Attribute-Based Access Control Models and Beyond

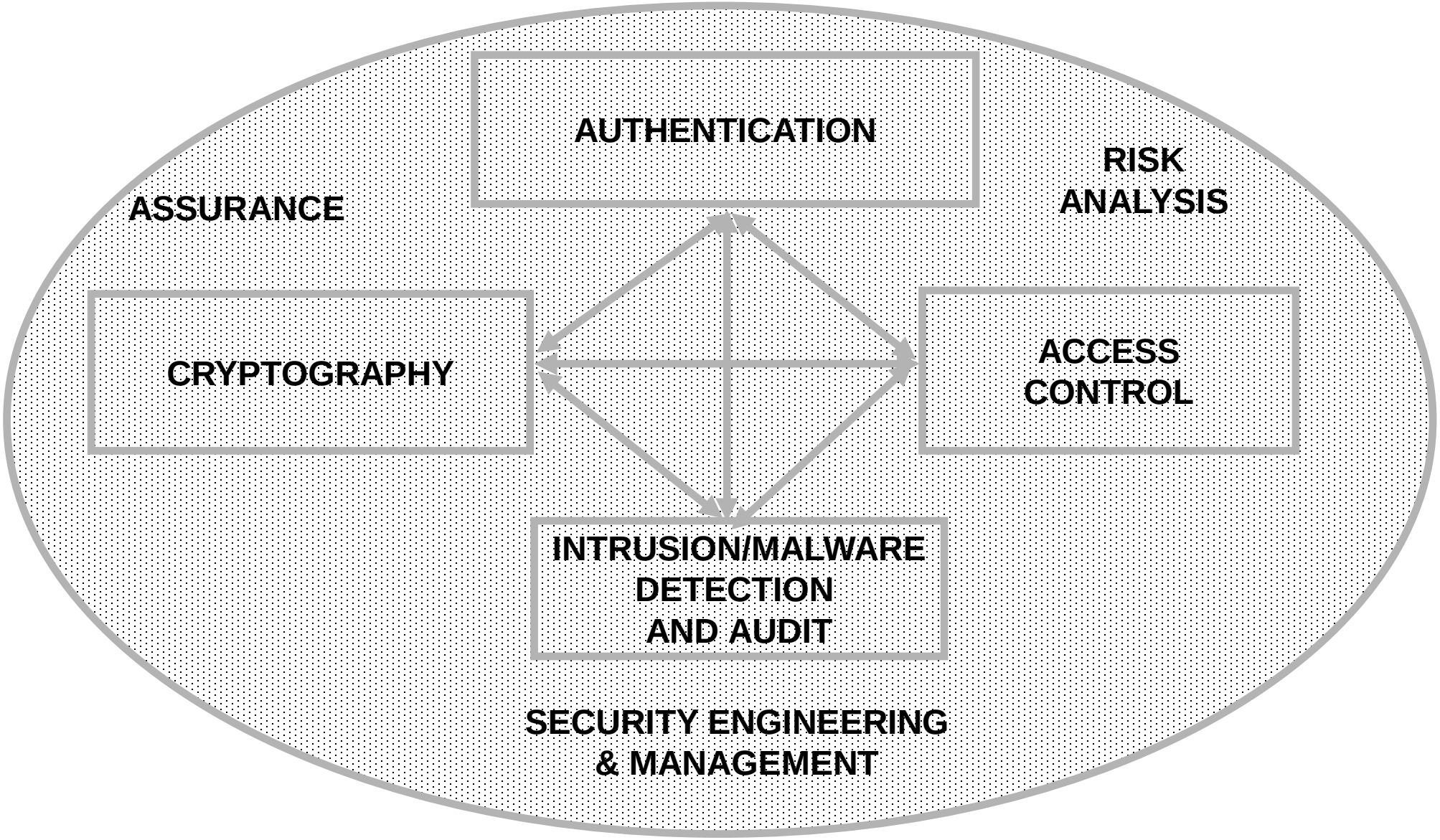
Prof. Ravi Sandhu

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

Future of Identity Workshop,
November 13 2014, City University London

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

Cyber Security Technologies

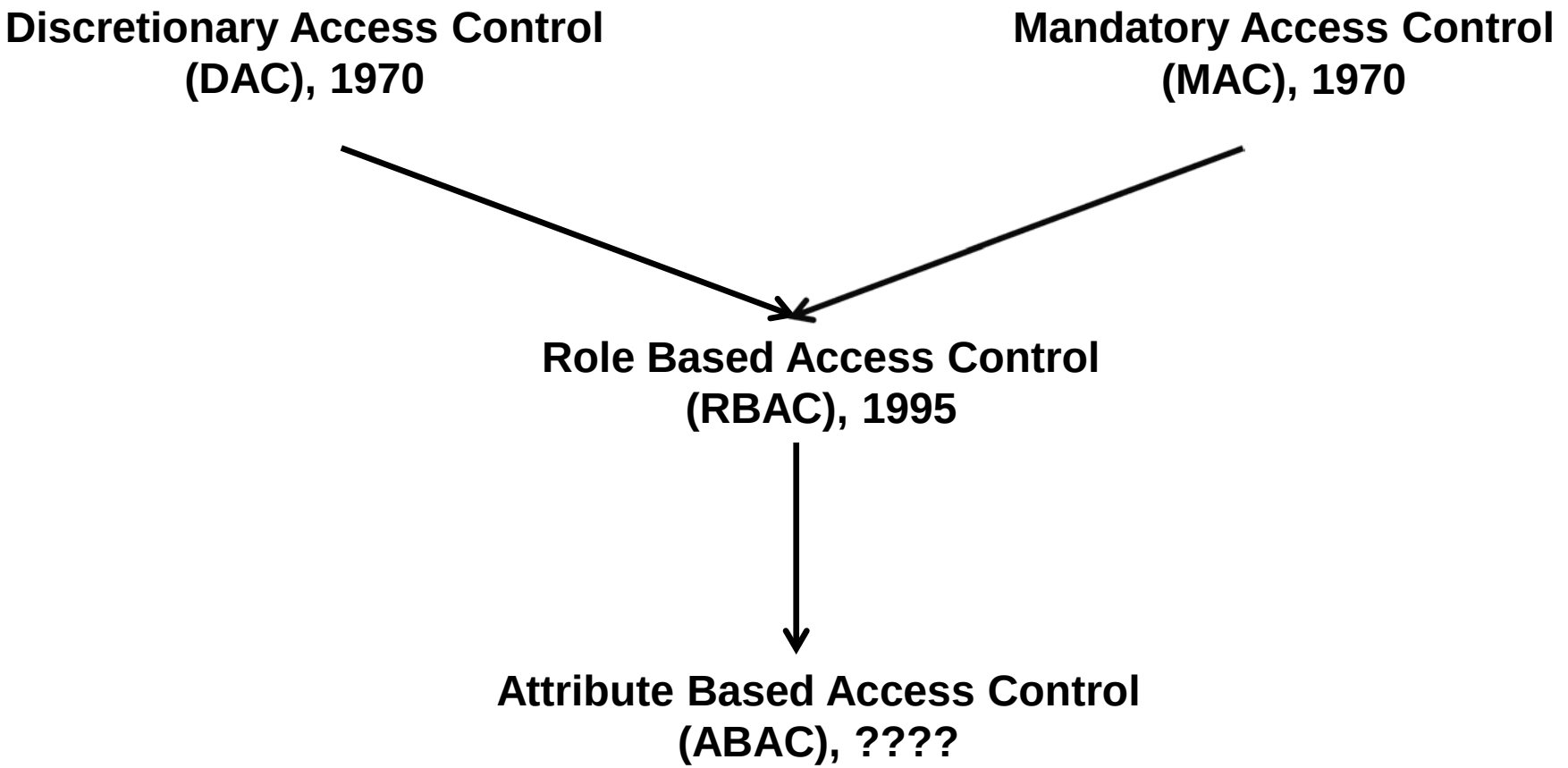


Security Limitations

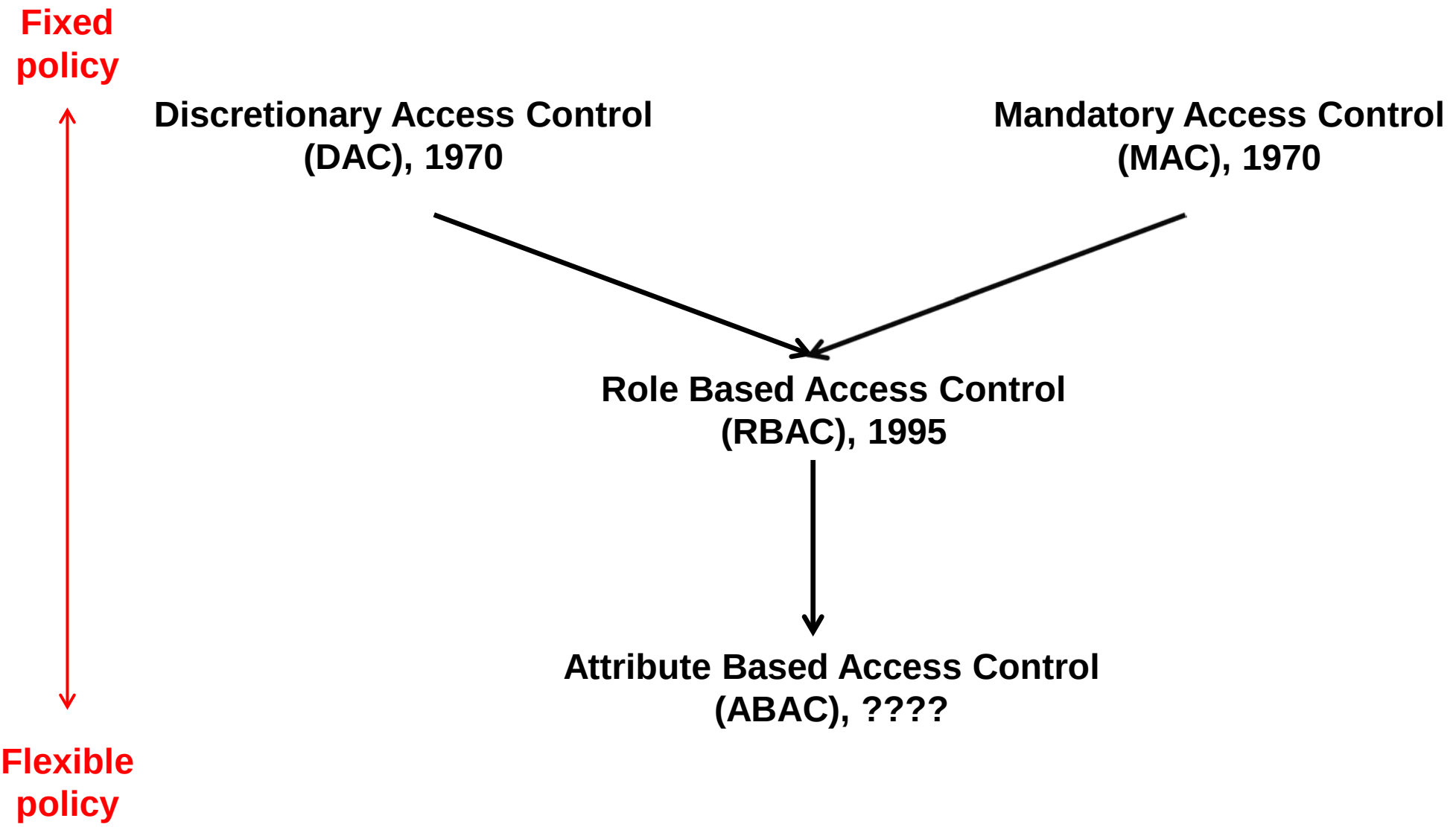
- Analog Hole
- Inference
- Covert Channels
- Side Channels
- Phishing
- Social Engineering
- Attack Asymmetry
- Privacy
- ….

