

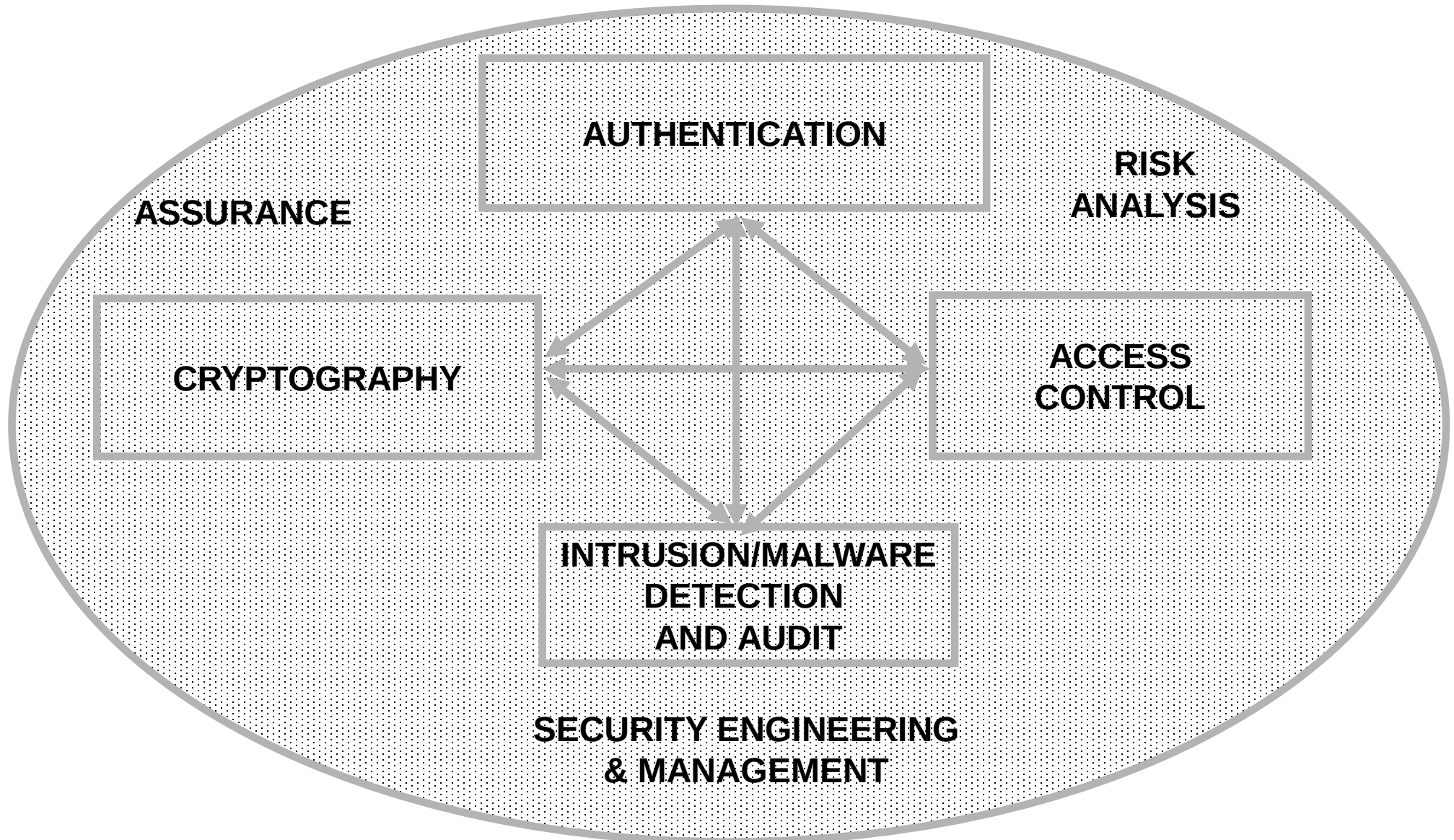
Attribute-Based Access Control Models

Prof. Ravi Sandhu

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

Colorado State University
Fort Collins
Sept. 16, 2014

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



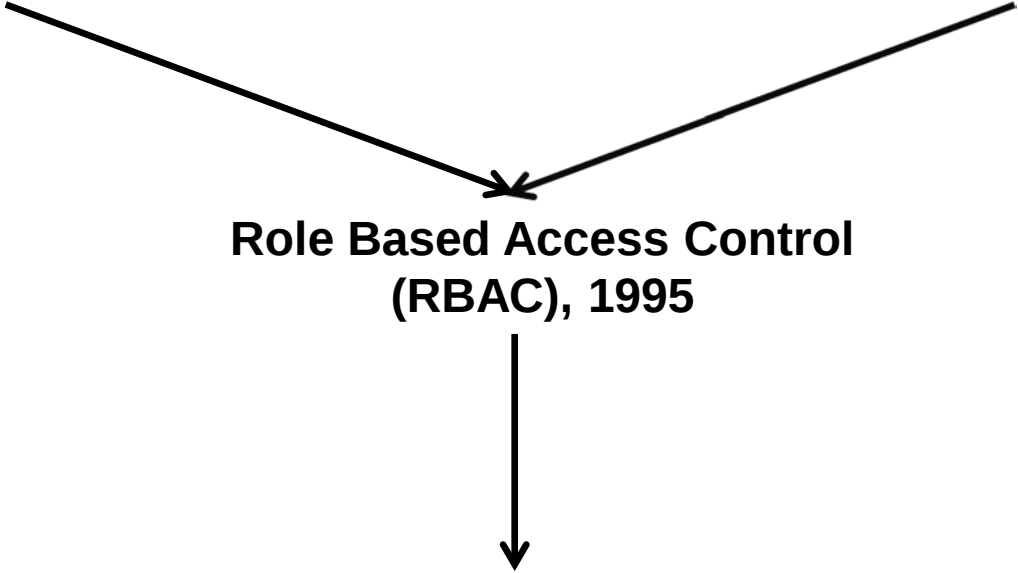
- Analog Hole
- Inference
- Covert Channels
- Side Channels
- Phishing
- Safety
- Usability
- Privacy
- Attack Asymmetry
- Compatibility
- Federation
-

