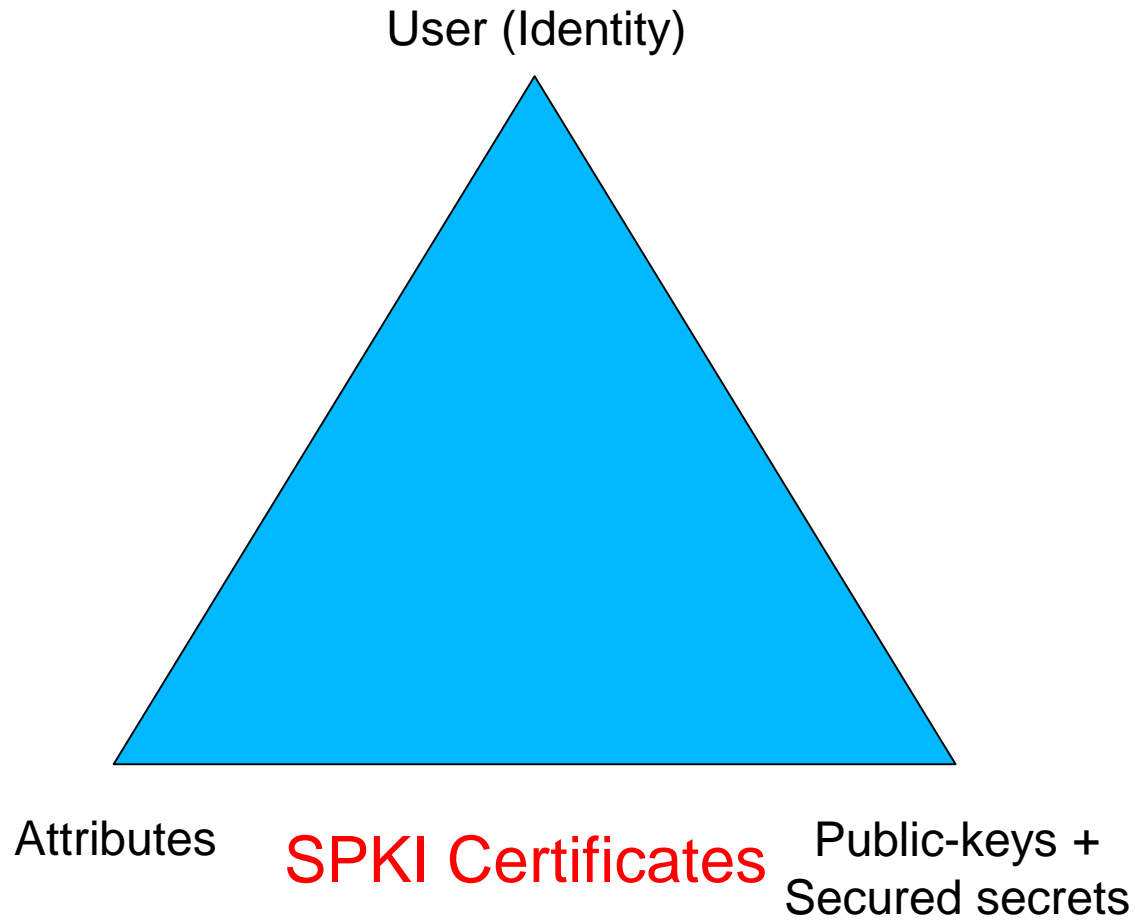




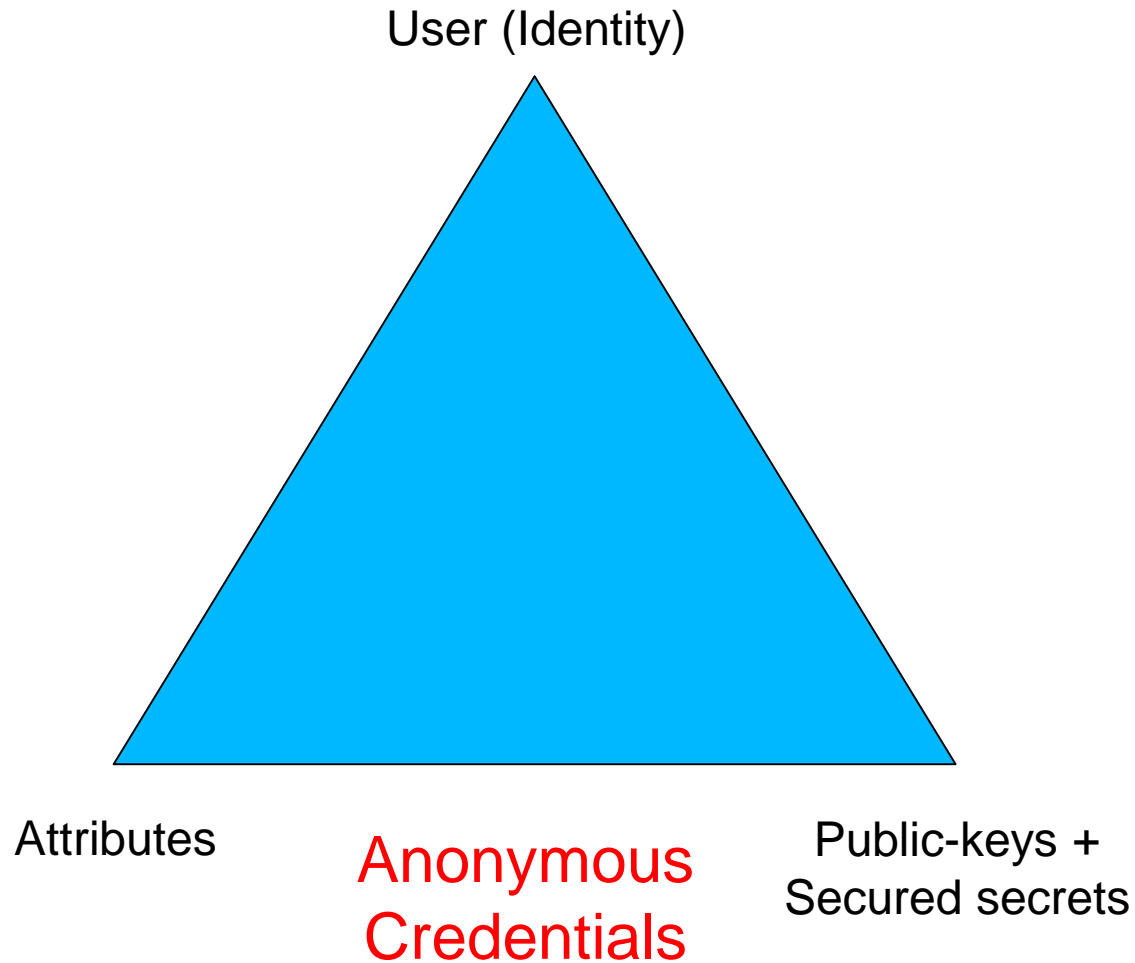
Pre Internet, early 1990s



Post Internet, late 1990s

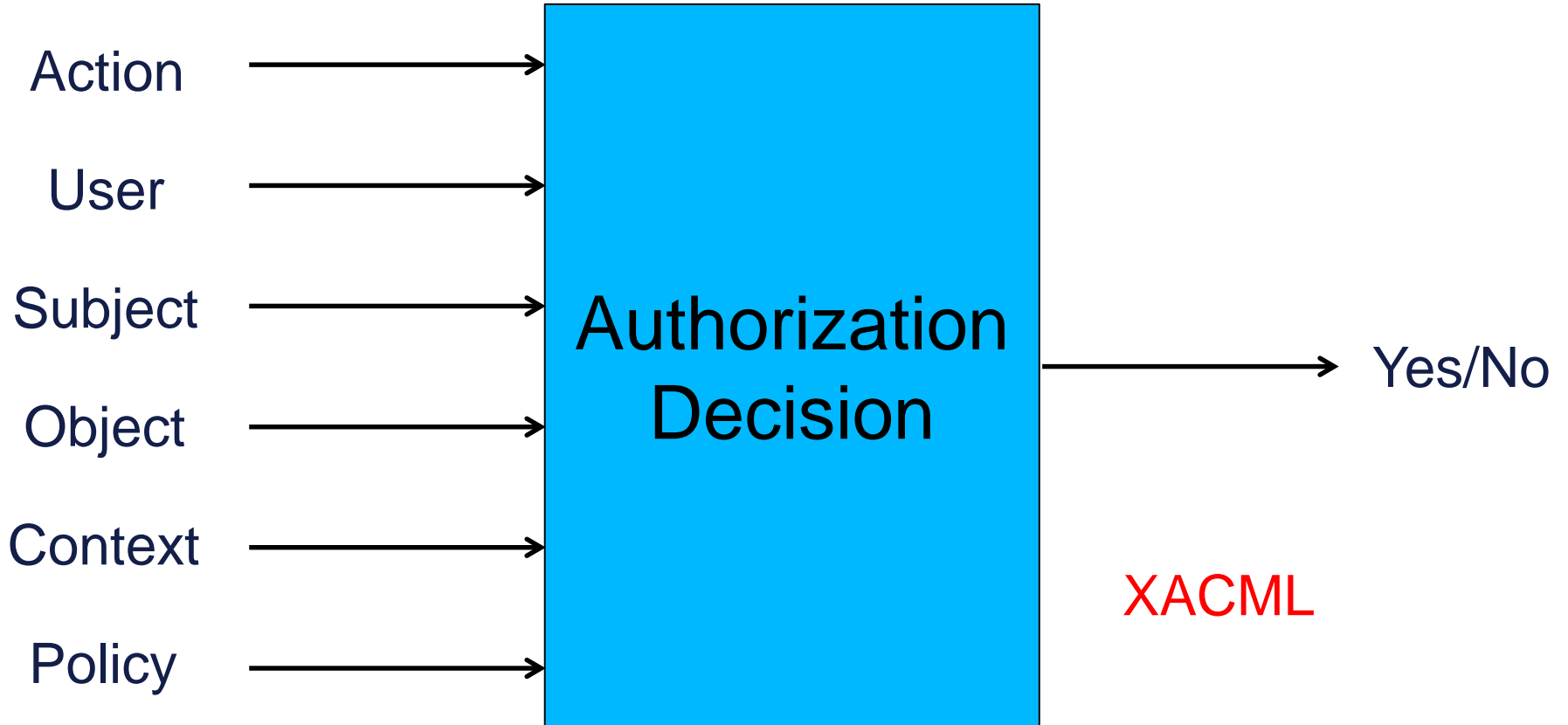


Post Internet, late 1990s