Can manage
Cannot eliminate

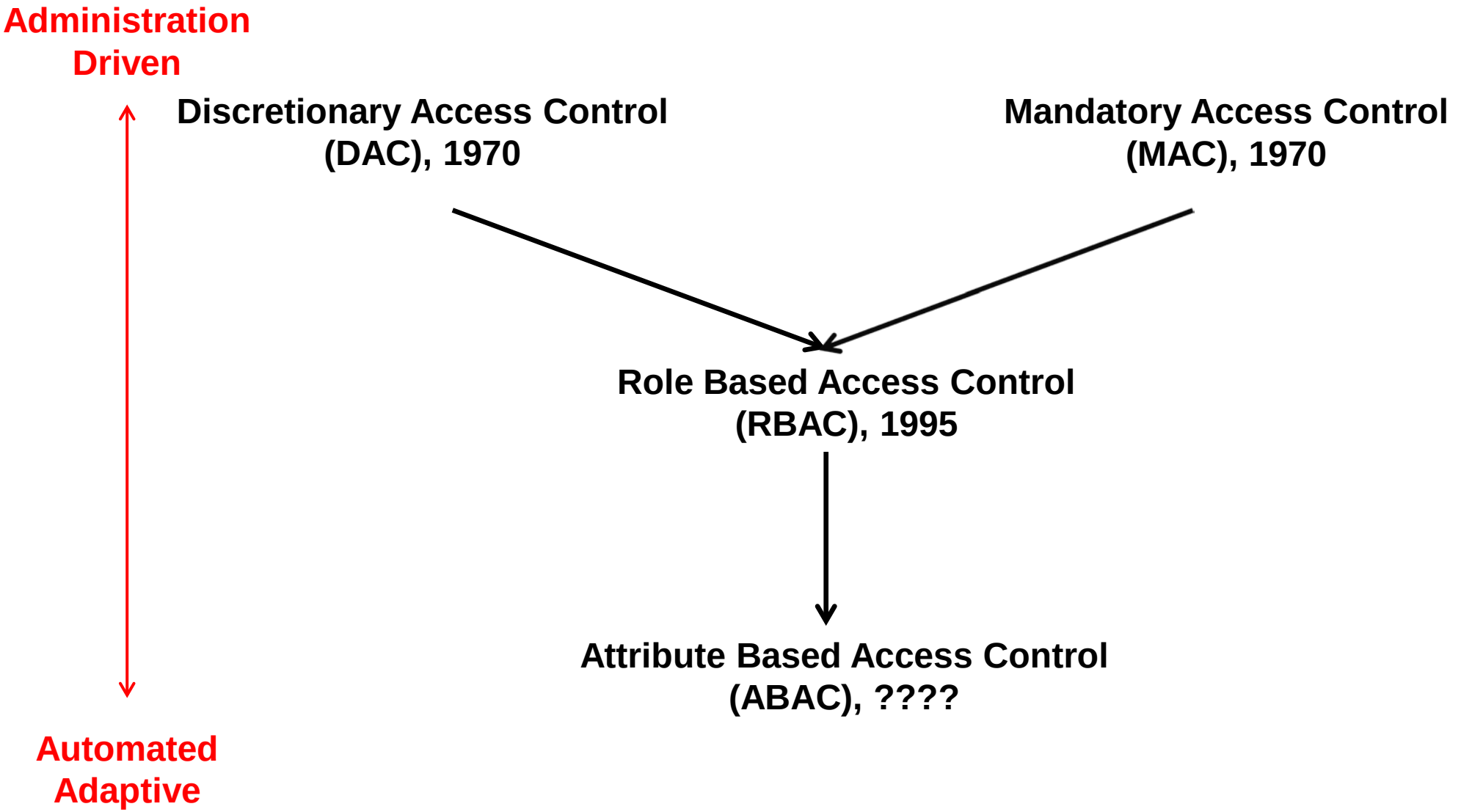
Access Control



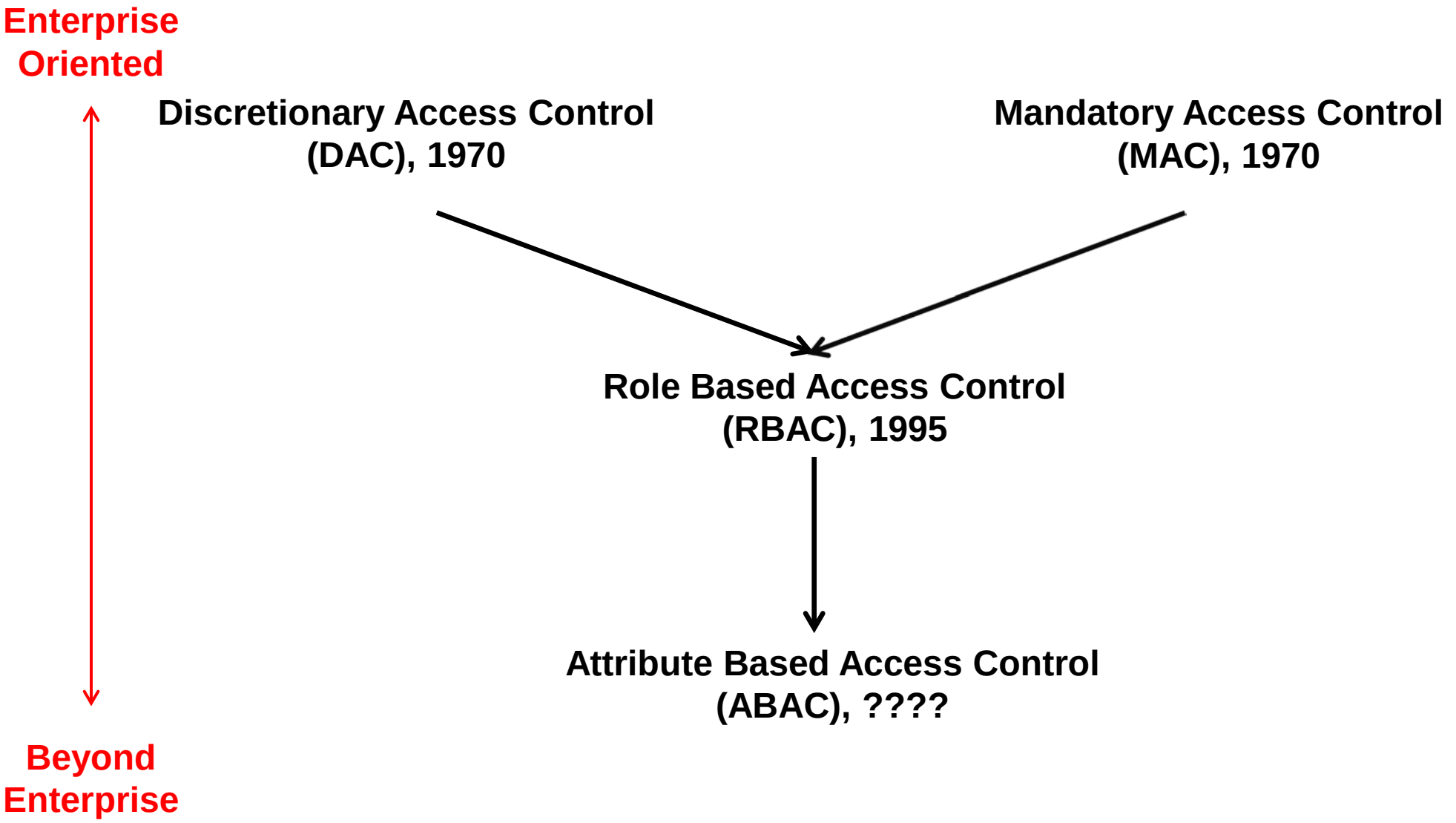
Access Control



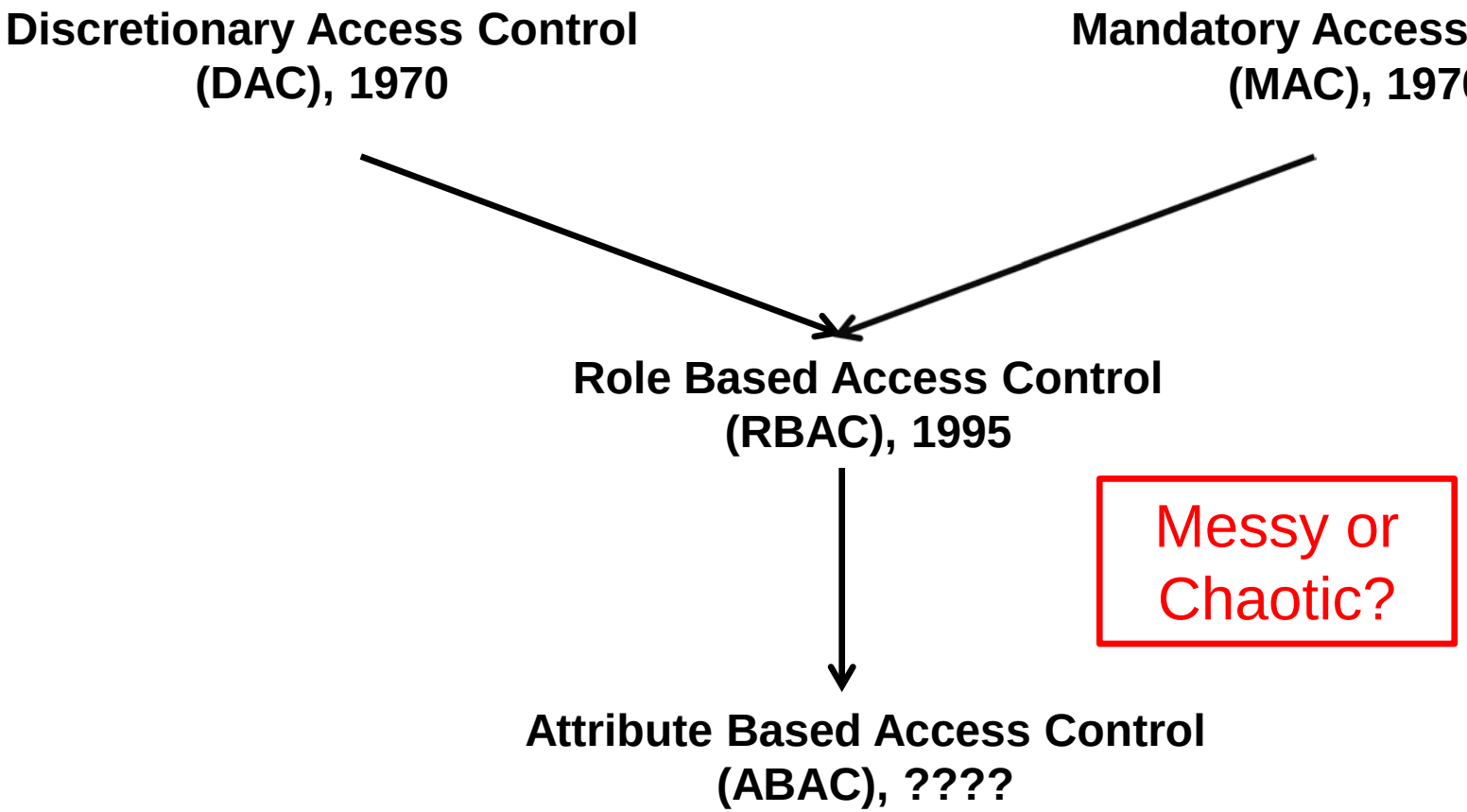
Access Control



Access Control



Access Control

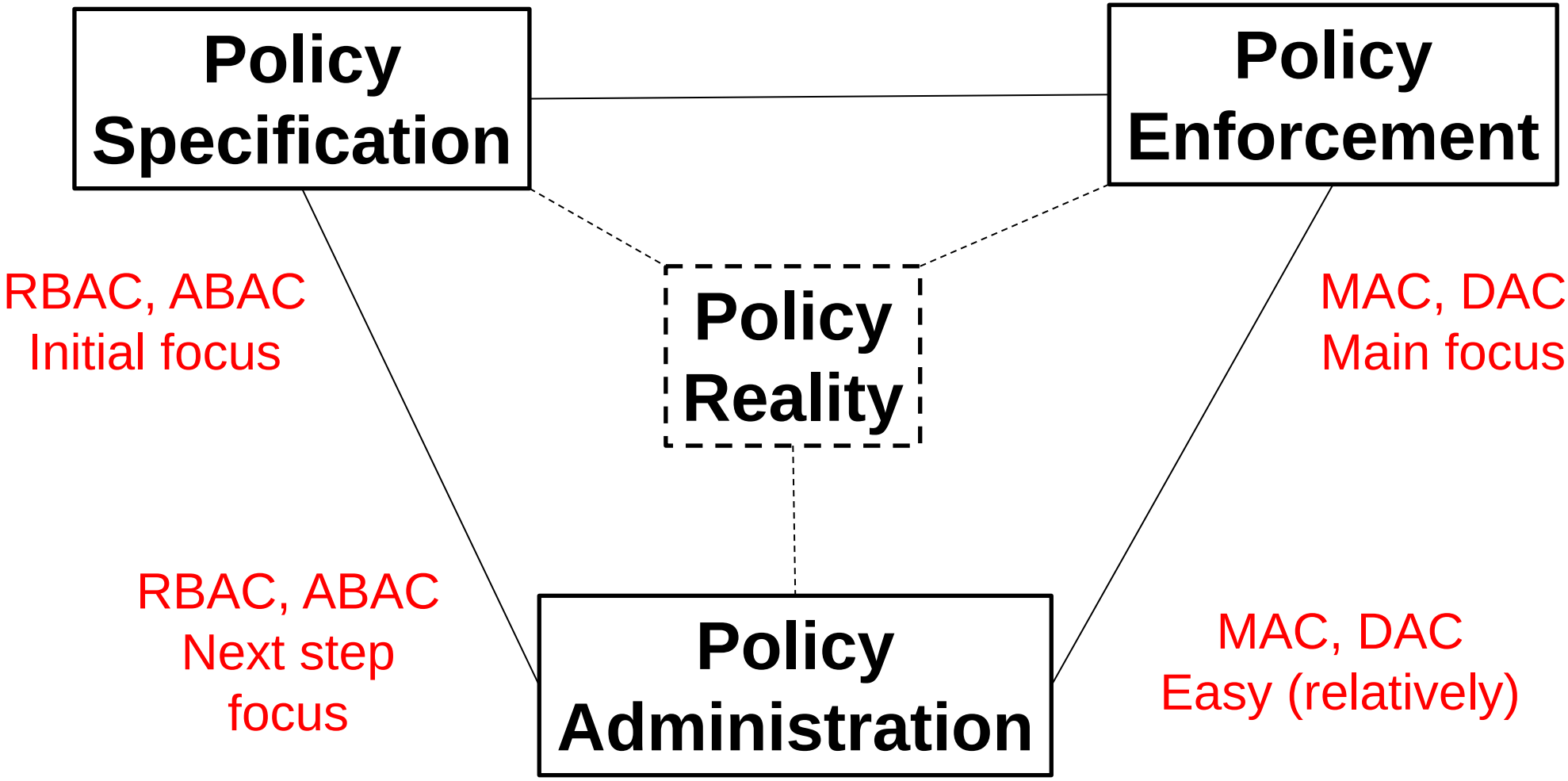


Access Control Models

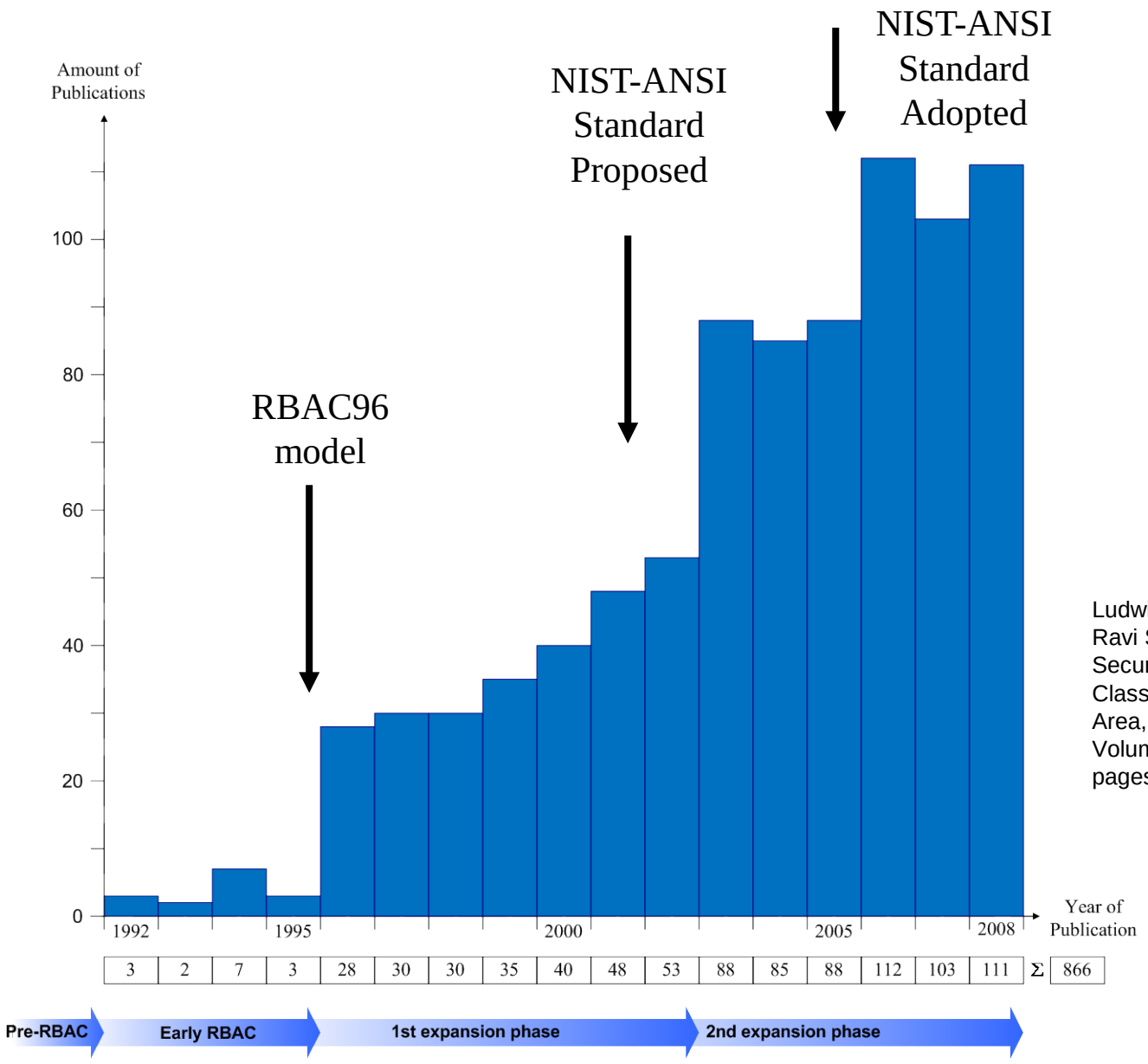
- Discretionary Access Control (DAC), 1970
  - Owner controls access
  - But only to the original, not to copies
  - Grounded in pre-computer policies of researchers
- Mandatory Access Control (MAC), 1970
  - Synonymous to Lattice-Based Access Control (LBAC)
  - Access based on security labels
  - Labels 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