- Analog Hole
- Inference
- Covert Channels
- Side Channels
- Phishing
- Safety
- Usability
- Privacy
- Attack Asymmetry
- Compatibility
- Federation
-

Can manage
Cannot eliminate

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

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



```
graph TD; DAC["Discretionary Access Control (DAC), 1970"] --> RBAC["Role Based Access Control (RBAC), 1995"]; MAC["Mandatory Access Control (MAC), 1970"] --> RBAC; RBAC --> ABAC["Attribute Based Access Control (ABAC), ????"];
```

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

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

**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**

**Human
Driven**

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

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

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

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

**Automated
Adaptive**

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

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

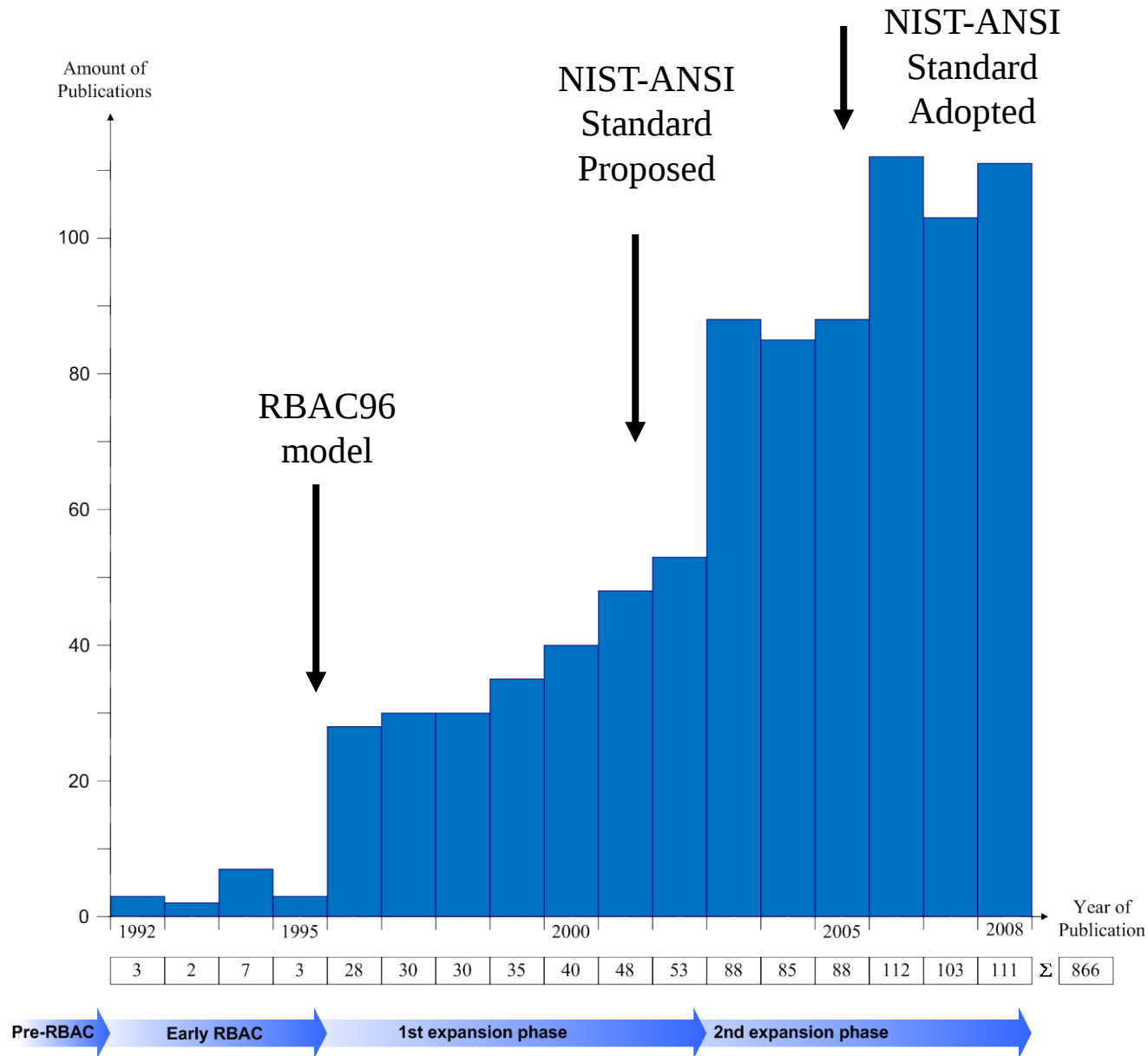
**Role Based Access Control
(RBAC), 1995**