Mature Internet, 2000s

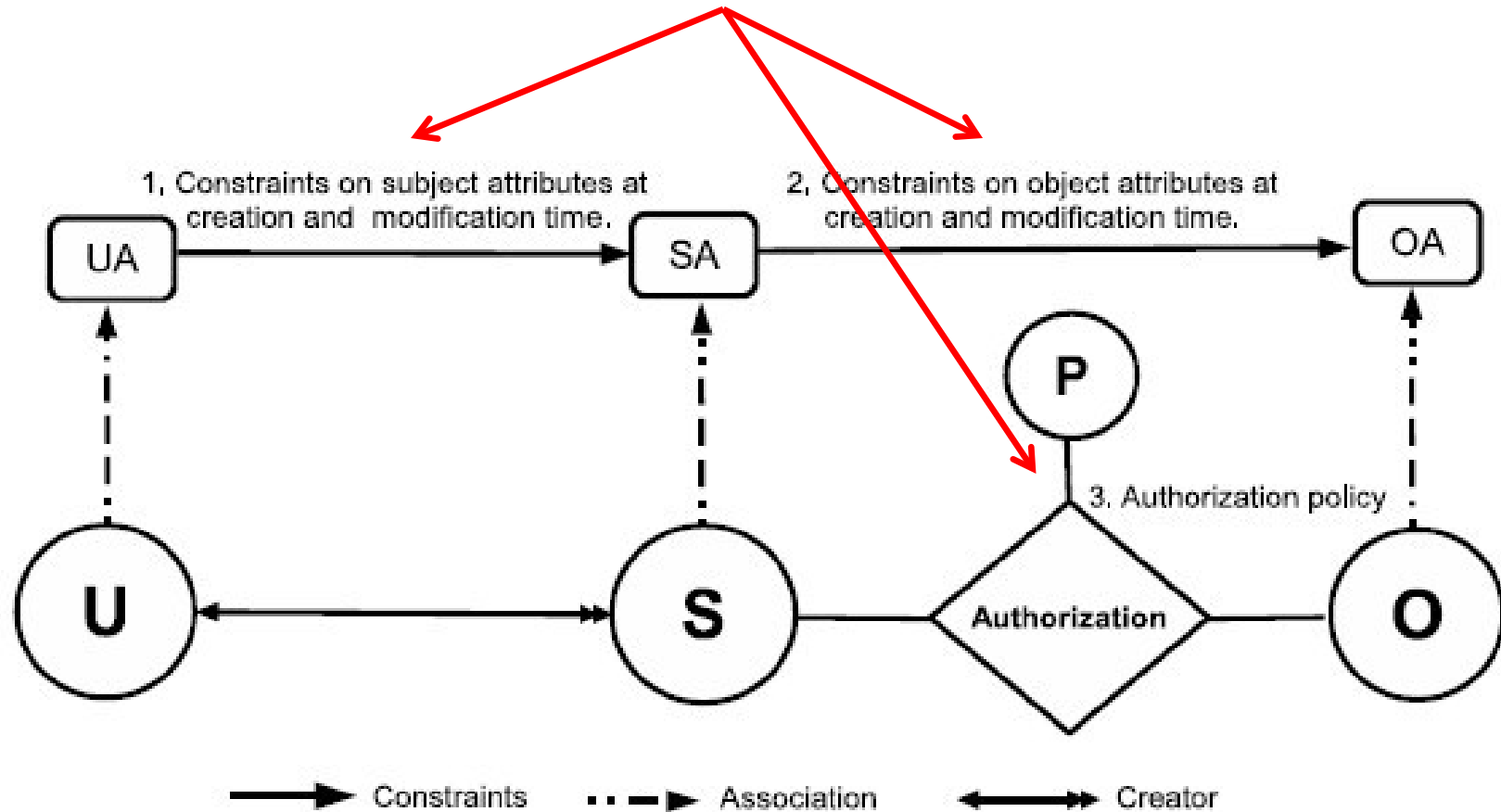
Attributes



Mature Internet, 2000s

ABAC α and ABAC β Models

Policy Configuration Points



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

