A Unified Attribute-Based Access Control Model Covering DAC, MAC and RBAC

Prof. Ravi Sandhu
Executive Director and Endowed Chair

DBSEC
July 11, 2012

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

Joint paper with Xin Jin and Ram Krishnan of UTSA

Attribute-Based Access Control (ABAC)

- 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

Yet Another Access Control Model!!

- Why another model?
- Why now?
- Why ABAC?
- Why ABACα (unifying DAC, MAC and RBAC)?

Access Control Status

- Dozens of models proposed and studied. Only three winners (meaningful practical traction)
  - DAC: Discretionary Access Control, 1970
  - MAC: Mandatory Access Control, 1970
  - RBAC: Role-Based Access Control, 1995
- RBAC emerged at an inflection point due to dissatisfaction with the then dominant DAC and MAC
  - We are currently at another inflection point due to dissatisfaction with the now dominant RBAC
  - ABAC (Attribute-Based Access Control) has emerged as the prime candidate to be the next dominant paradigm

RBAC Overall Assessment

- 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?

ABAC Prior Work Includes

- 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 ……..

Yet Another Access Control Model!!

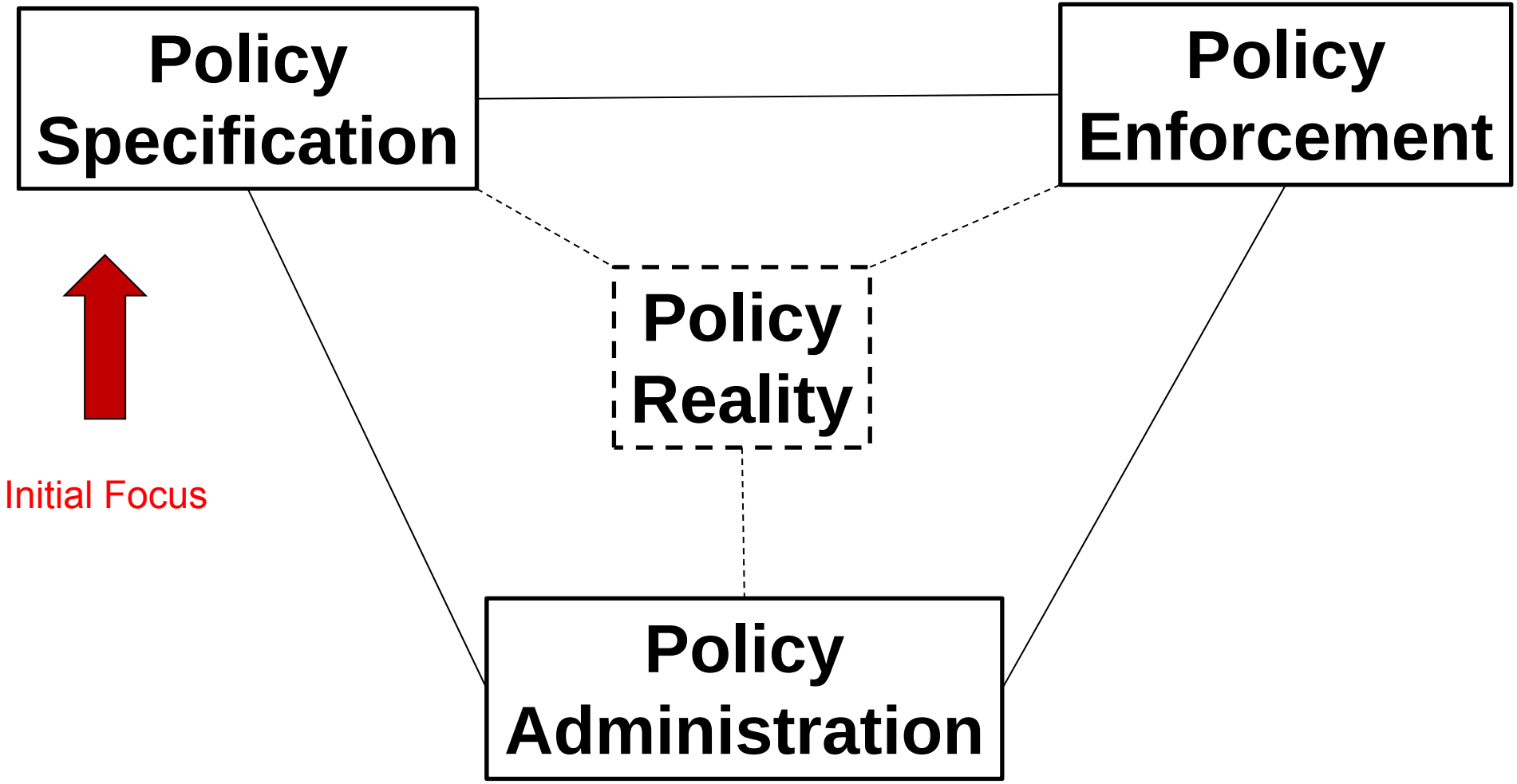
- Why another model?
- Why now?
- Why ABAC?
- Why ABACα (unifying DAC, MAC and RBAC)?