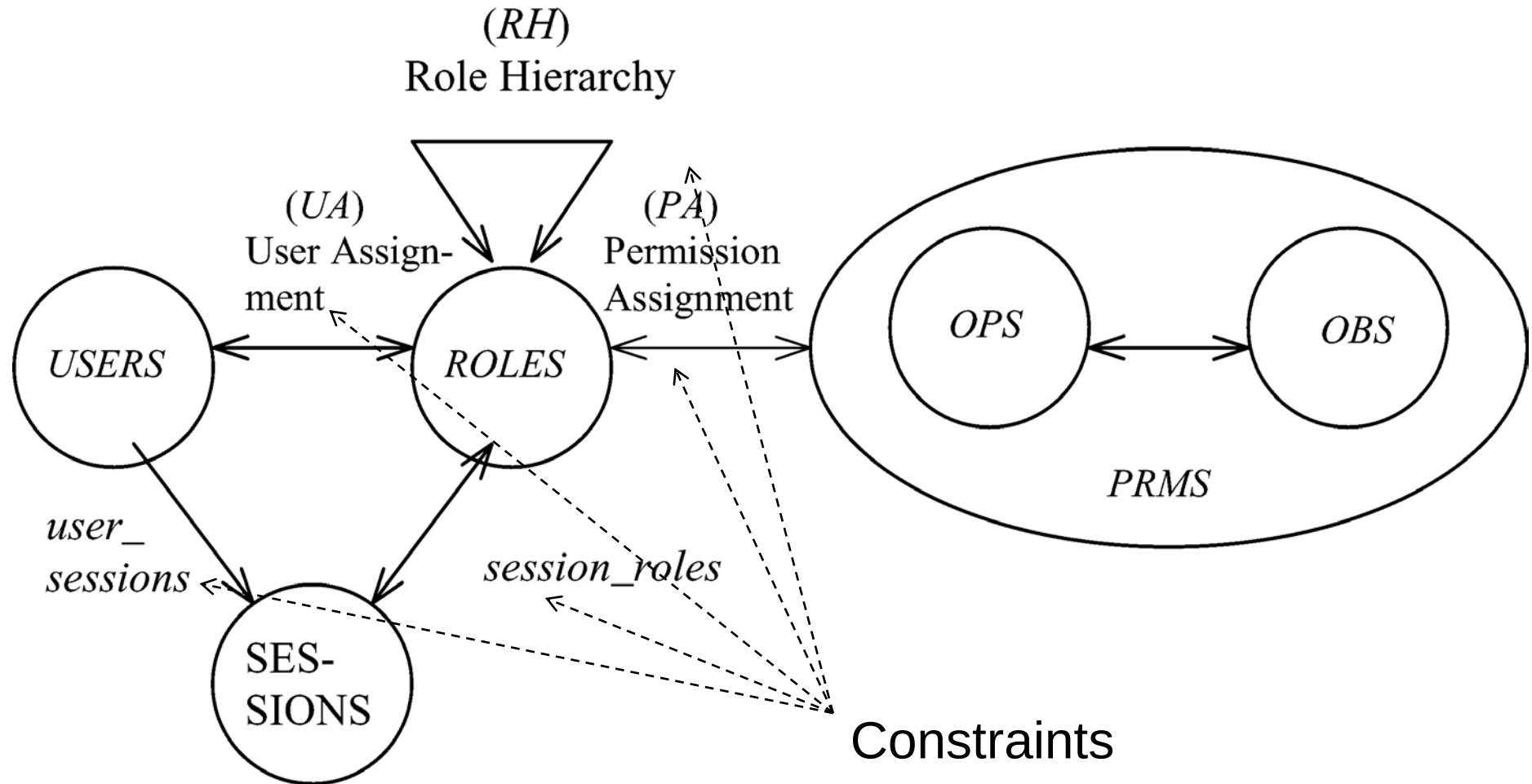
Messy or
Chaotic?

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

- Discretionary Access Control (DAC), 1970
 - ❖ Owner controls access
 - ❖ But only to the original, not to copies
 - ❖ Grounded in pre-computer policies of researchers
- Mandatory Access Control (MAC), 1970
 - ❖ Synonymous to Lattice-Based Access Control (LBAC)
 - ❖ Access based on security labels
 - ❖ Labels propagate to copies
 - ❖ Grounded in pre-computer military and national security policies
- Role-Based Access Control (RBAC), 1995
 - ❖ Access based on roles
 - ❖ Can be configured to do DAC or MAC
 - ❖ Grounded in pre-computer enterprise policies