Access Control Models

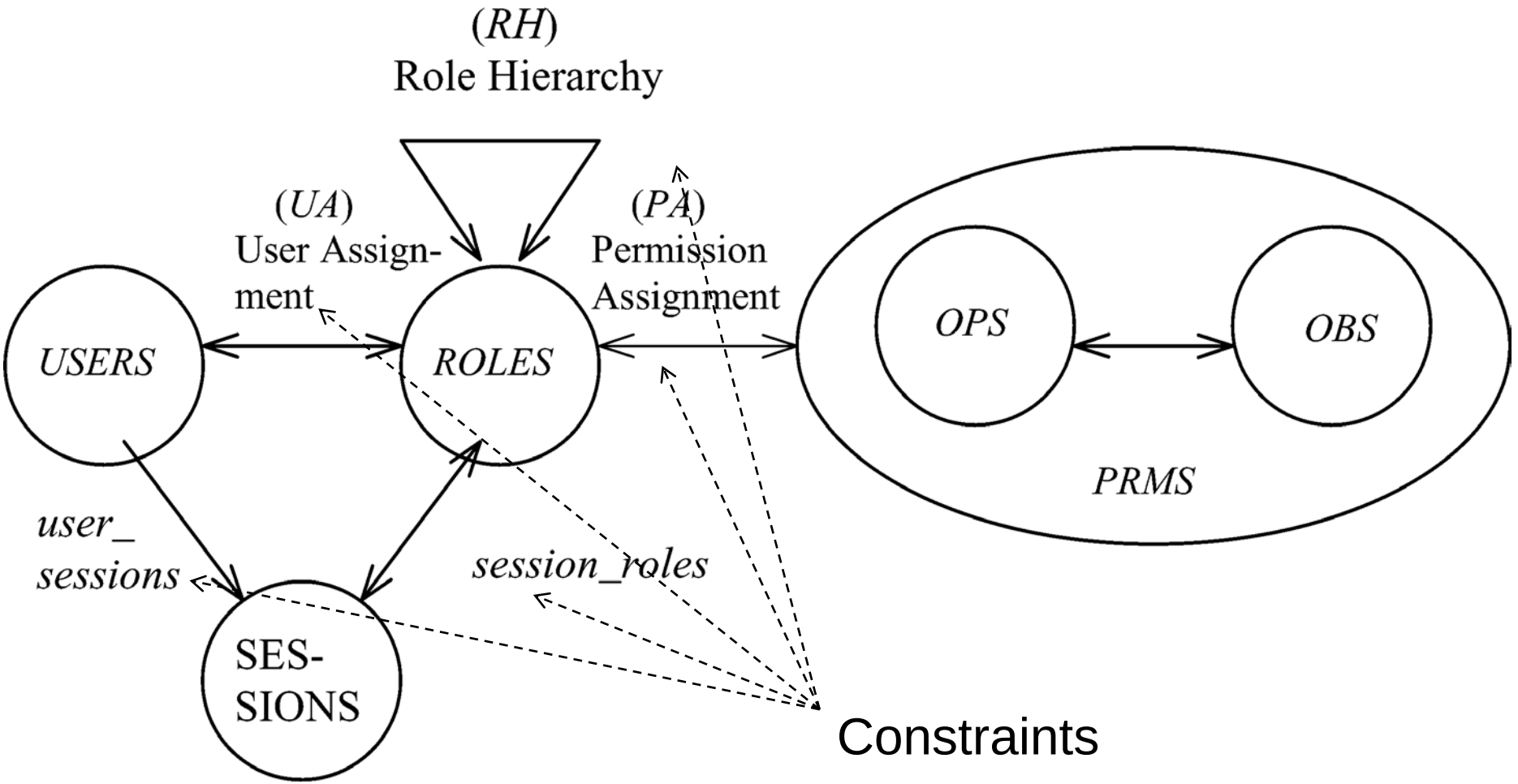


The RBAC Story

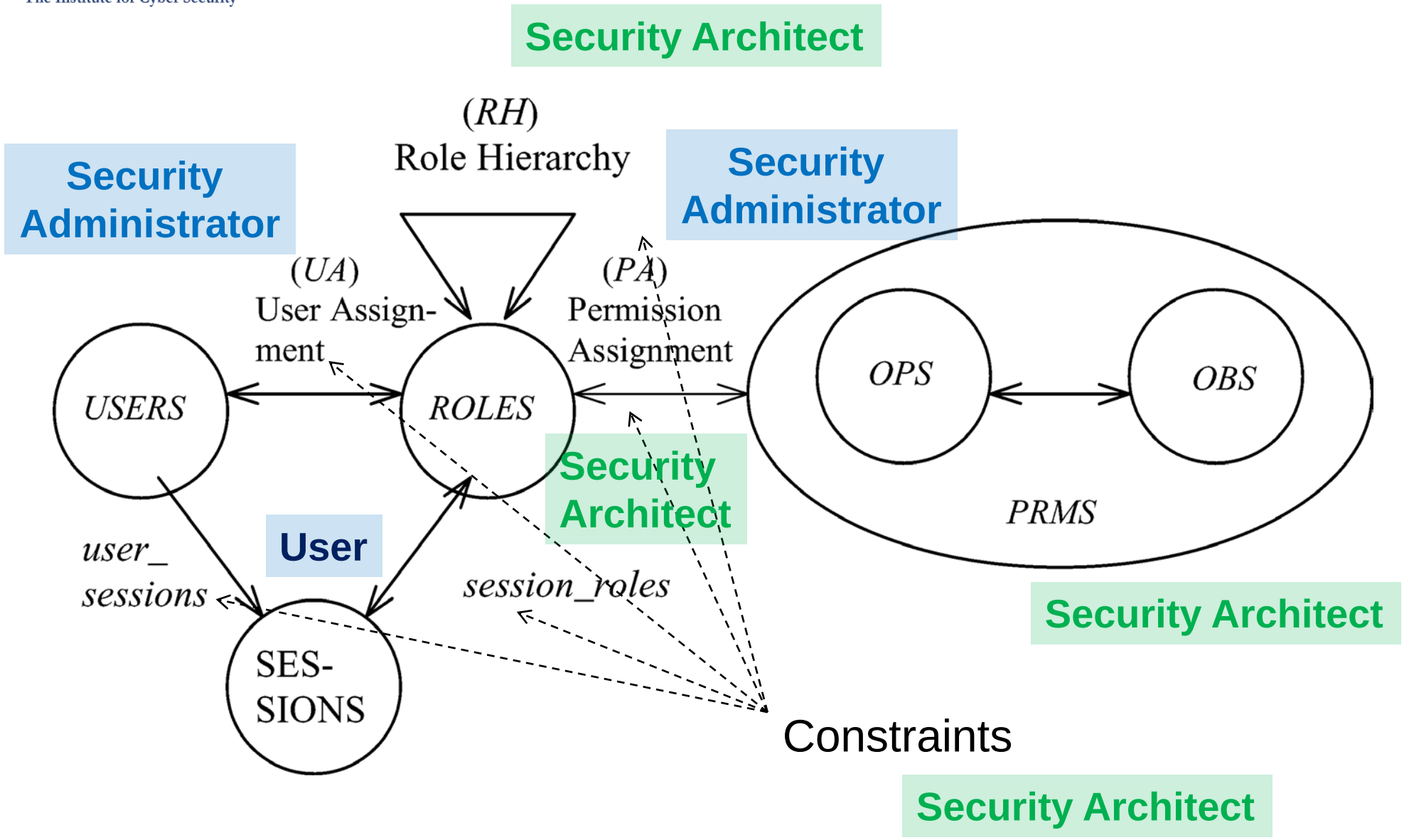


Ludwig Fuchs, Gunther Pernul and Ravi Sandhu, Roles in Information Security-A Survey and Classification of the Research Area, Computers & Security, Volume 30, Number 8, Nov. 2011, pages 748-76

RBAC96 Model



RBAC Policy Configuration Points



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!

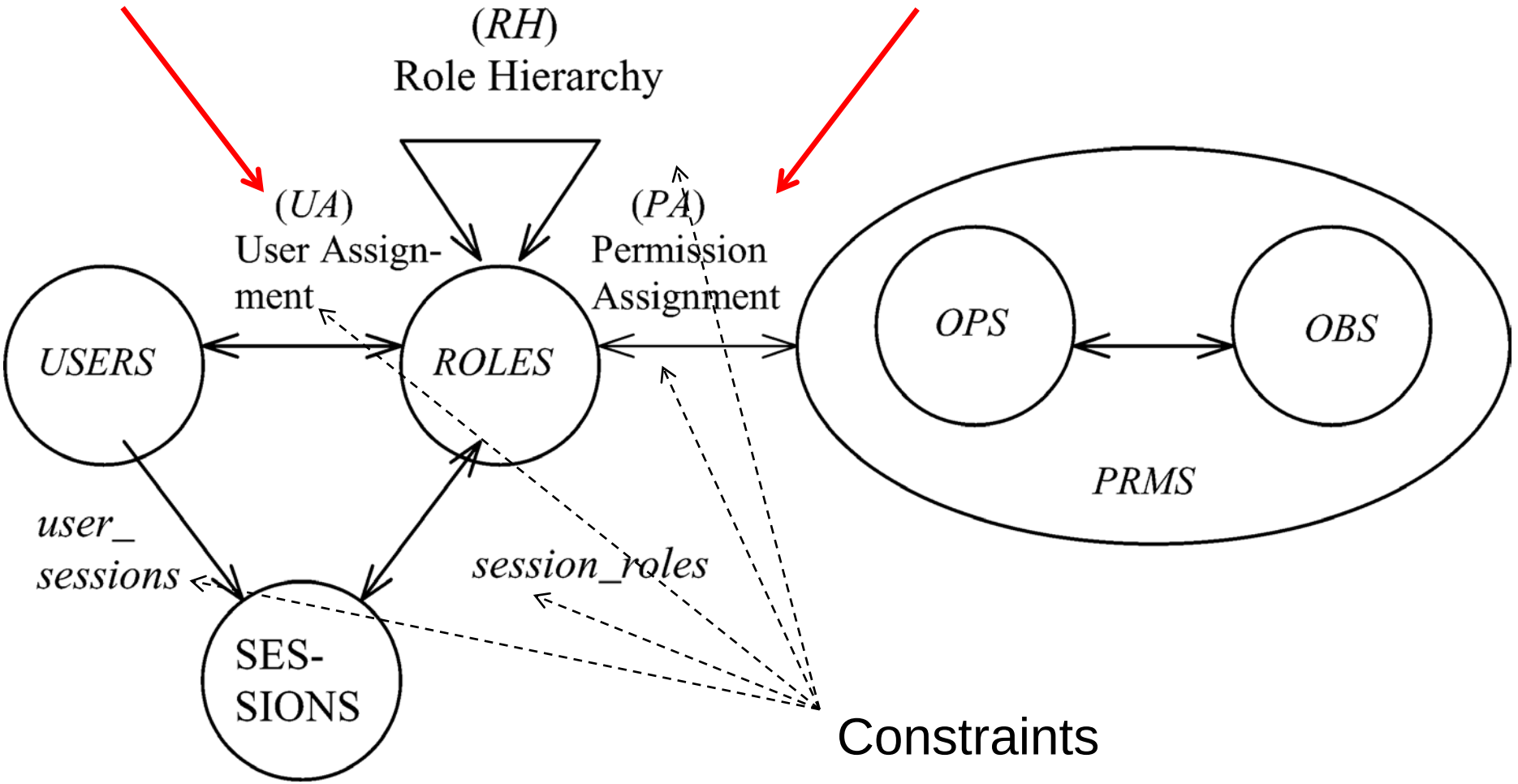
RBAC Shortcomings

- 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?