How the Dominant Access Control Models got Built

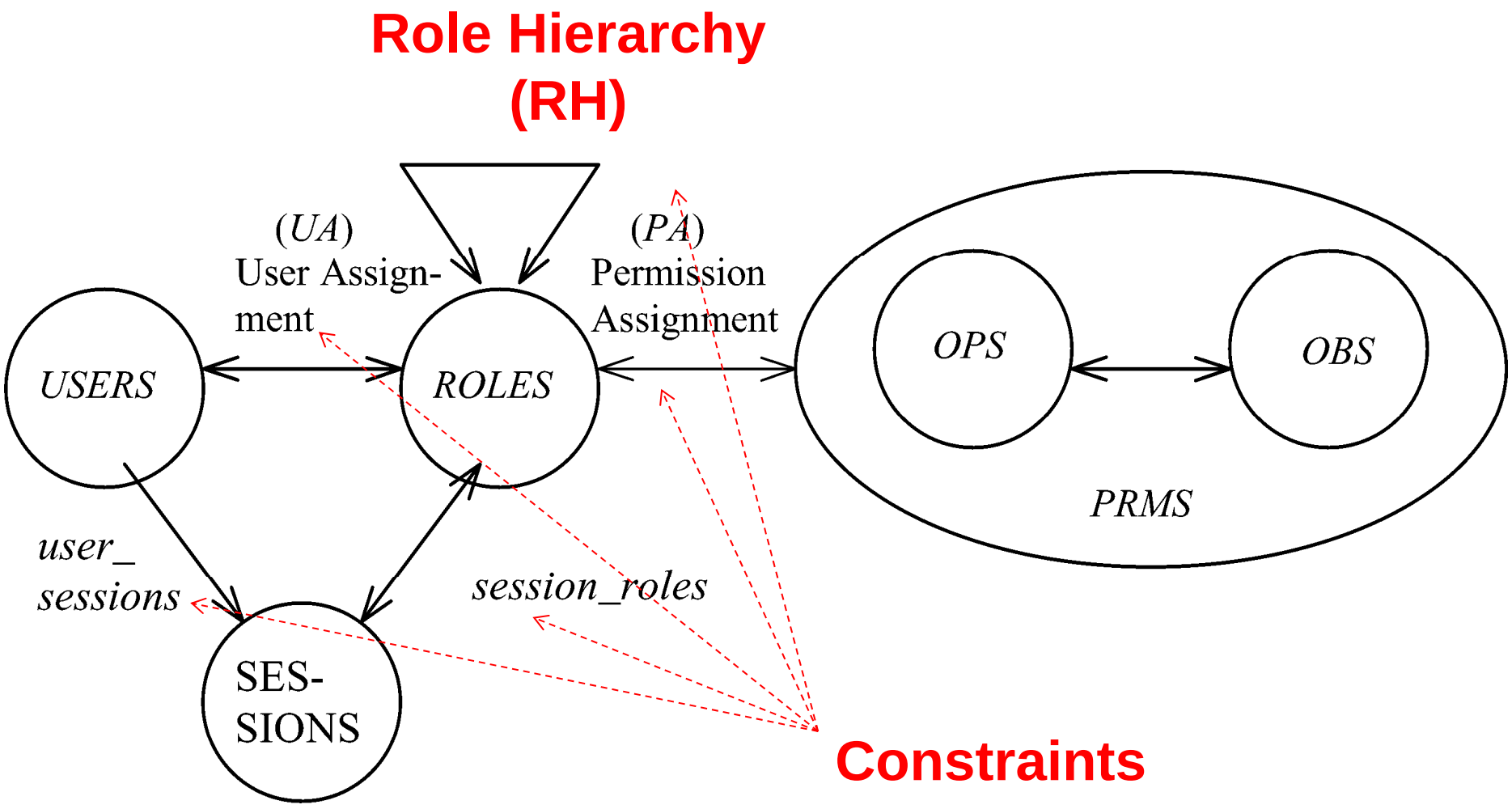
- DAC: Discretionary Access Control, 1970
  - Vendors and researchers coping for the first time with multi-user operating systems in different ways
  - Requirements abstracted from research organizations
- MAC: Mandatory Access Control, 1970
  - Requirements abstracted from established real world pre-computer military and national security policies
- RBAC: Role-Based Access Control, 1995
  - Requirements abstracted from established real world pre-computer policies common to commercial organizations
  - Vendor implementations of early RBAC-like systems

How do we build ABAC models?

