I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

Access Control Evolution and Prospects

Ravi Sandhu
Executive Director

Professor of Computer Science
Lutcher Brown Chair in Cyber Security

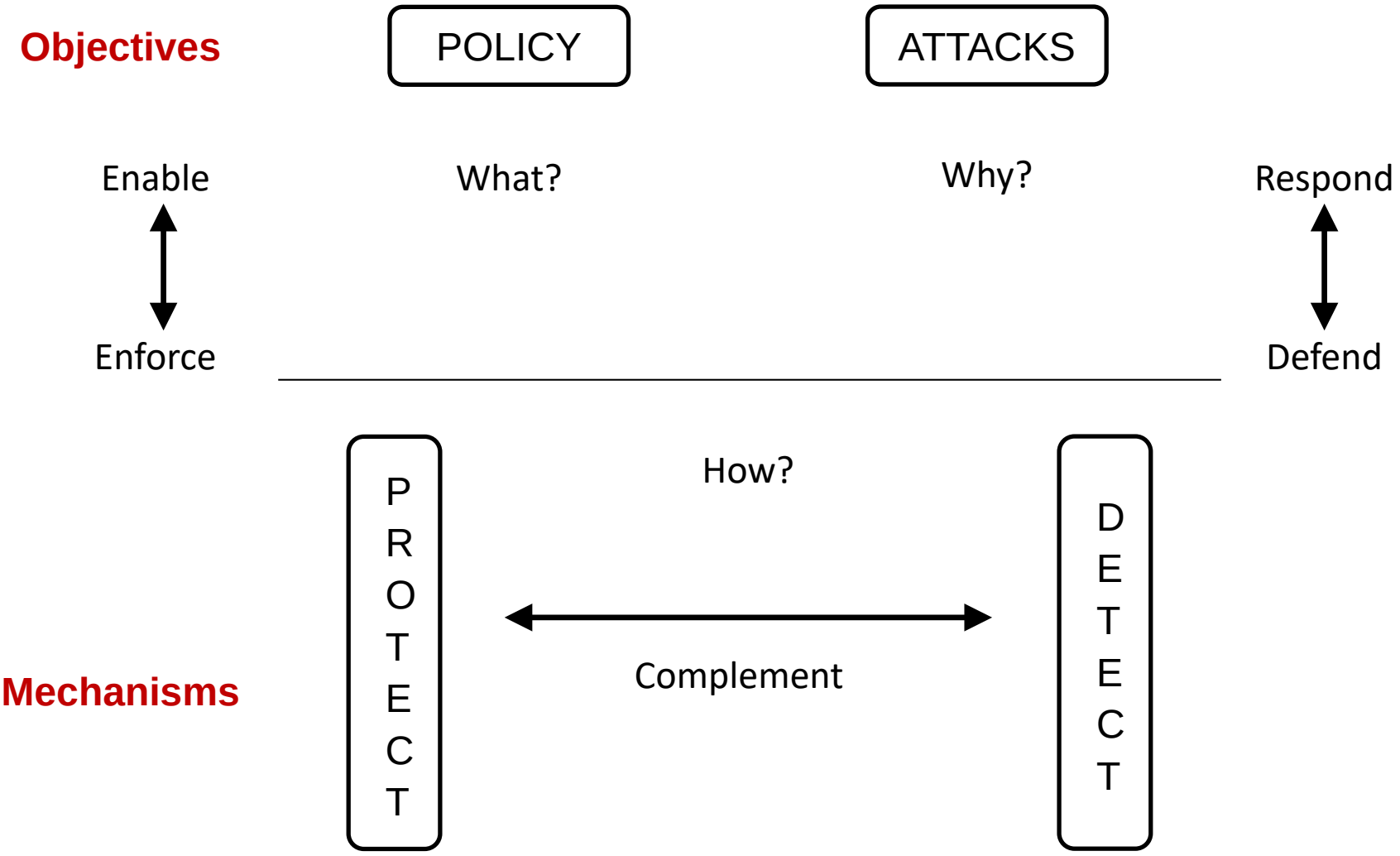
June 2019

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

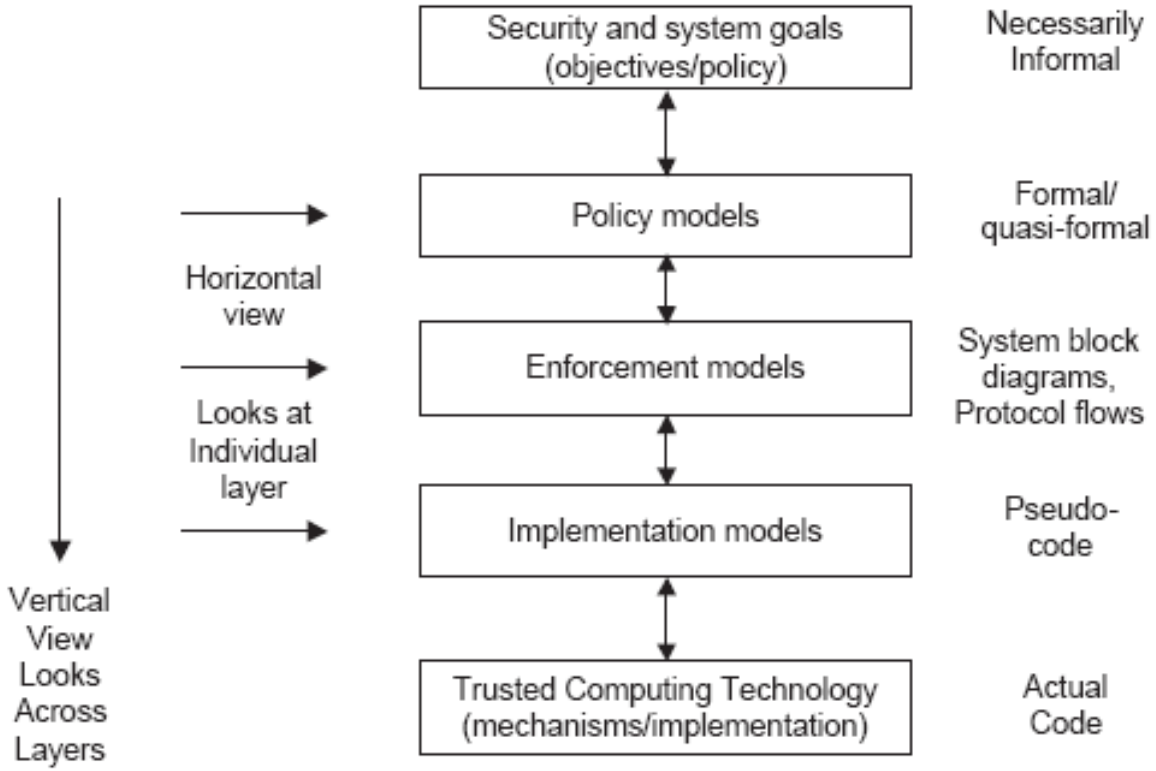
World-Leading Research with Real-World Impact!

UTSA Computer Science

Holistic Cyber Security



Access Control PEI Layers



Idealized

Enforceable (Approximate)

Codeable

Access Control Fundamental Limits

- Copy control
- Inference
- Trusting humans vs trusting software
- Trusted computing base vulnerabilities
- Side channels and covert channels