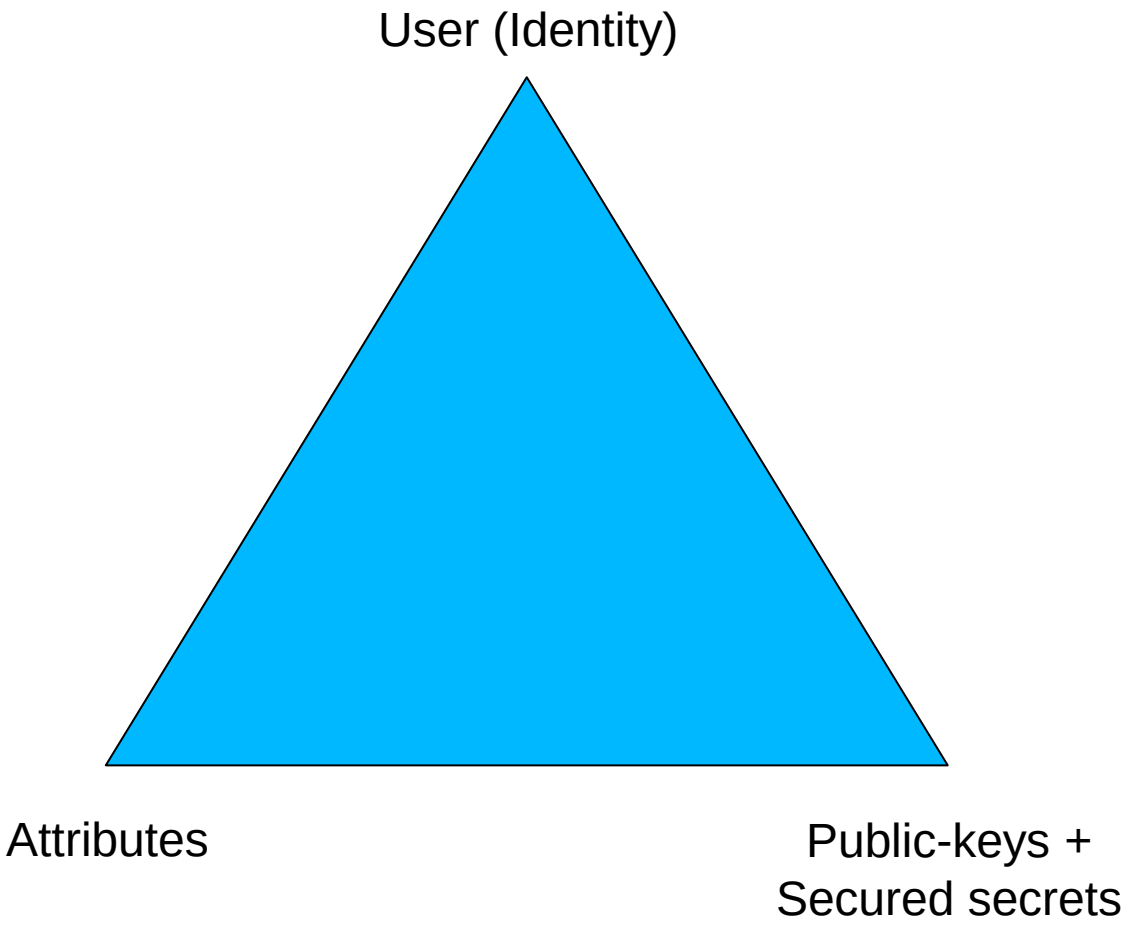
RBAC Shortcomings

Hard Enough

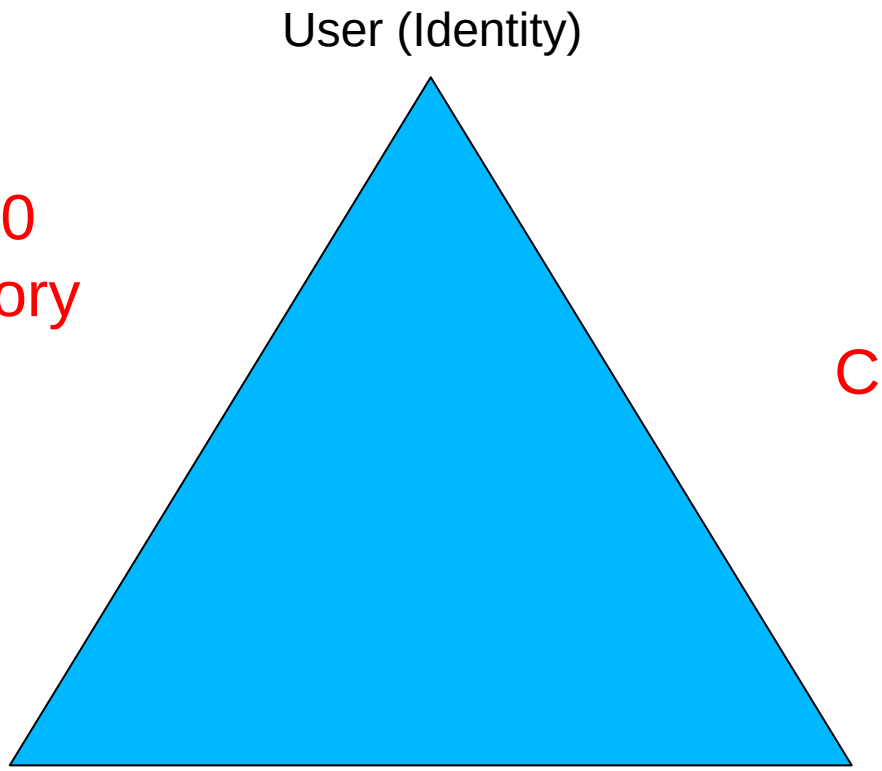
Impossible



ABAC is not New

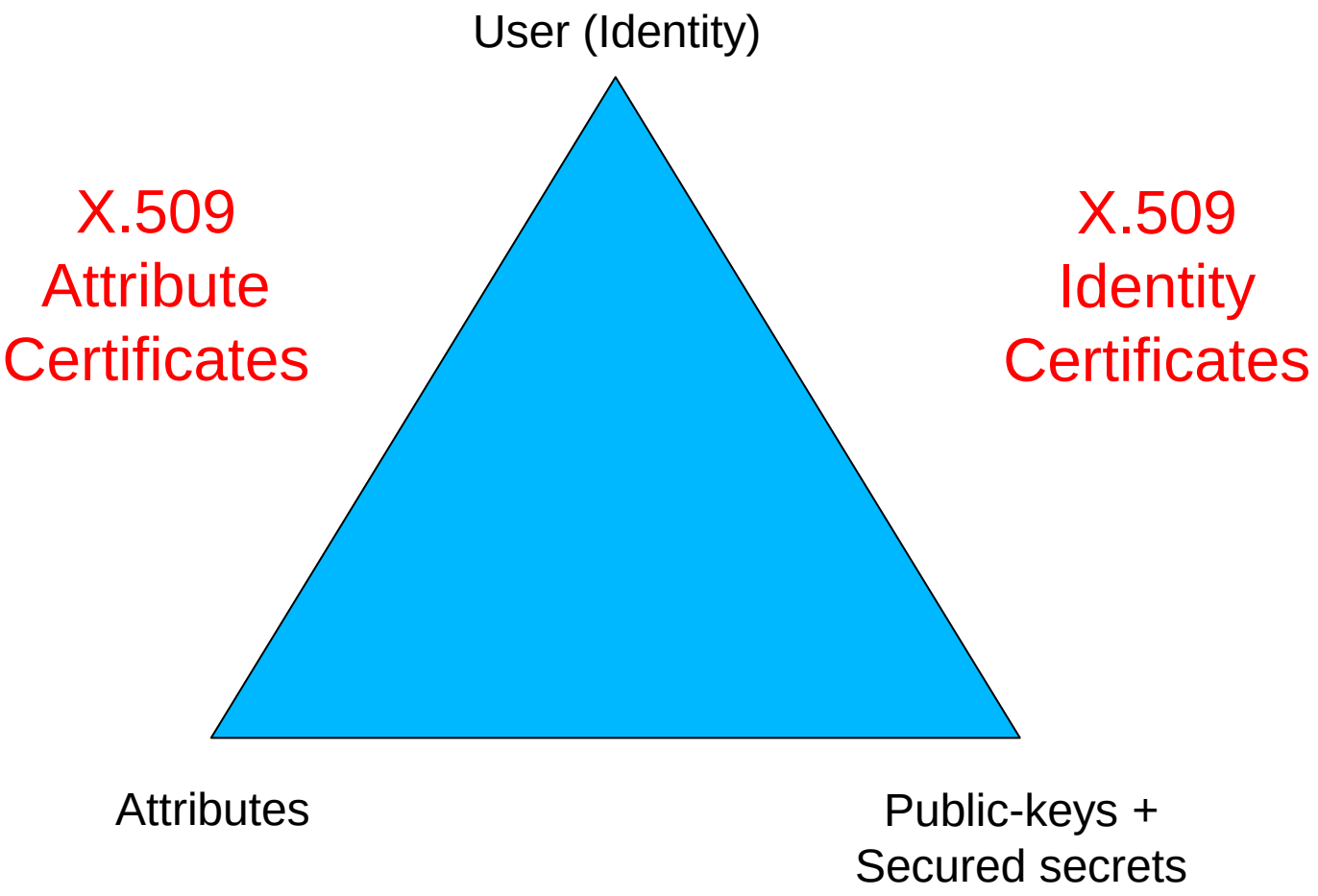


ABAC is not New



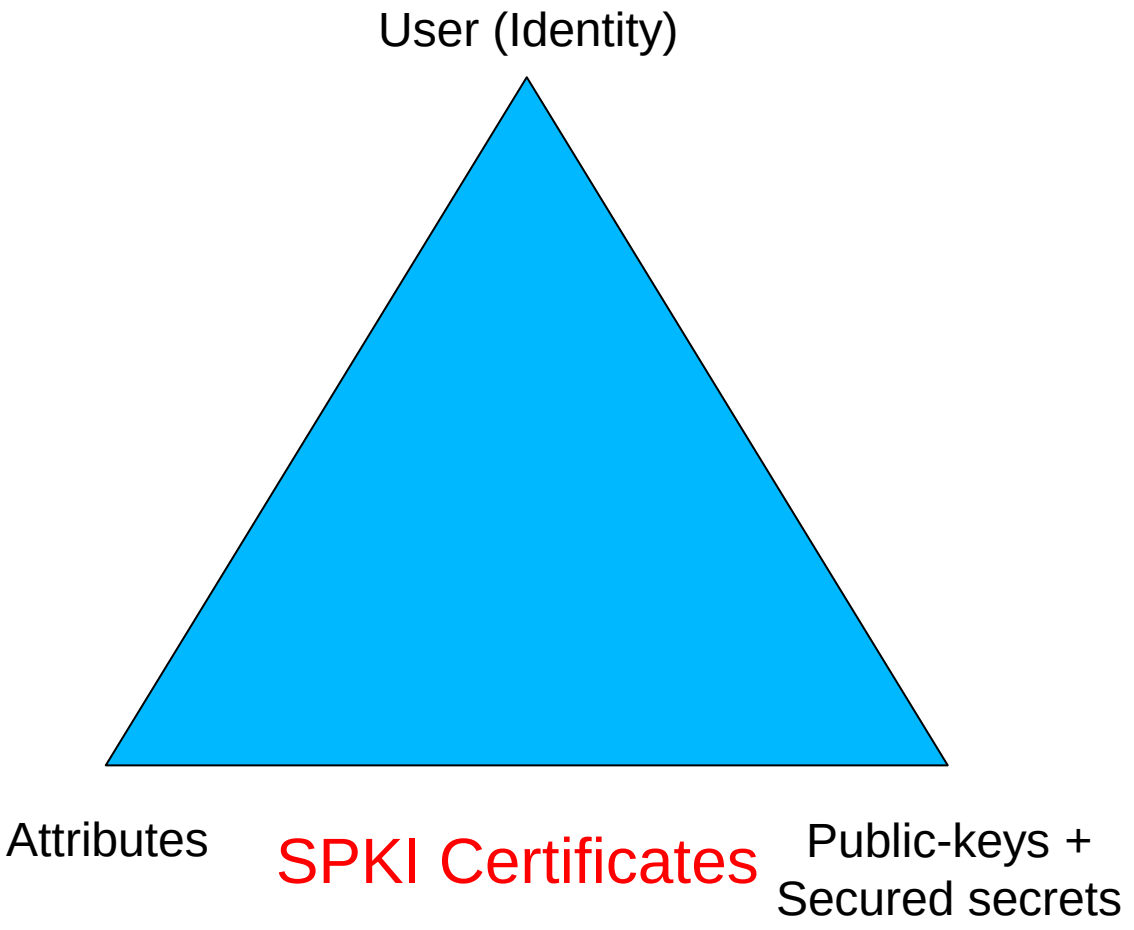
Pre Internet, early 1990s

ABAC is not New



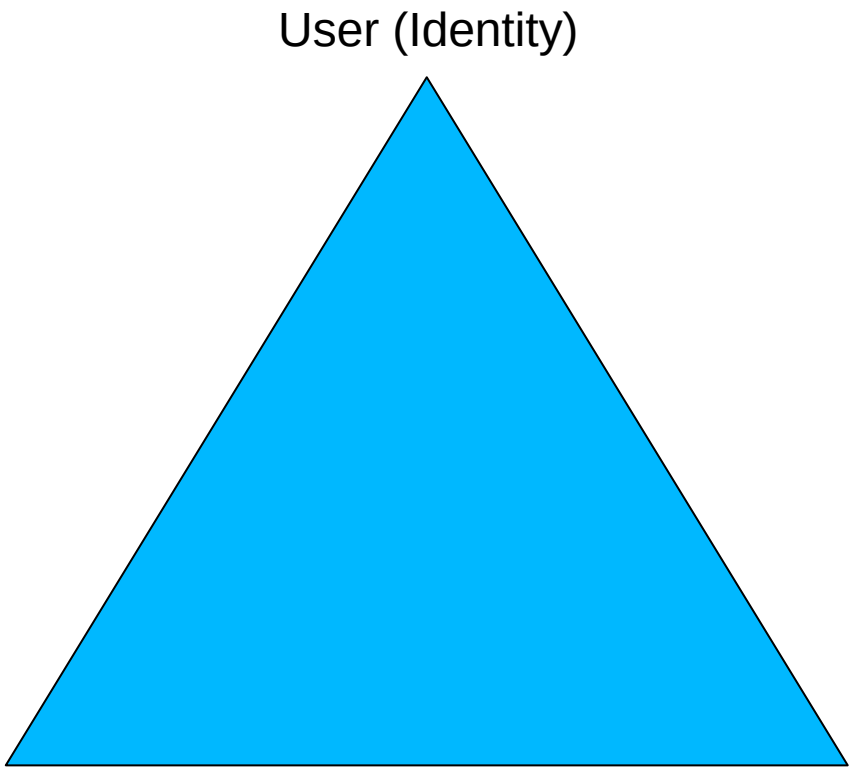
Post Internet, late 1990s

ABAC is not New



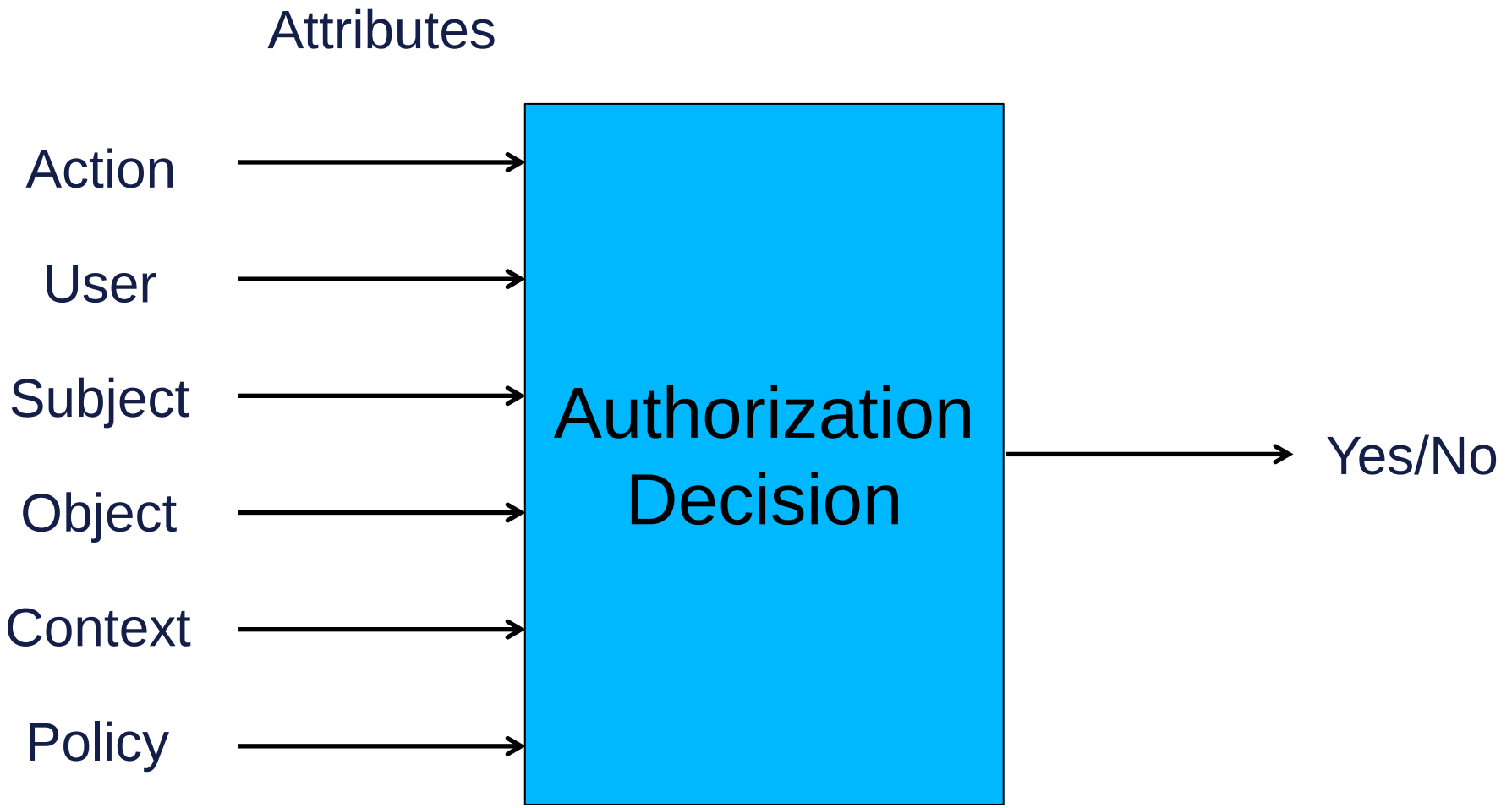
Post Internet, late 1990s

ABAC is not New

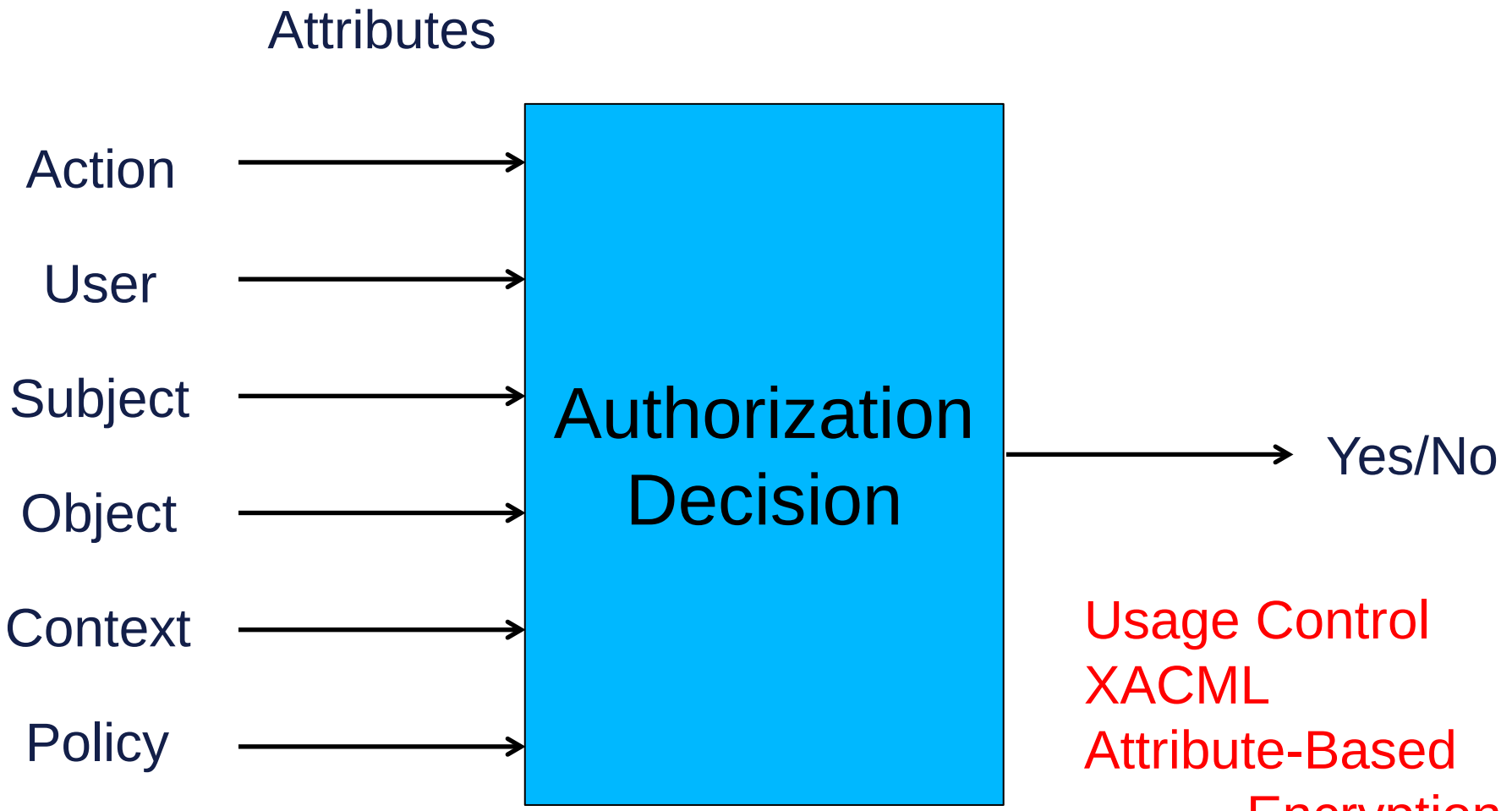


Mature Internet, 2000s

ABAC is not New



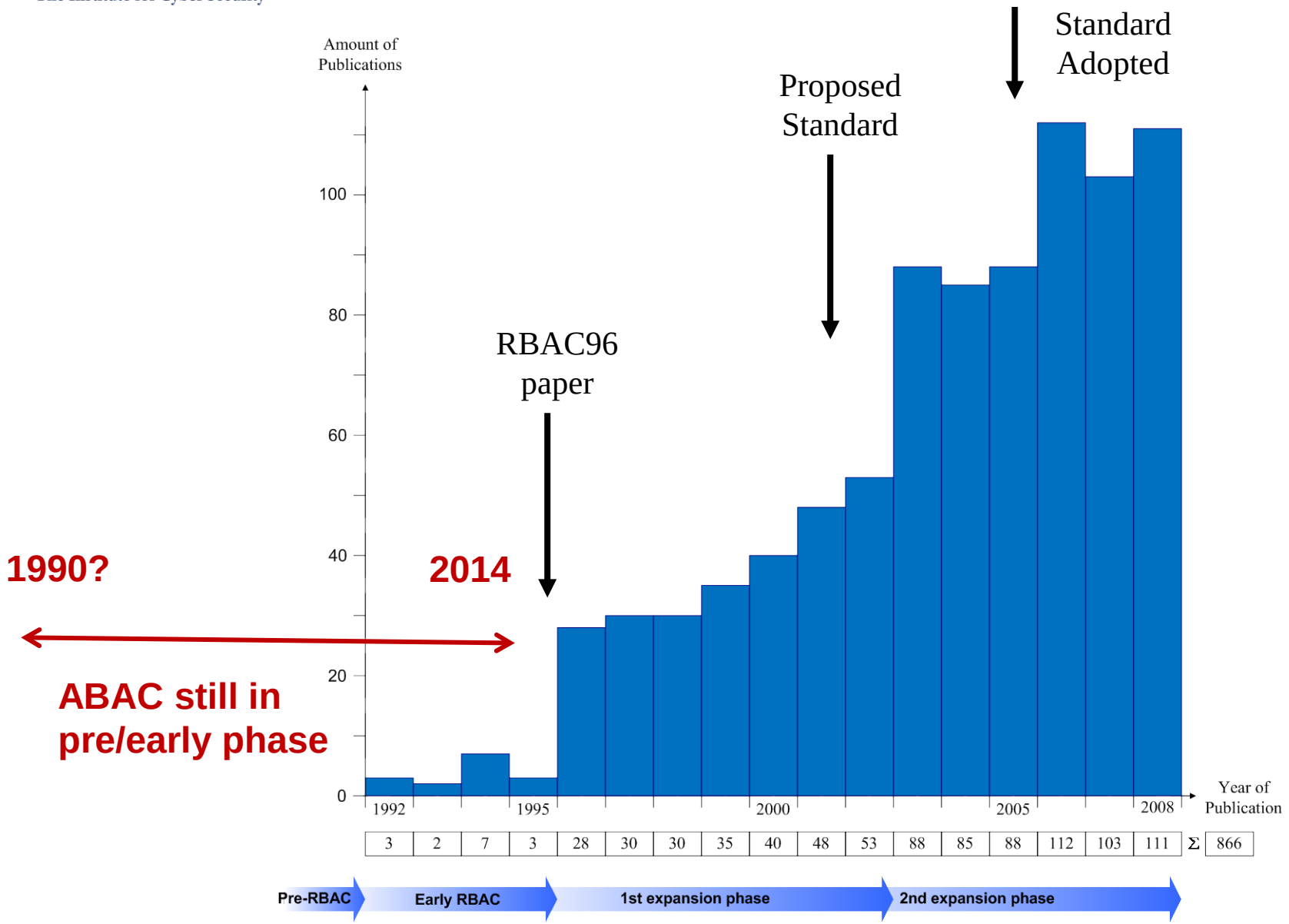