Numerous other models but only 3 successes: SO FAR



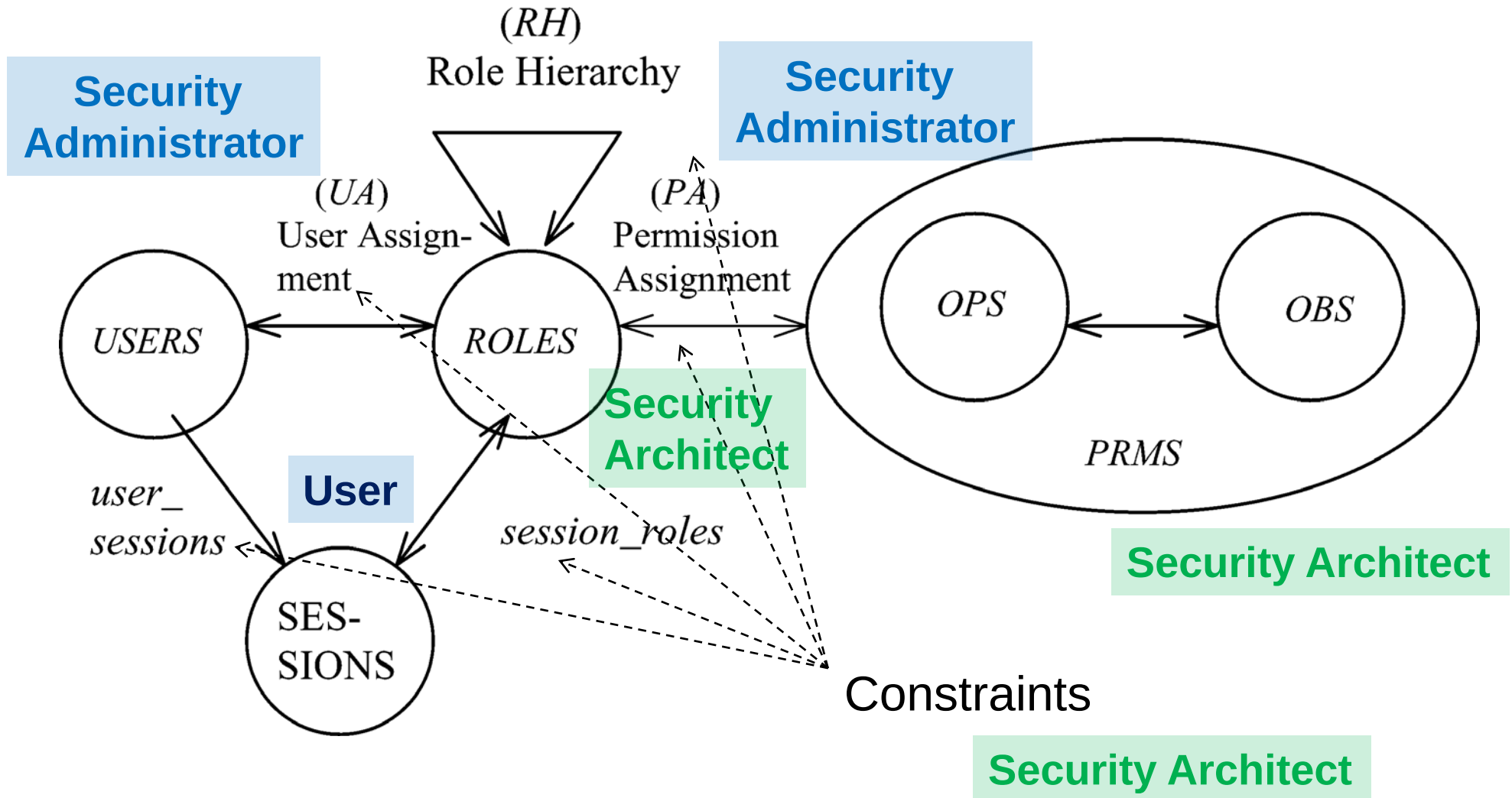


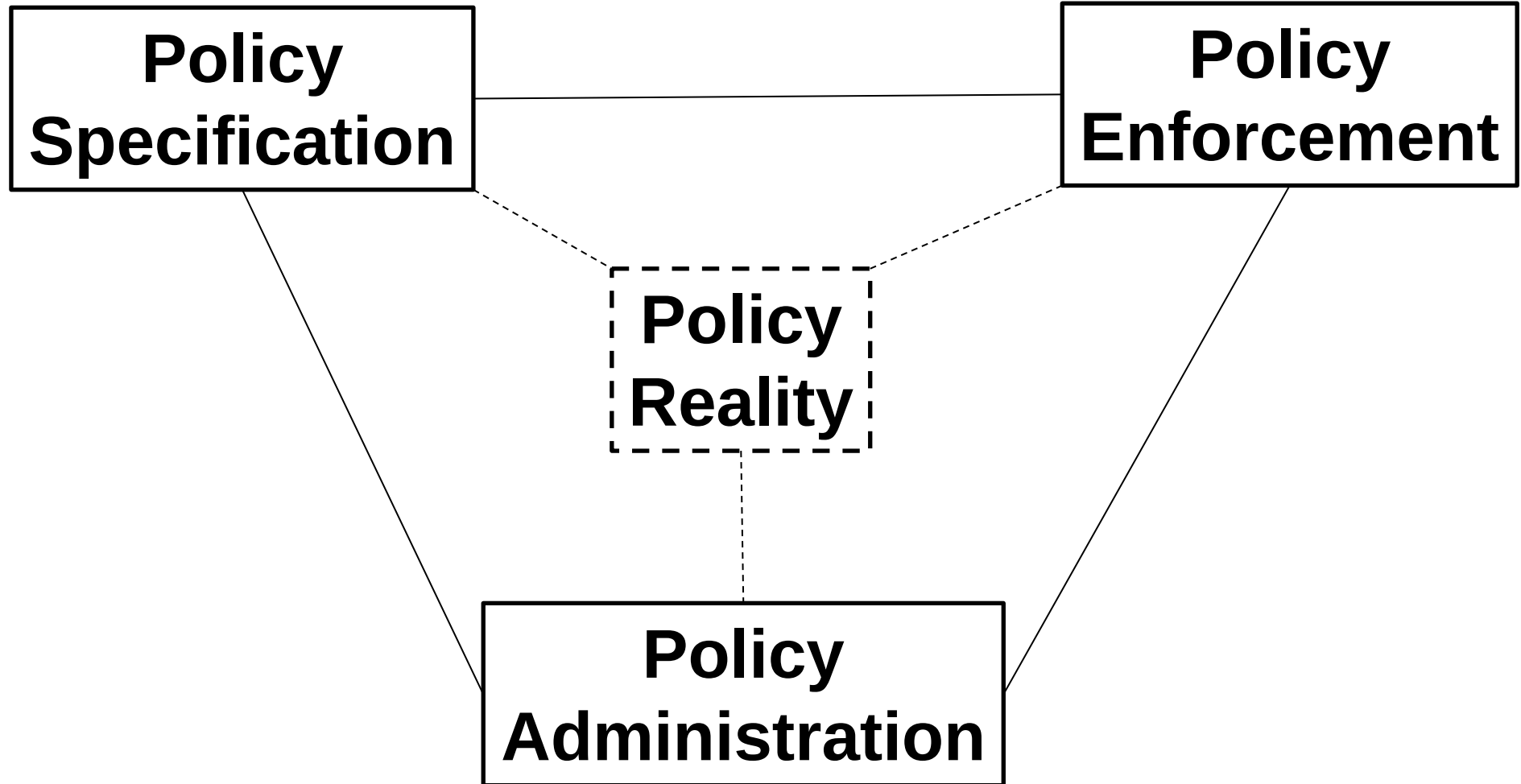
- RBAC can be configured to do MAC
- RBAC can be configured to do DAC
- RBAC is policy neutral