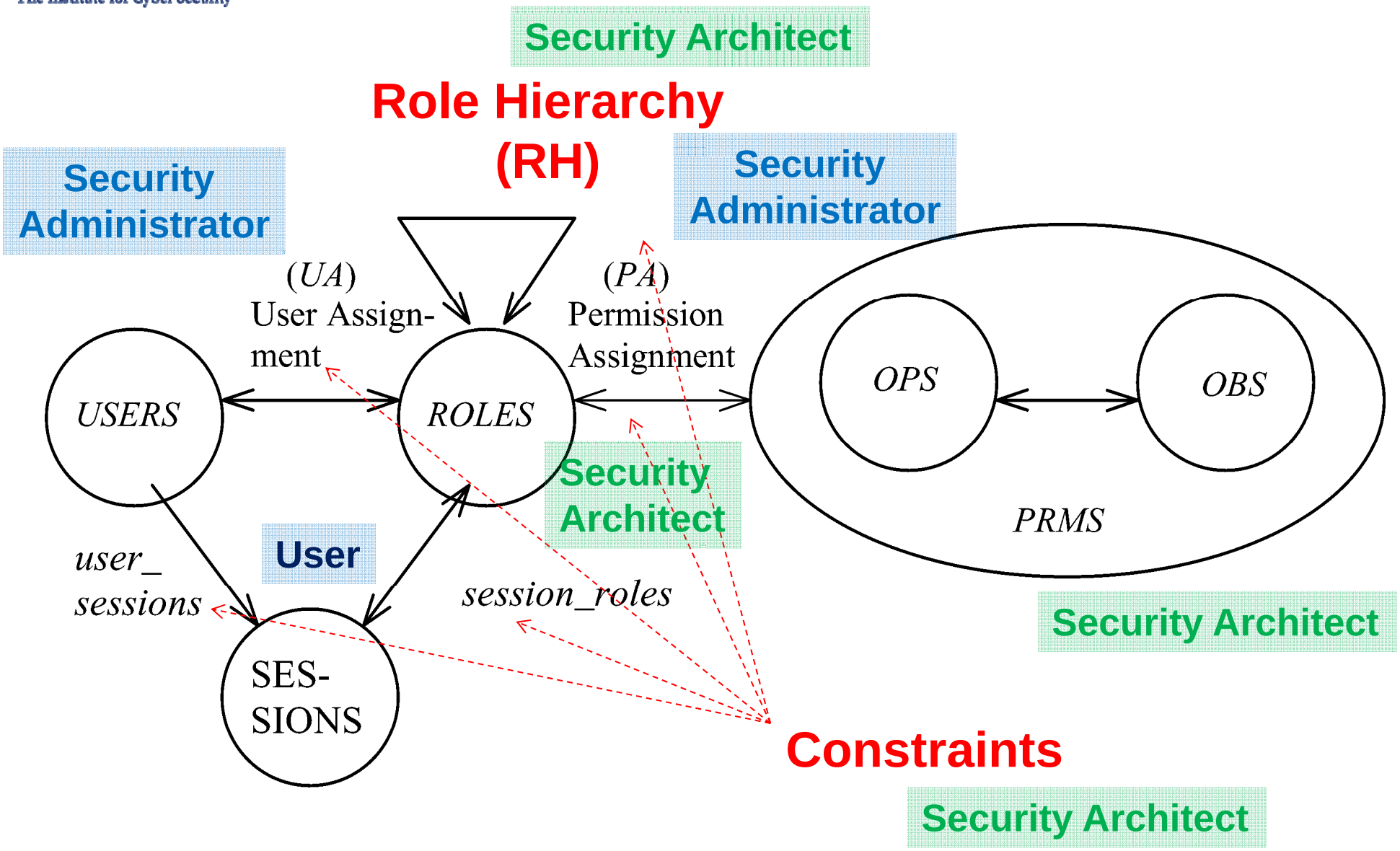
Access Control Models



RBAC Policy Configuration Points



RBAC Policy Configuration Points



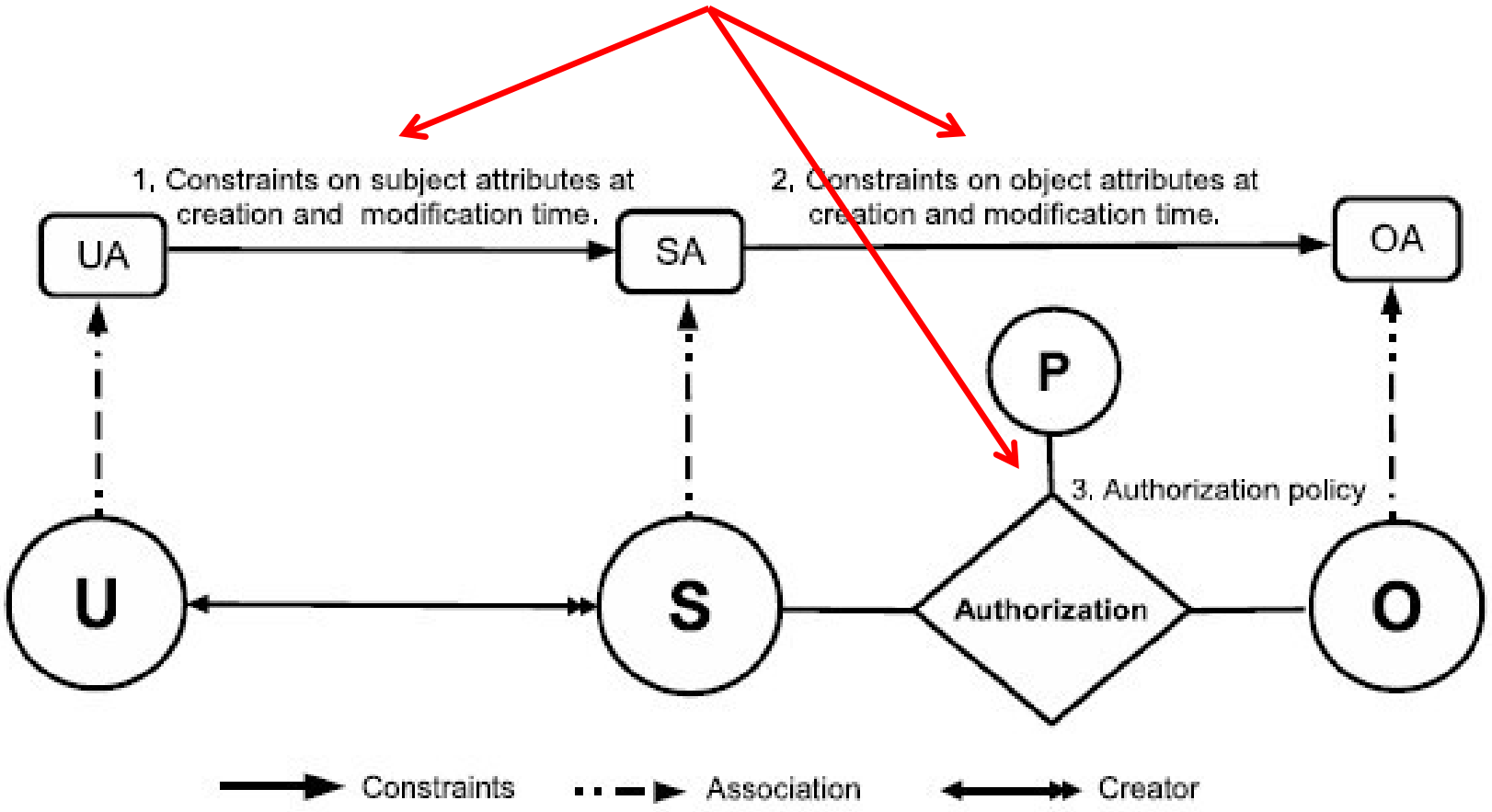
ABACα Hypothesis

- 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 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

ABACα Requirements

	Subject attribute value constrained by creating user ?	Object attribute value constrained by creating subject ?	Attribute range ordered?	Attribute function return set value?	Object attribute modification?	Subject attribute modification by creating user?
DAC	YES	YES	NO	YES	YES	NO
MAC	YES	YES	YES	NO	NO	NO
RBAC0	YES	NA	NO	YES	NA	YES
RBAC1	YES	NA	YES	YES	NA	YES
ABACα	YES	YES	YES	YES	YES	YES

ABACα Model Structure



Authorization Policy: LAuthorization

- 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

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

Subject Attribute Constraints; LConstrSub

- MAC $ConstrSub(u, s, \{(sclearance, value)\}) \equiv value \leq uclearance(u)$
- RBAC0 $ConstrSub(u, s, \{srole, value\}) \equiv value \subseteq urole(u)$
- RBAC1 $ConstrSub(u, s, \{srole, value\}) \equiv \forall r1 \in value. \exists r2 \in urole(u). r1 \leq r2$

Object Attribute Constraints

Constraints at creation: LConstrObj

- DAC $ConstrObj(s, o, \{(reader, val1), (writer, val2), (createdby, val3)\}) \equiv val3 = SubCreator(s)$
- MAC $ConstrObj(s, o, \{sensitivity, value\}) \equiv sclearance(s) \leq value$

Constraints at modification: LConstrObjMod

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

ABACα Model Structure