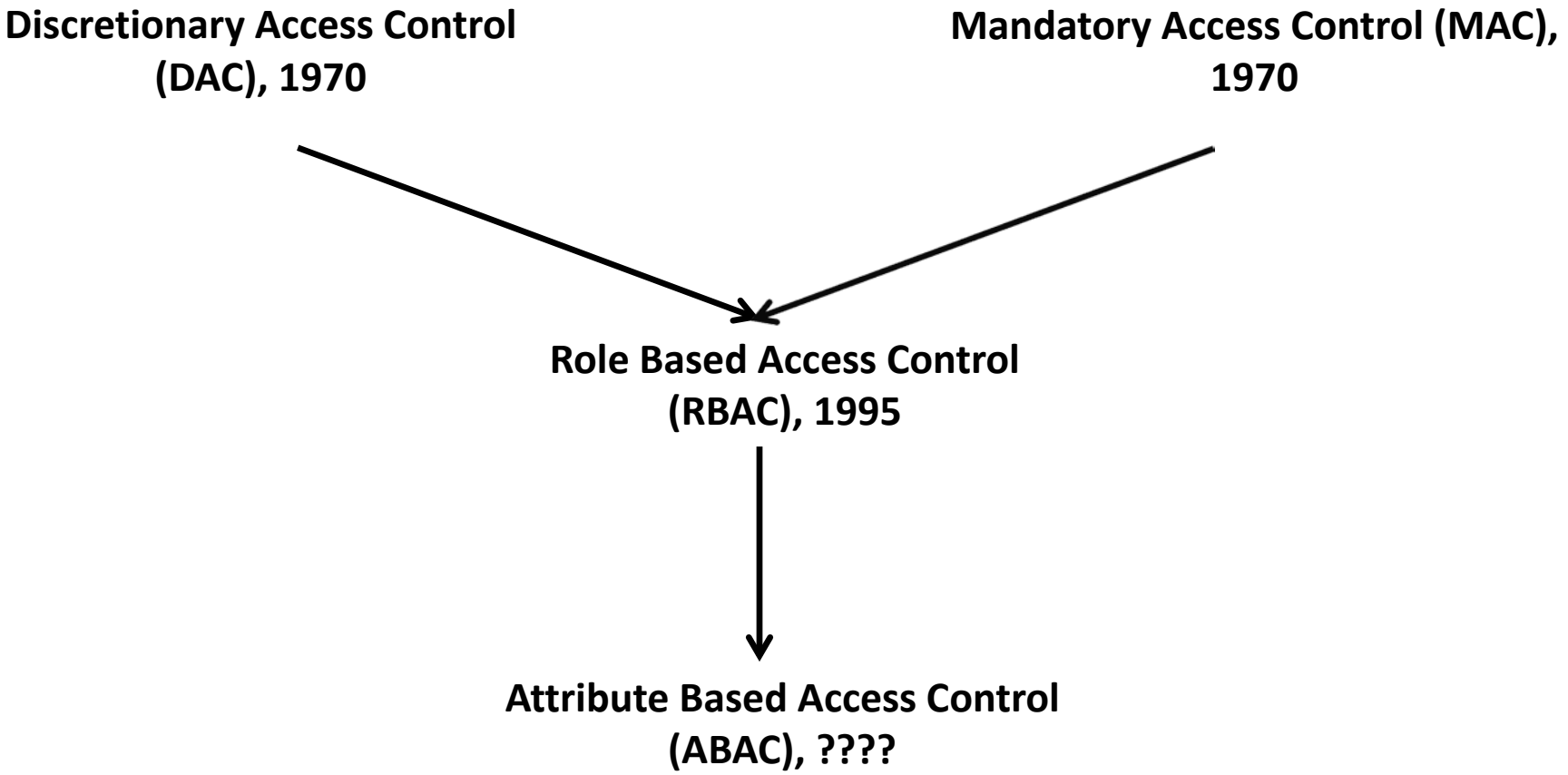
Cryptography

Symmetric Key Cryptography, 1977

Asymmetric Key Cryptography, 1996

BlockChain Applications, ????

Access Control



Discretionary Access Control (DAC)

- Core concept:

  Custodian of information determines access

- Core drawback:

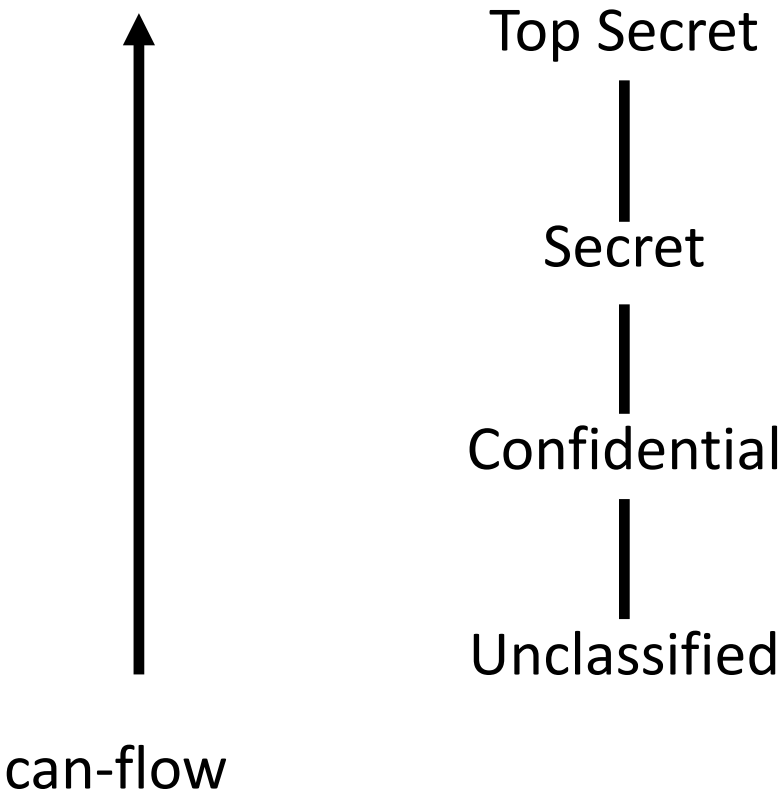
  Does not protect copies
  Therefore OK for integrity but not for confidentiality