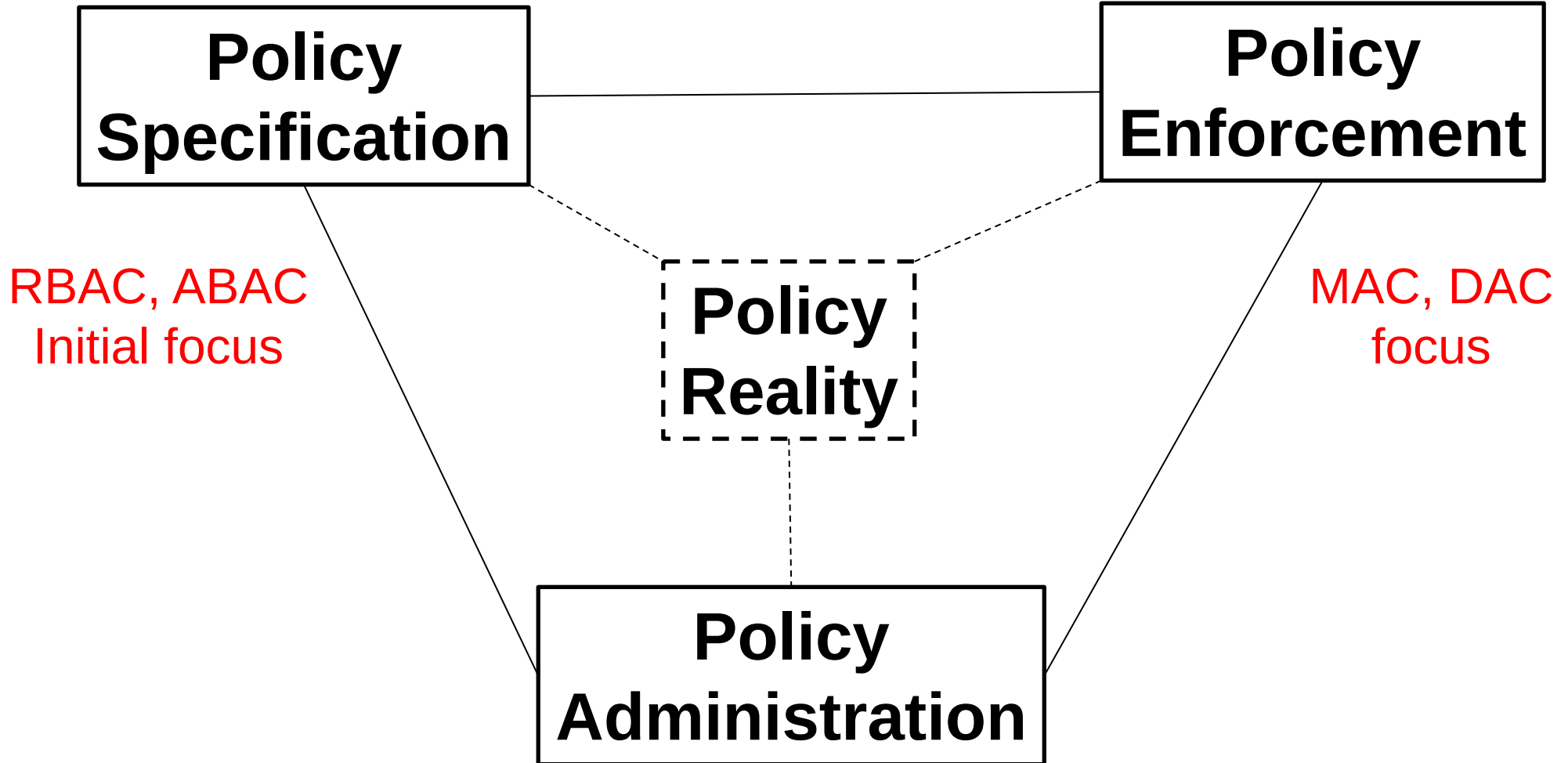
RBAC is neither MAC nor DAC!

- Role granularity is not adequate leading to role explosion
 - ❖ Researchers have suggested several extensions such as parameterized privileges, role templates, parameterized roles (1997-)
- Role design and engineering is difficult and expensive
 - ❖ Substantial research on role engineering top down or bottom up (1996-), and on role mining (2003-)
- Assignment of users/permissions to roles is cumbersome
 - ❖ Researchers have investigated decentralized administration (1997-), attribute-based implicit user-role assignment (2002-), role-delegation (2000-), role-based trust management (2003-), attribute-based implicit permission-role assignment (2012-)
- Adjustment based on local/global situational factors is difficult
 - ❖ Temporal (2001-) and spatial (2005-) extensions to RBAC proposed
- **RBAC does not offer an extension framework**
 - ❖ **Every shortcoming seems to need a custom extension**
 - ❖ **Can ABAC unify these extensions in a common open-ended framework?**