ABAC is not New



Usage Control
XACML
Attribute-Based Encryption

Mature Internet, 2000s

ABAC Status


Amount of Publications
Standard Adopted
Proposed Standard
RBAC96 paper
1990?
2014
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

Attribute-Based Access Control (ABAC)

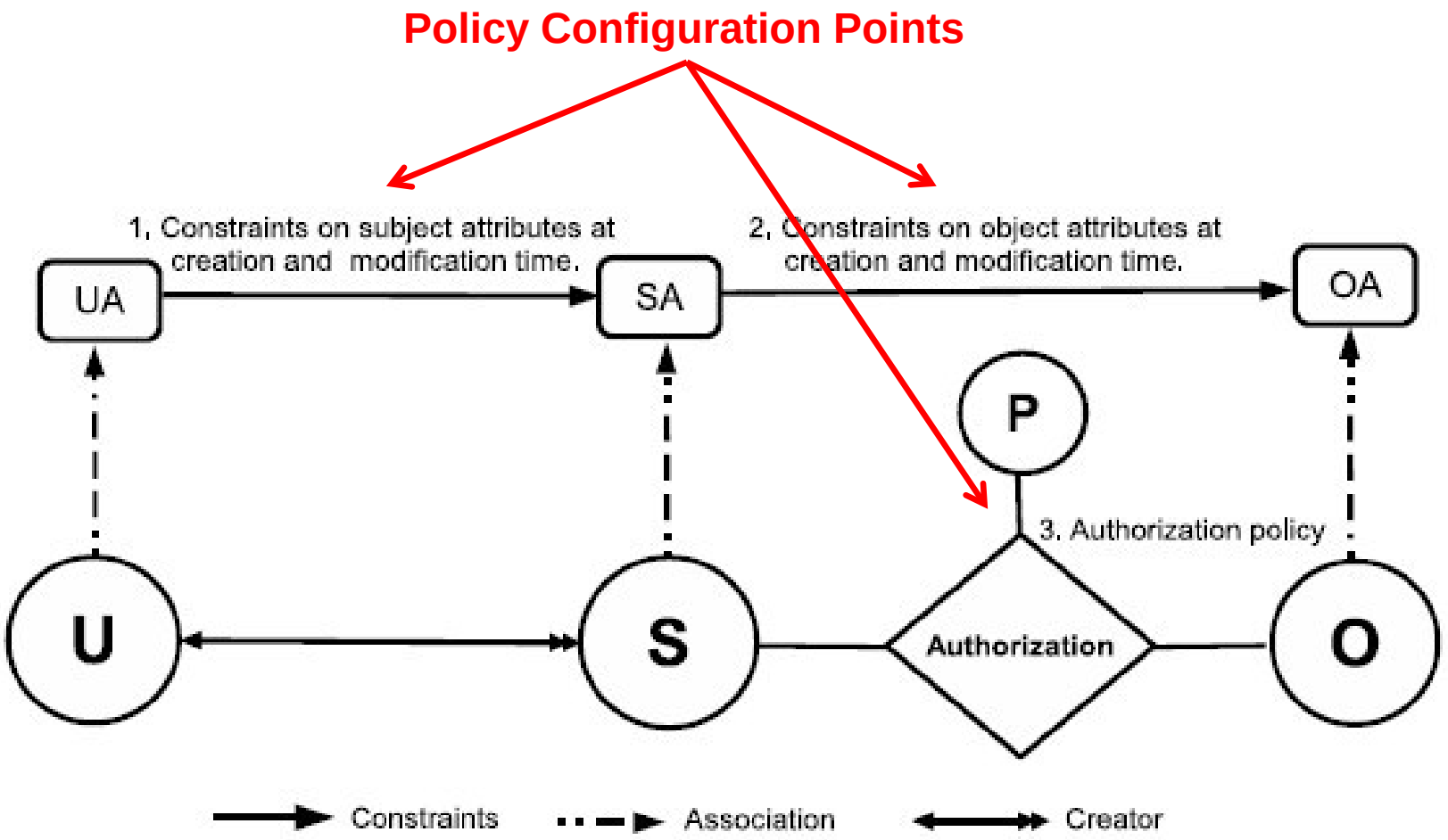
- Attributes are name:value pairs
  - possibly chained
  - values can be complex data structures
- Associated with
  - actions
  - users
  - subjects
  - objects
  - contexts
  - policies
- Converted by policies into rights just in time
  - policies specified by security architects