- Sophistication:

  Delegation of custody

  Denials or negative rights

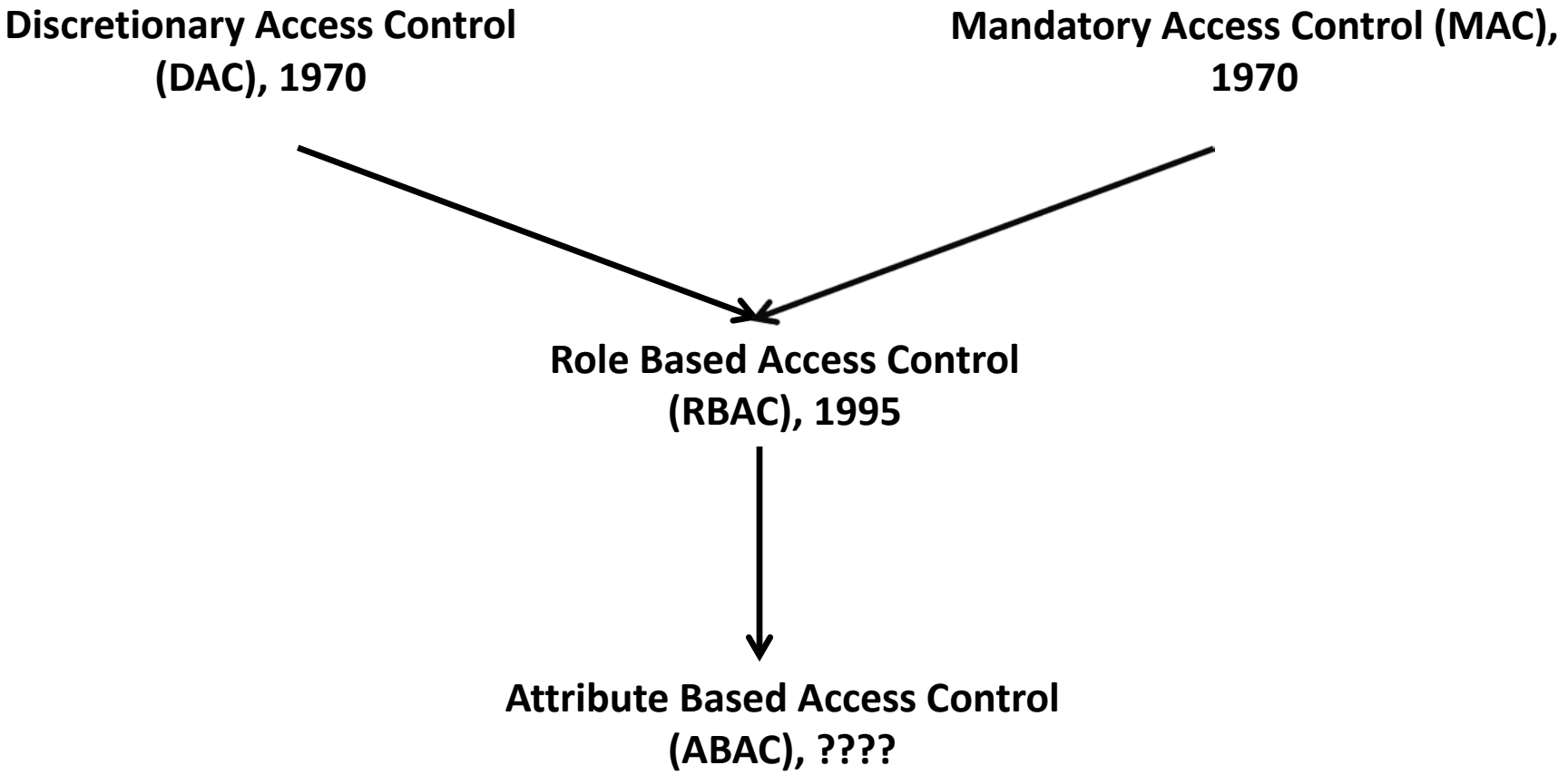
Mandatory Access Control (MAC)