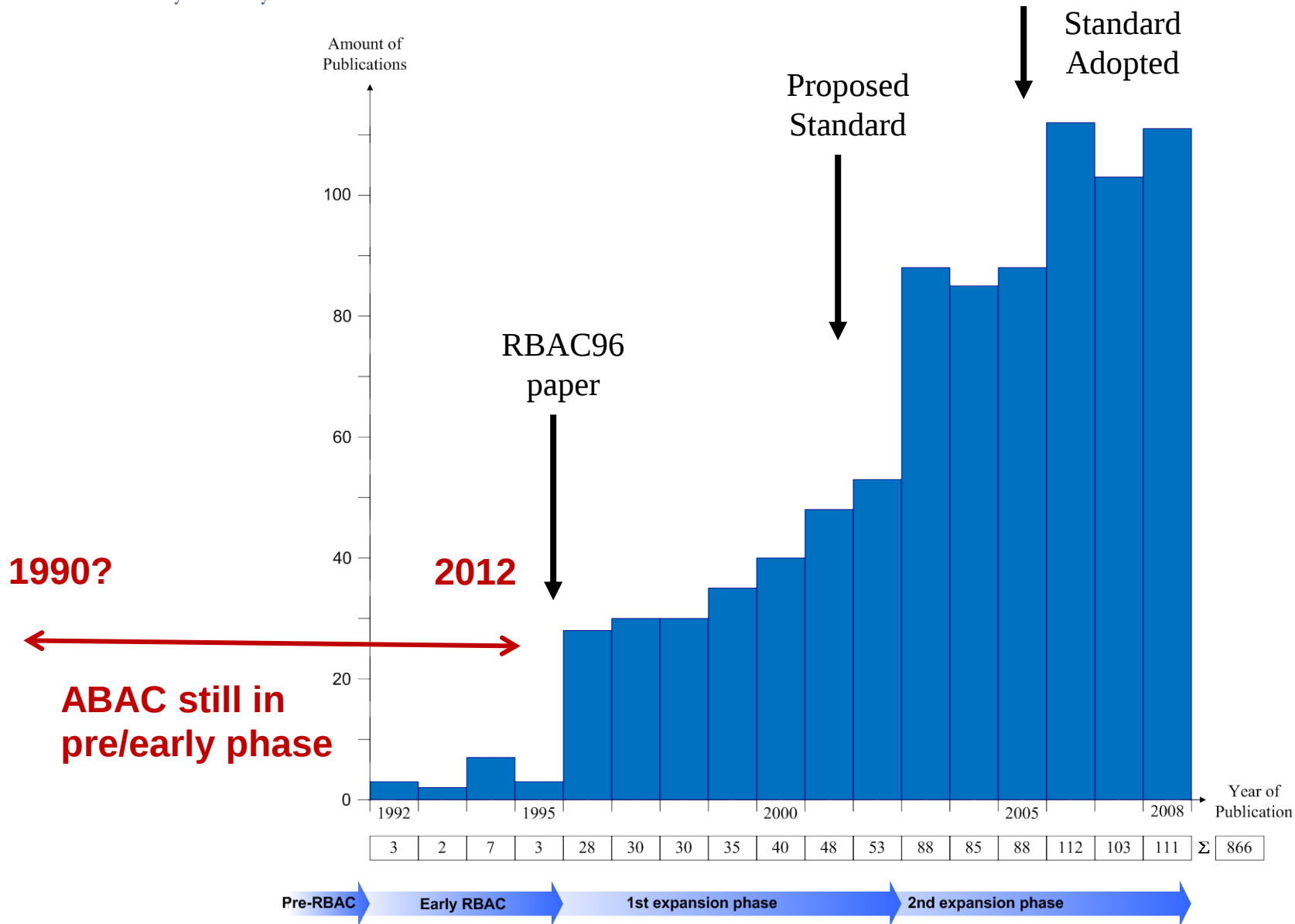
Security Architect







- Attributes are name:value pairs
 - ❖ possibly chained
 - ❖ values can be complex data structures
- Associated with
 - ❖ users
 - ❖ subjects
 - ❖ objects
 - ❖ contexts
 - device, connection, location, environment, system ...
- Converted by policies into rights just in time
 - ❖ policies specified by security architects
 - ❖ attributes maintained by security administrators
 - ❖ ordinary users morph into architects and administrators
- **Inherently extensible**

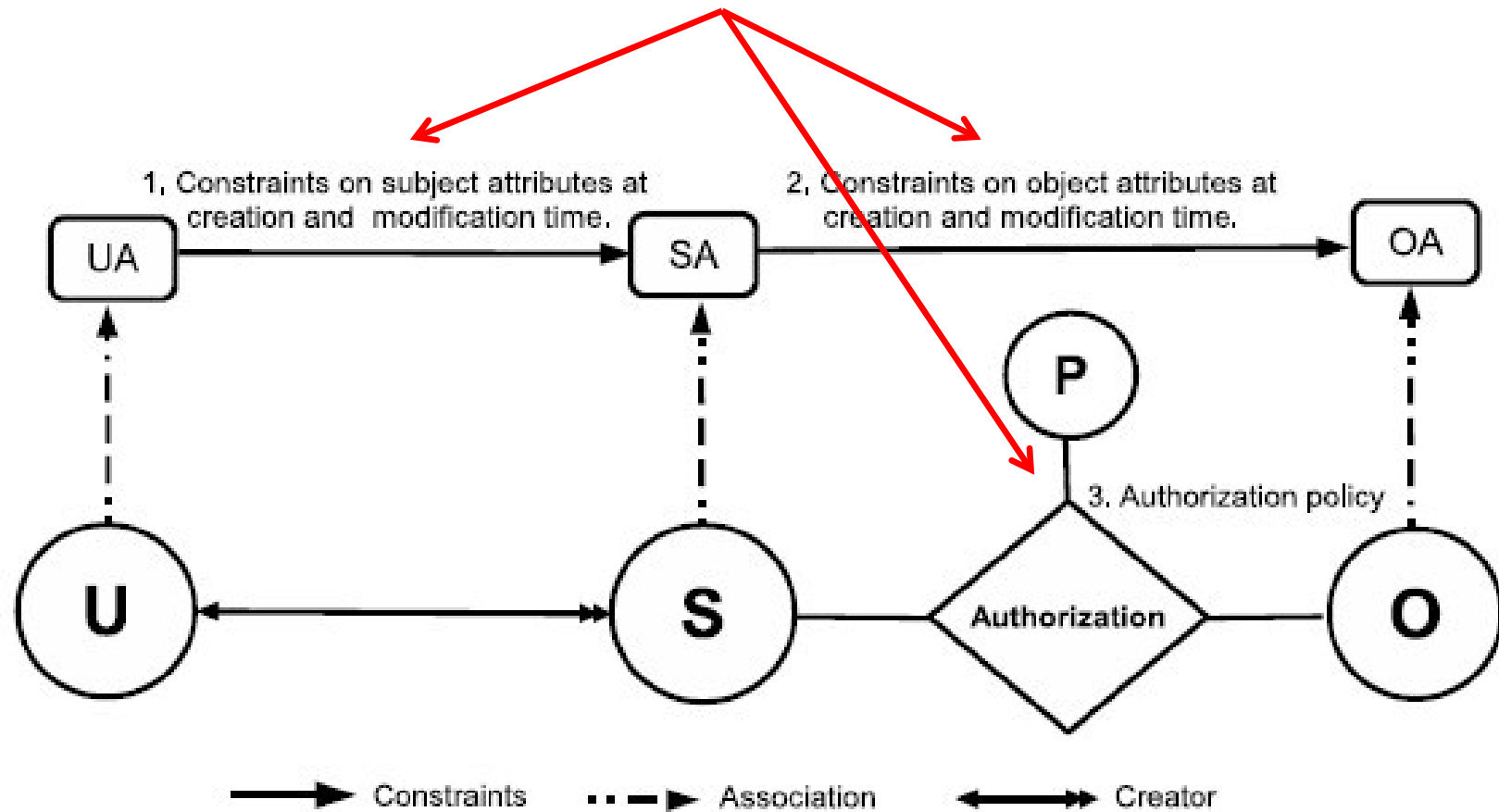


- X.509, SPKI Attribute Certificates (1999 onwards)
 - ❖ IETF RFCs and drafts
 - ❖ Tightly coupled with PKI (Public-Key Infrastructure)
- XACML (2003 onwards)
 - ❖ OASIS standard
 - ❖ Narrowly focused on particular policy combination issues
 - ❖ Fails to accommodate the ANSI-NIST RBAC standard model
 - ❖ Fails to address user subject mapping
- Usage Control or UCON (Park-Sandhu 2004)
 - ❖ Fails to address user subject mapping
 - ❖ Focus is on extended features
 - Mutable attributes
 - Continuous enforcement
 - Obligations
 - Conditions
- Several others