❖ 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

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

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

❖ DAC Creation

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

Modification

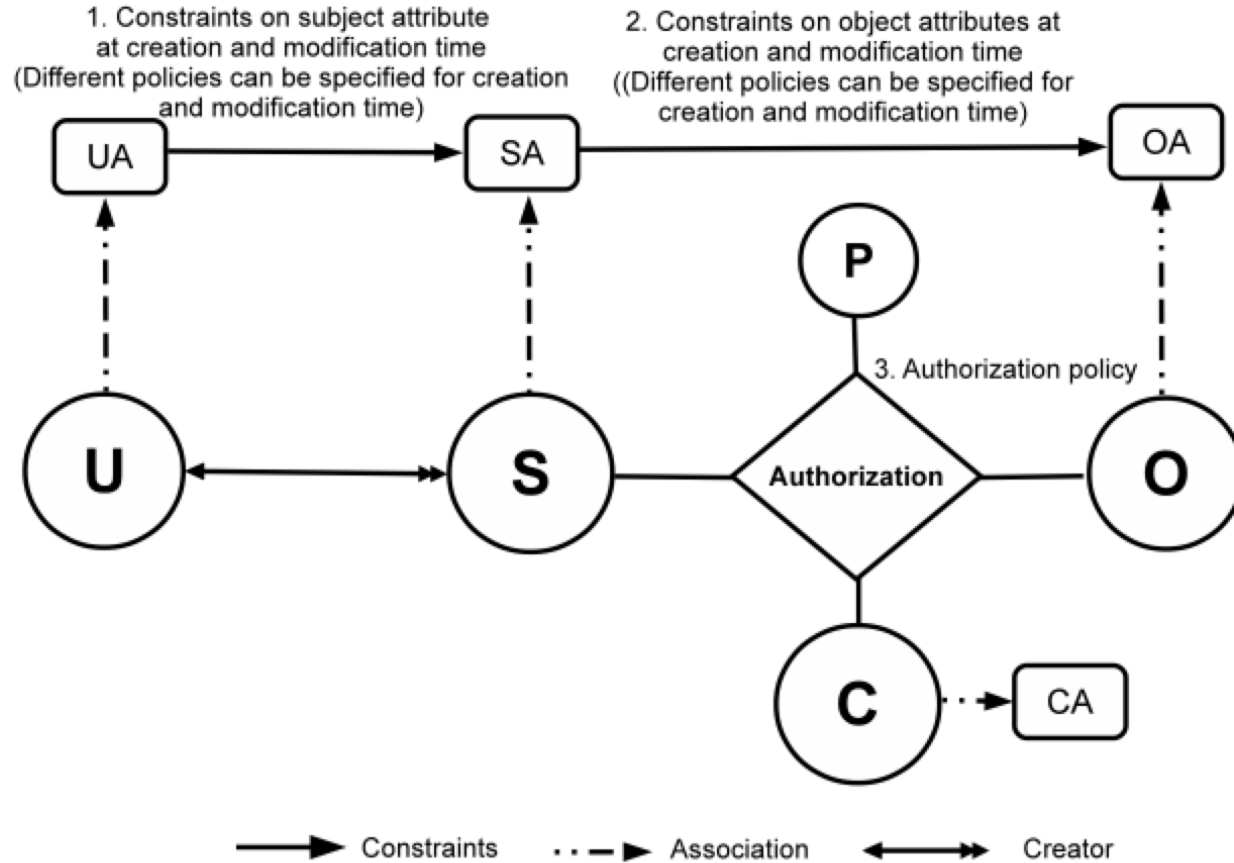
$ConstrObj(s, o, \{(reader, val1), (writer, val2), (createdby, val3)\}) \equiv createdby(o) = SubCreator(s)$