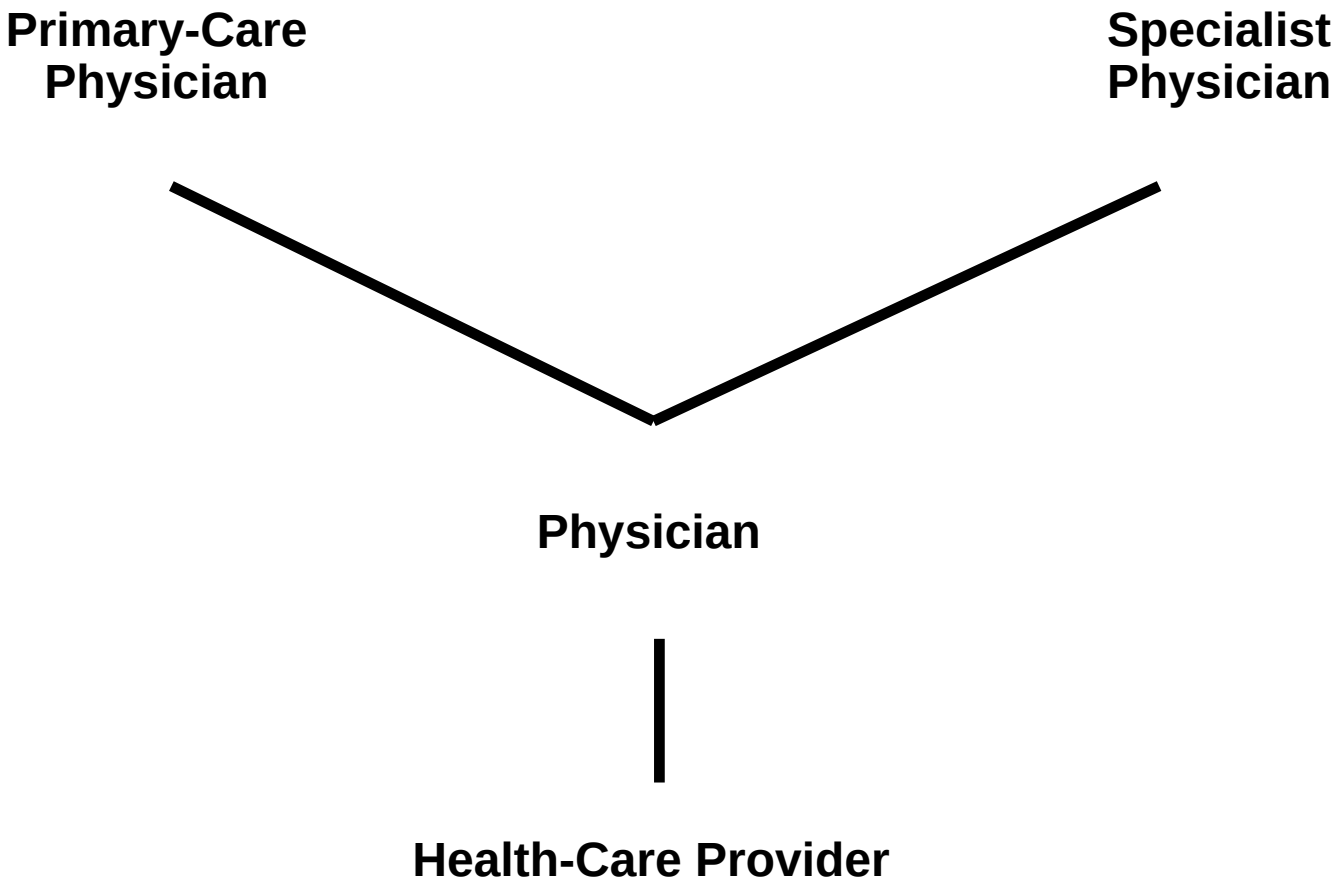
Mandatory Access Control (MAC)