  - attributes maintained by security administrators
  - but also possibly by users OR reputation and trust mechanisms
- Inherently extensible

ABACα Hypothesis (DBSEC 2012)

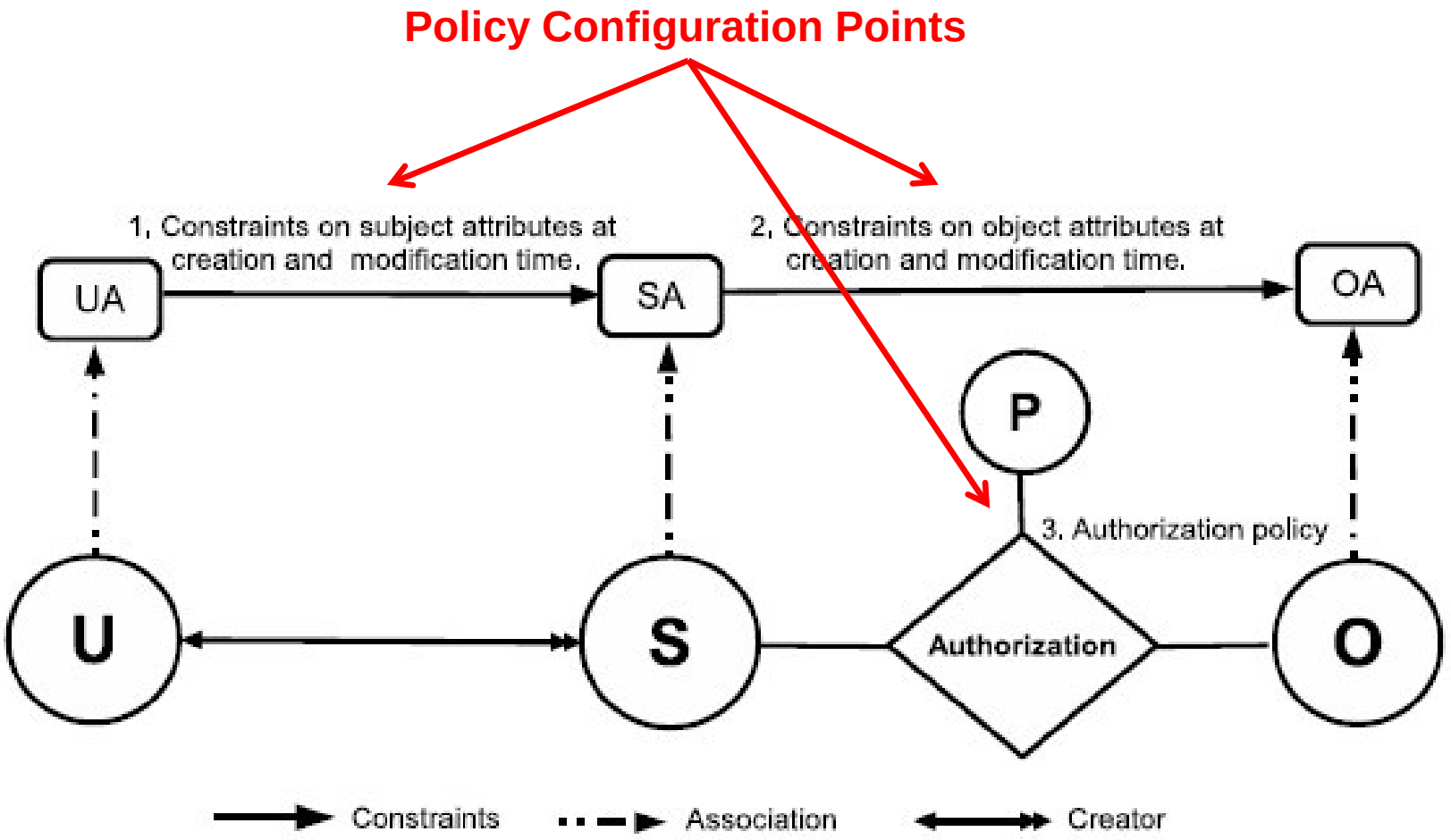
- An ABAC model requires
  - identification of policy configuration points (PCPs)
  - languages and formalisms for each PCP
- A core set of PCPs can be discovered by building the ABACα model to unify simple forms of DAC, MAC and RBAC
- Additional ABAC models can then be developed by
  - increasing the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