❖ MAC Creation

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

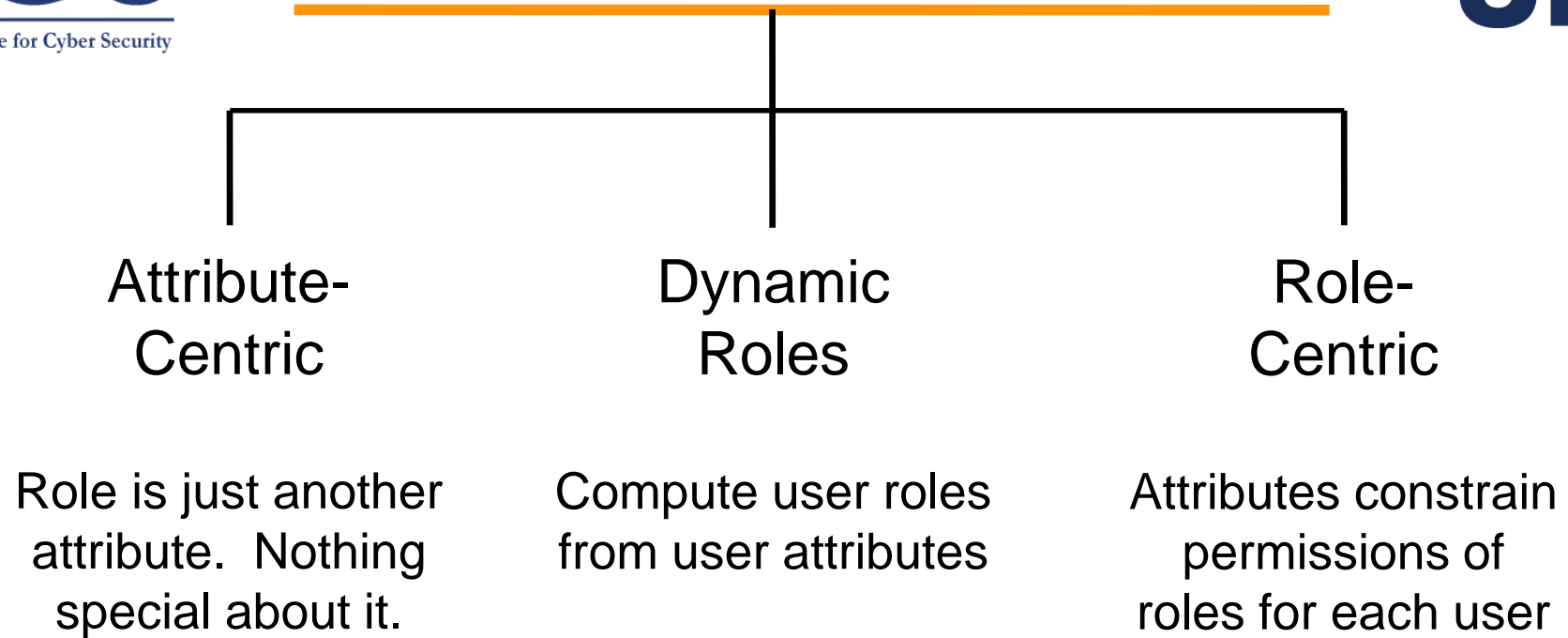
Modification

FALSE



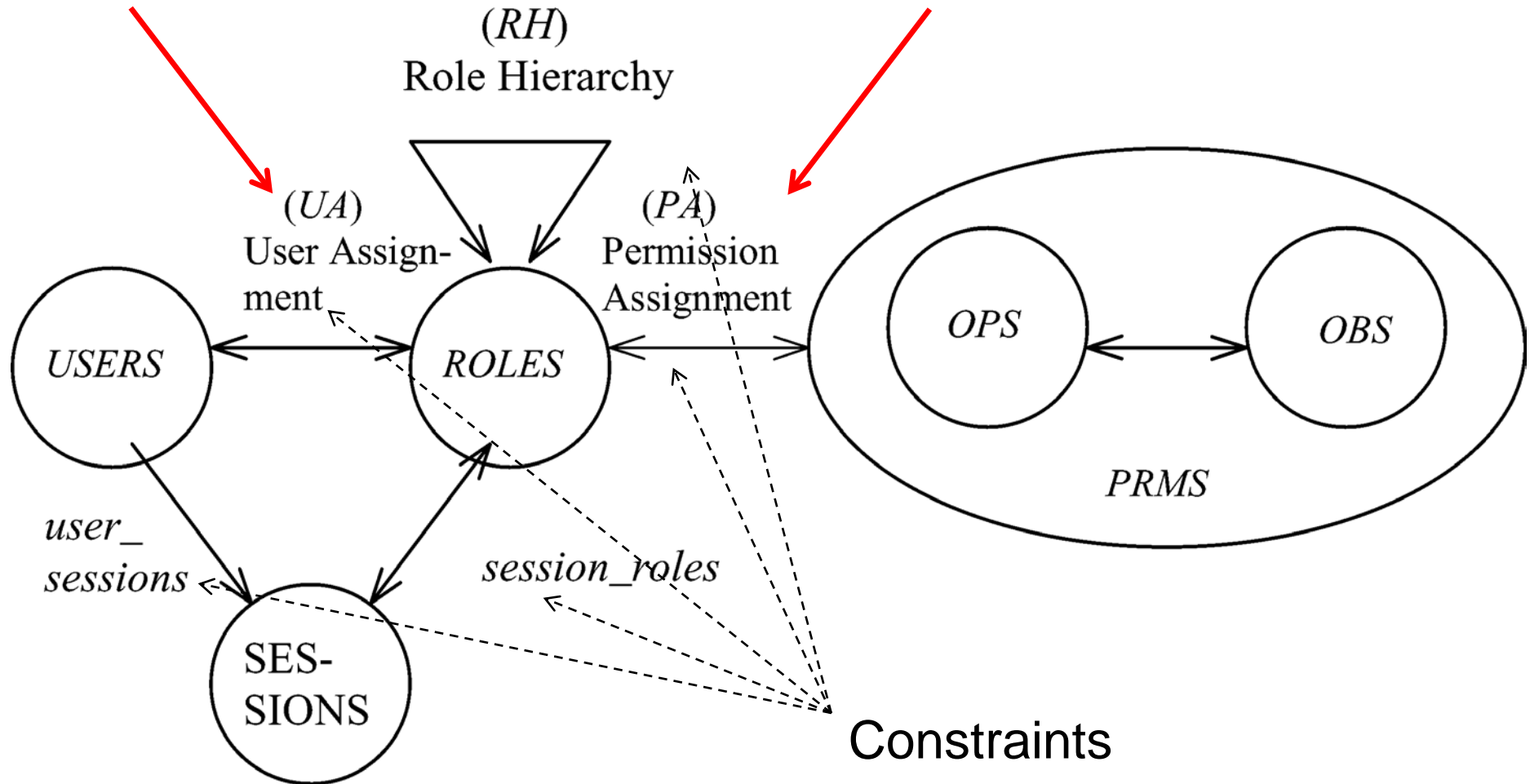
Can be configured to do many but not all RBAC extensions

Roles and Attributes



Hard Enough

Impossible



Beyond Attributes

**Fixed
policy**



**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control
(MAC), 1970**

**Relationship Based Access
Control (ReBAC), 2008**

**Role Based Access Control
(RBAC), 1995**

**Attribute Based Access Control
(ABAC), ????**

**Flexible
policy**

**Fixed
policy**



**Discretionary Access Control
(DAC), 1970**

**Mandatory Access Control
(MAC), 1970**

**Relationship Based Access
Control (ReBAC), 2008**

**Role Based Access Control
(RBAC), 1995**

**Attribute Based Access Control
(ABAC), ????**

**Flexible
policy**