- Core concept:
  - Extend control to copies by means of security labels
- Core drawback:
  - Covert/side channels enable copies that bypass this control
  - Inference not prevented
  - Too strict
- Sophistication:
  - Dynamic labels

Access Control



Role-Based Access Control (RBAC)



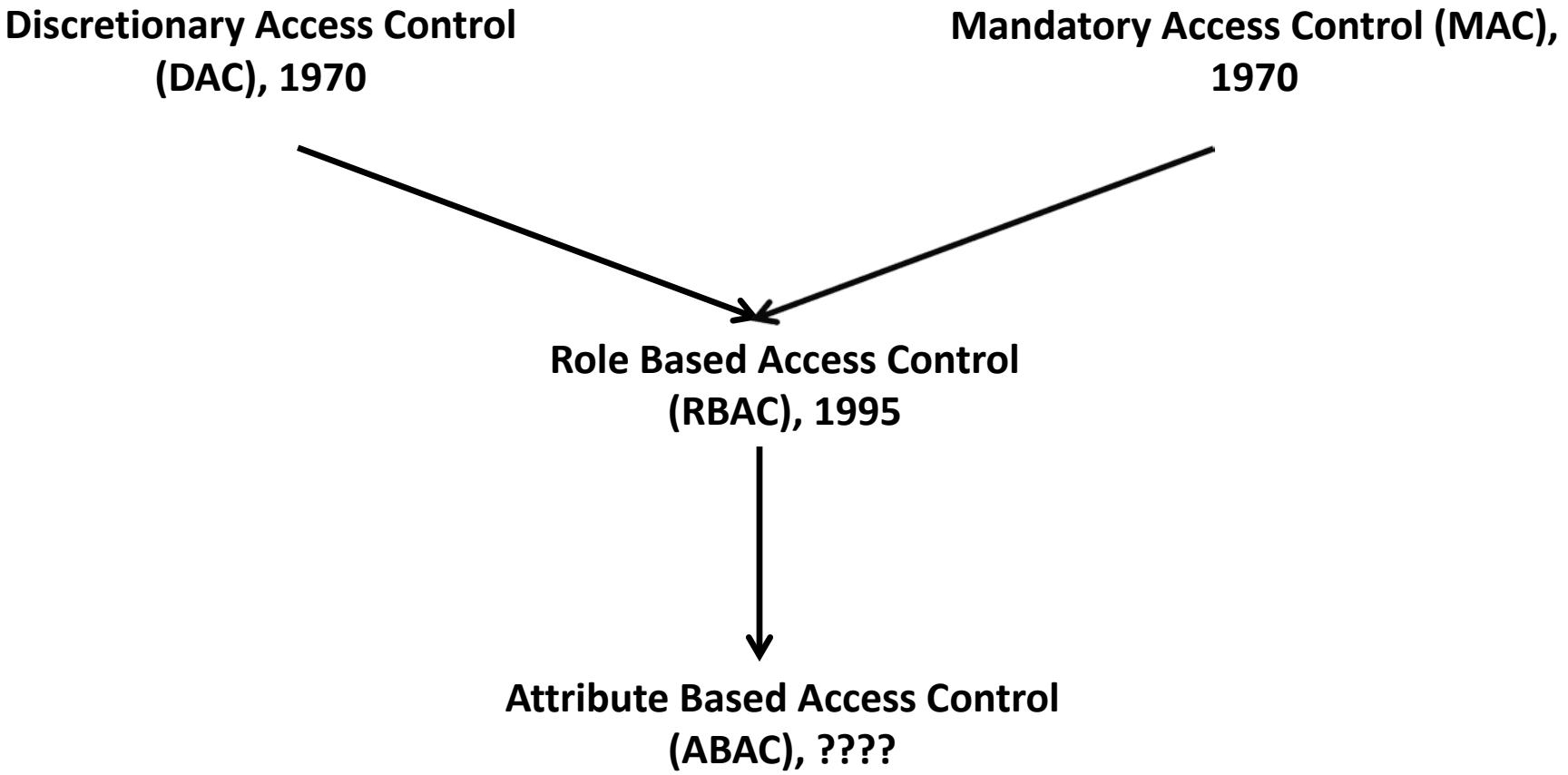
Role-Based Access Control (RBAC)