A small but crucial first step

ABACα Model Structure

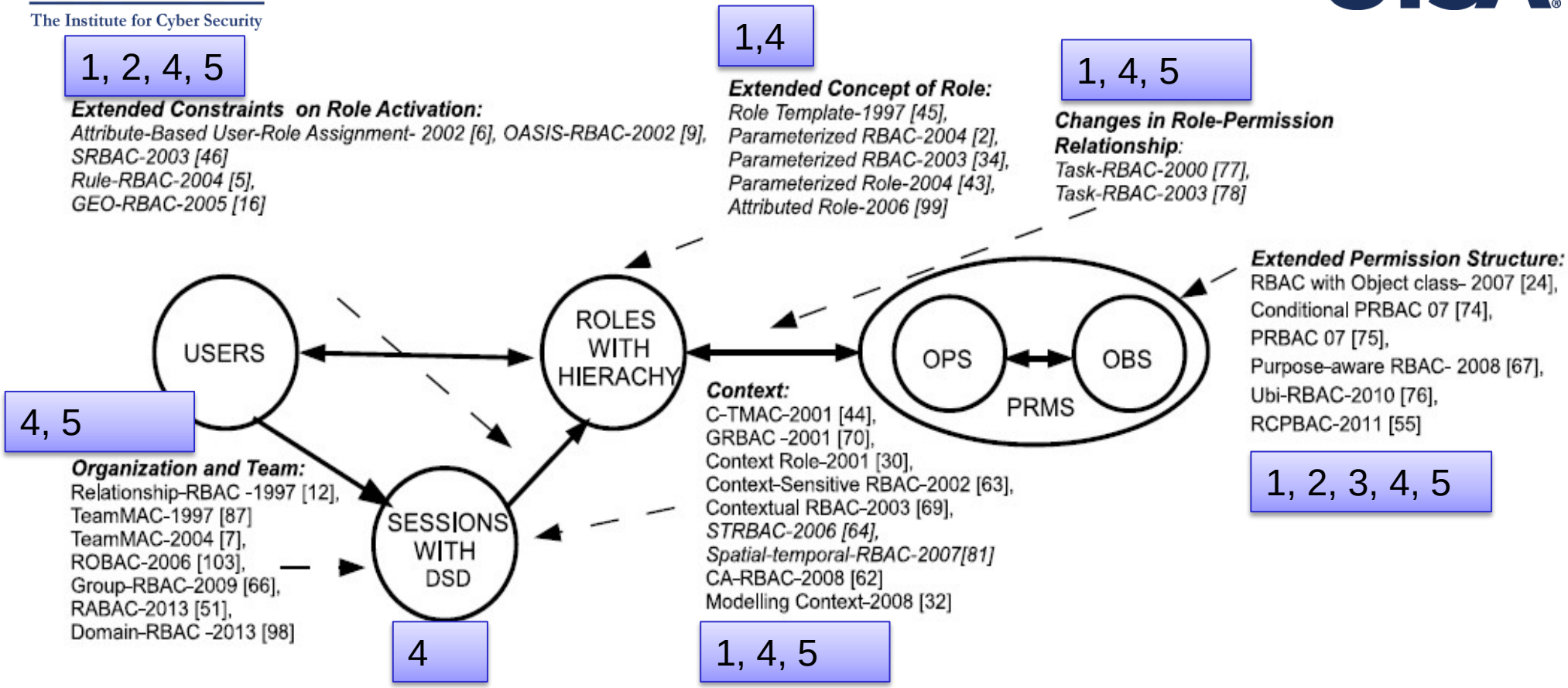


ABACα Model Structure



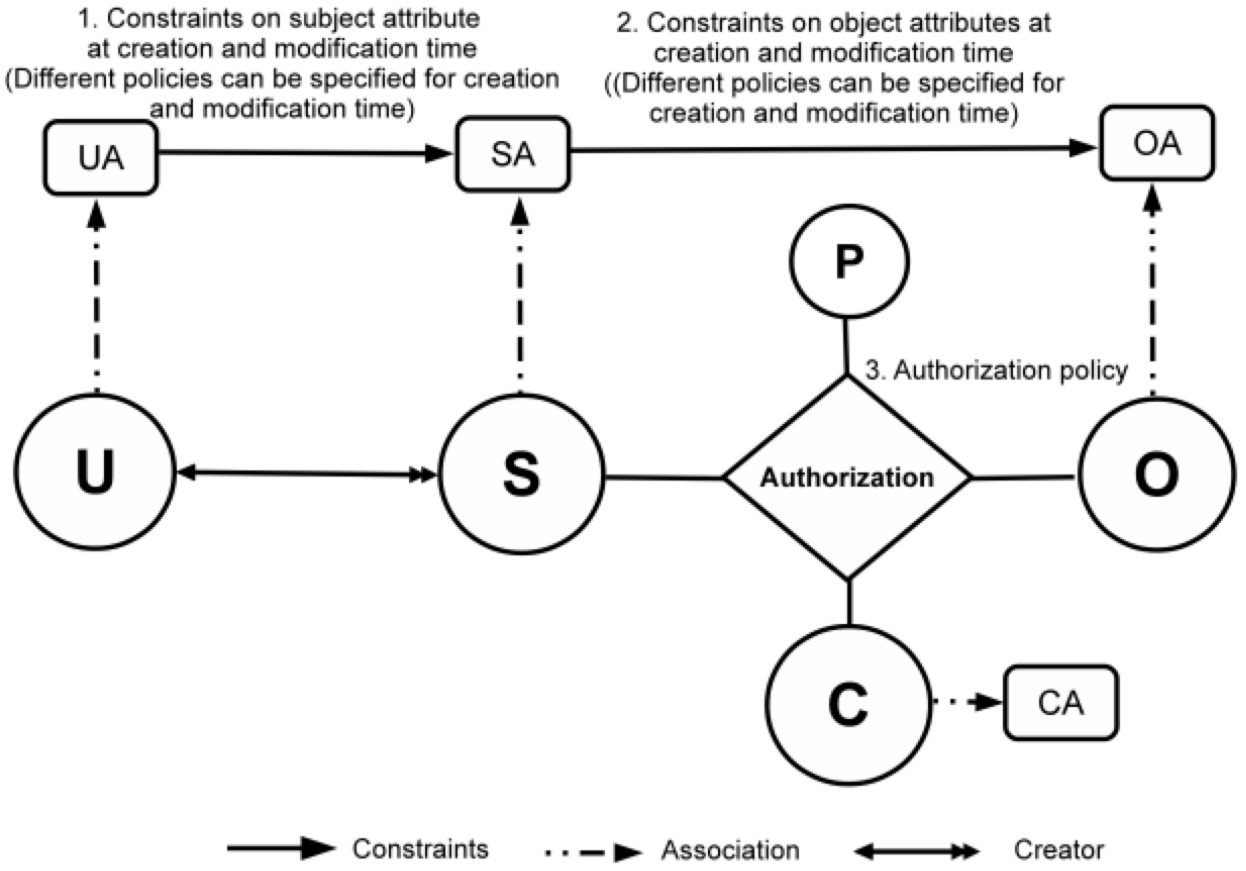
Can be configured to do DAC, MAC, RBAC

ABAC$_\beta$ Scope

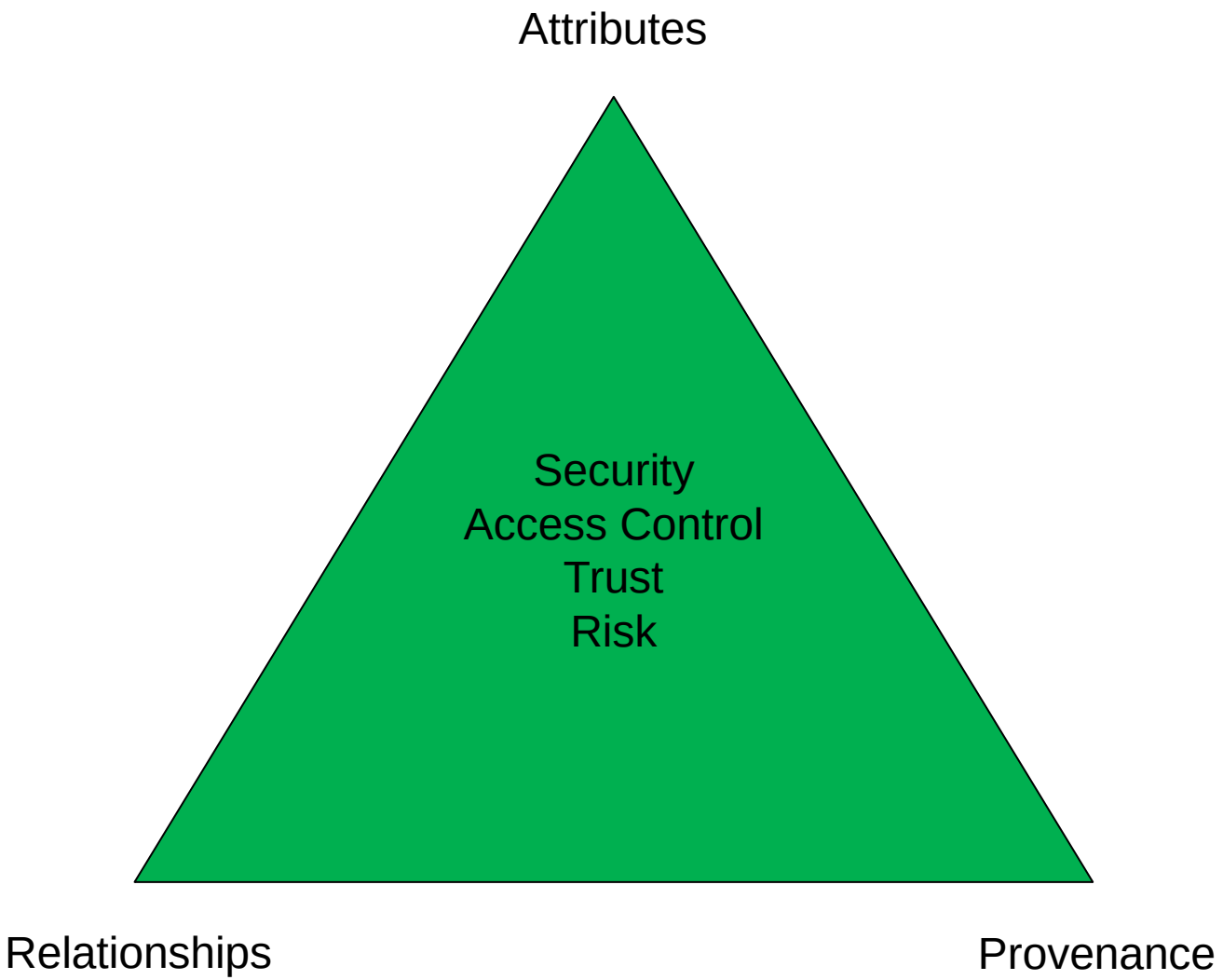


1. Context Attributes
2. Subject attribute constraints policy are different at creation and modification time.
3. Subject attributes constrained by attributes of subjects created by the same user.
4. Policy Language
5. Meta-Attributes

ABAC$_\beta$ Model



Beyond ABAC



ABAC Research at ICS

- 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