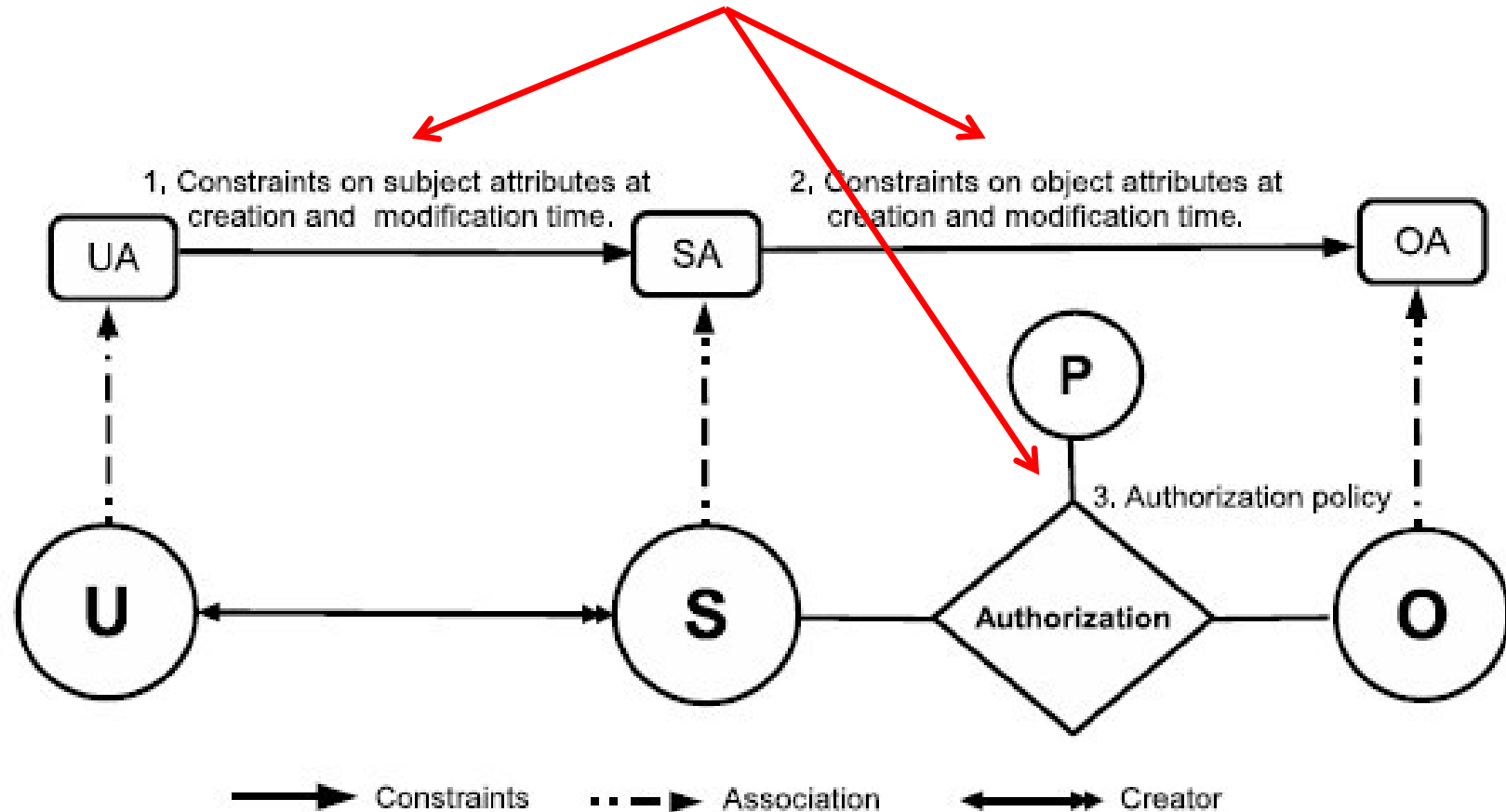
- An ABAC model requires
 - ❖ identification of policy configuration points (PCPs)
 - ❖ languages and formalisms for each PCP
- A core set of PCPs can be discovered by building the ABAC α model to unify DAC, MAC and RBAC
- Additional ABAC models can then be developed by
 - ❖ increasing the sophistication of the ABAC α PCPs
 - ❖ discovering additional PCPs driven by requirements beyond DAC, MAC and RBAC

A small but crucial step

Policy Configuration Points



Policy Configuration Points



Can be configured to do DAC, MAC, RBAC

1, 2, 4, 5

Extended Constraints on Role Activation:

Attribute-Based User-Role Assignment- 2002 [6], OASIS-RBAC-2002 [9], SRBAC-2003 [46], Rule-RBAC-2004 [5], GEO-RBAC-2005 [16]

1,4

Extended Concept of Role:

Role Template-1997 [45], Parameterized RBAC-2004 [2], Parameterized RBAC-2003 [34], Parameterized Role-2004 [43], Attributed Role-2006 [99]

1, 4, 5

Changes in Role-Permission Relationship:

Task-RBAC-2000 [77], Task-RBAC-2003 [78]

Extended Permission Structure:

RBAC with Object class- 2007 [24], Conditional PRBAC 07 [74], PRBAC 07 [75], Purpose-aware RBAC- 2008 [67], Ubi-RBAC-2010 [76], RCPBAC-2011 [55]

4, 5

Organization and Team:

Relationship-RBAC -1997 [12], TeamMAC-1997 [87], TeamMAC-2004 [7], ROBAC-2006 [103], Group-RBAC-2009 [66], RABAC-2013 [51], Domain-RBAC -2013 [98]

4

1, 4, 5

Context:

C-TMAC-2001 [44], GRBAC -2001 [70], Context Role-2001 [30], Context-Sensitive RBAC-2002 [63], Contextual RBAC-2003 [69], STRBAC-2006 [64], Spatial-temporal-RBAC-2007[81], CA-RBAC-2008 [62], Modelling Context-2008 [32]