- Core concept:
  - Roles determine everything
- Core drawback:
  - Roles are a natural concept for human users
  - But not so natural for:
  - Information objects
  - IoT things
  - Contextual attributes
- Sophistication:
  - Role hierarchies
  - Role constraints

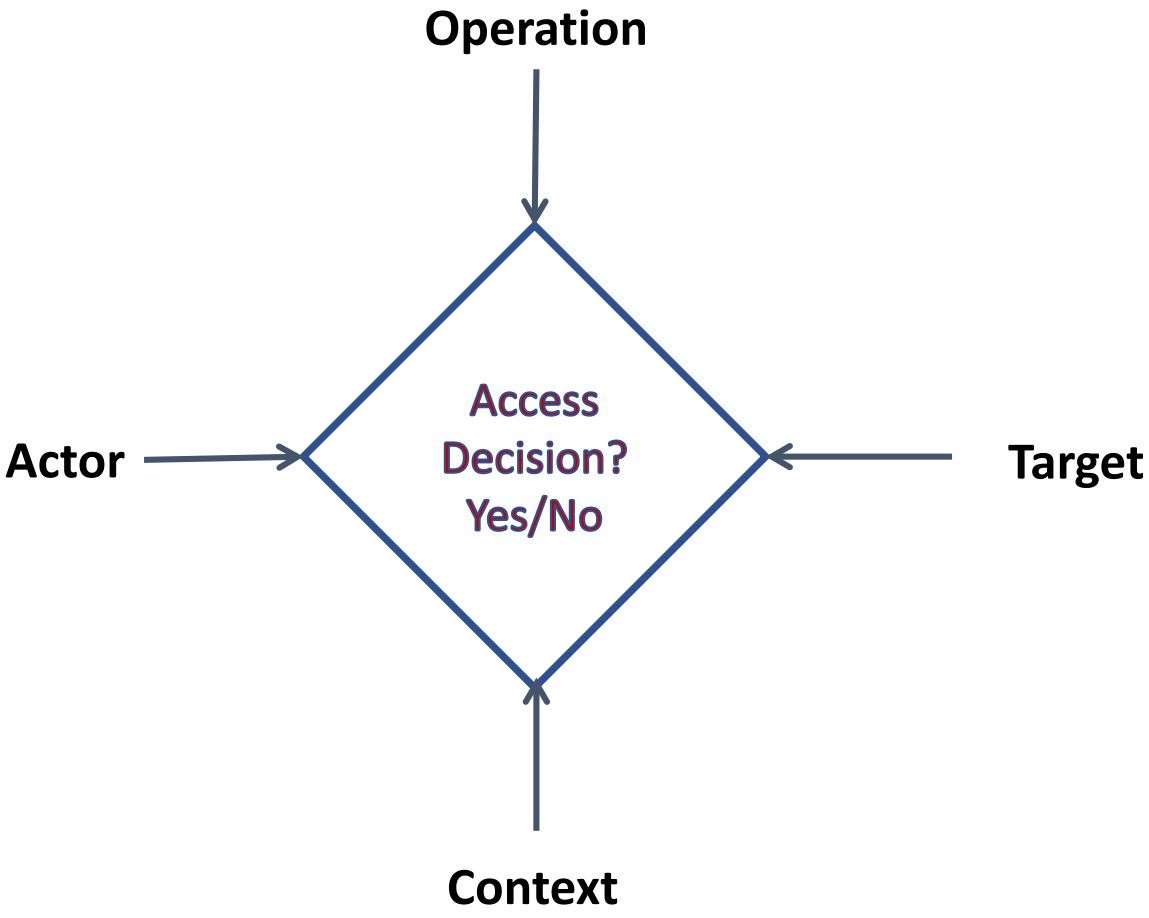
Role-Based Access Control (RBAC)