1, 2, 3, 4, 5

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

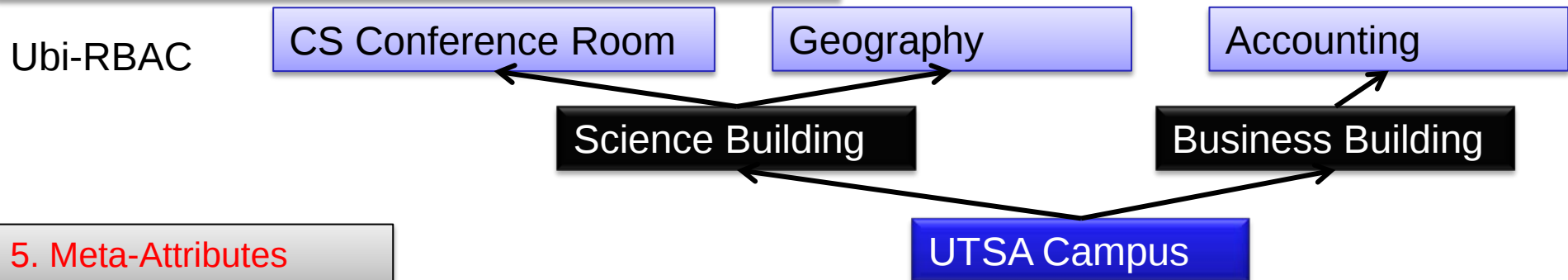
1. Context Attributes

2. Subject attribute constraints policy are different at creation and modification time.

OASIS-RBAC

- Prerequisite role
- Initial role assignment constraints
- Other role assignment constraints

3. Subject attributes constraints by attributes of subjects created by the same user.



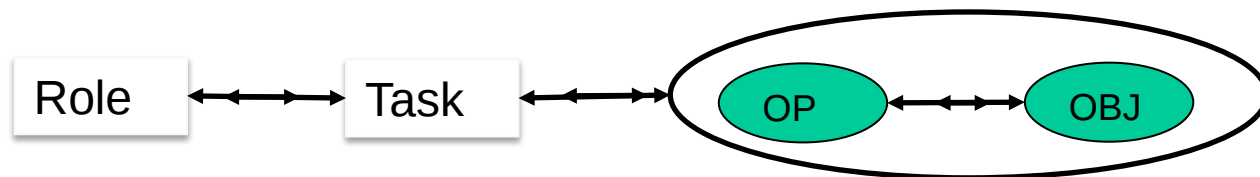
5. Meta-Attributes

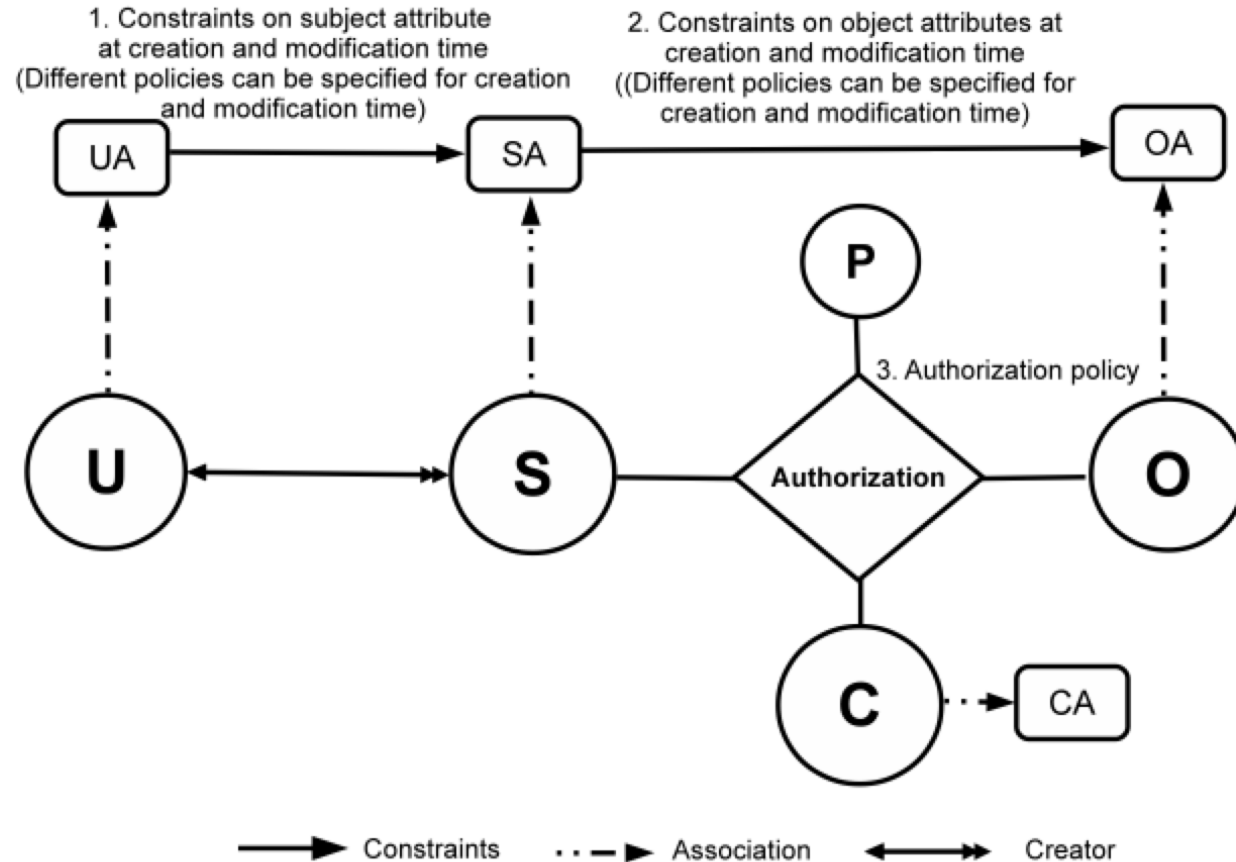
Task-RBAC

$\text{task}(r1) = \{t1, t2\}$

$\text{readtask}(o1) = \{t1, t2, t3\}$

$\text{urole}(u) = \{r1, r2\}$





- GURA model for user-attribute assignment
- Safety analysis of $ABAC_{\alpha}$ and $ABAC_{\beta}$
- Undecidable safety for ABAC models
- Decidable safety for ABAC with finite fixed attributes
- Constraints in ABAC
- ABAC Cloud IaaS implementations (OpenStack)
- Attribute Engineering
- Attribute Mining
- Unification of Attributes, Relationships and Provenance