- Fundamental theorem of RBAC:
  - RBAC can be configured to do DAC
  - RBAC can be configured to do MAC

Access Control



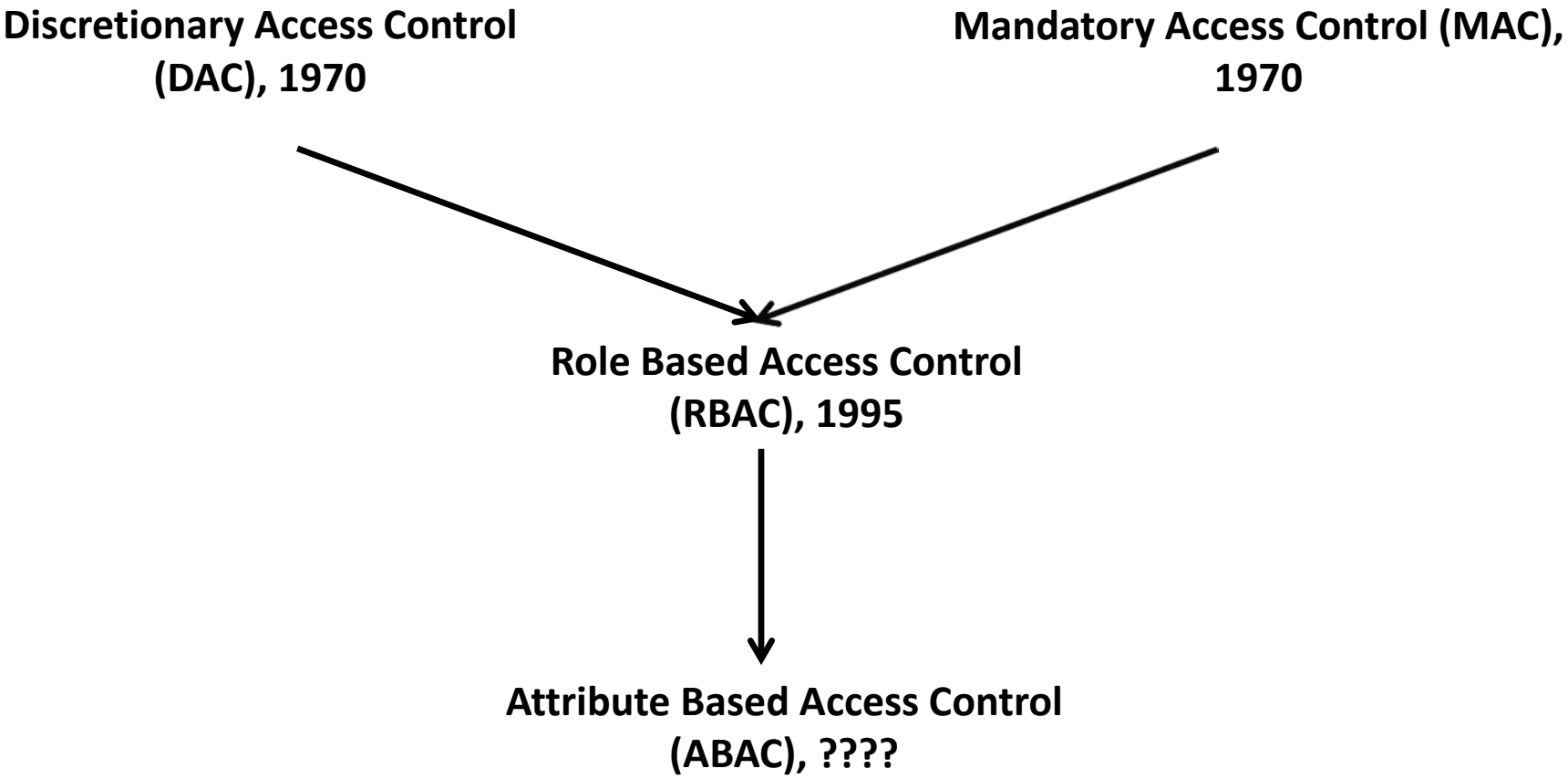
Attribute-Based Access Control (ABAC)



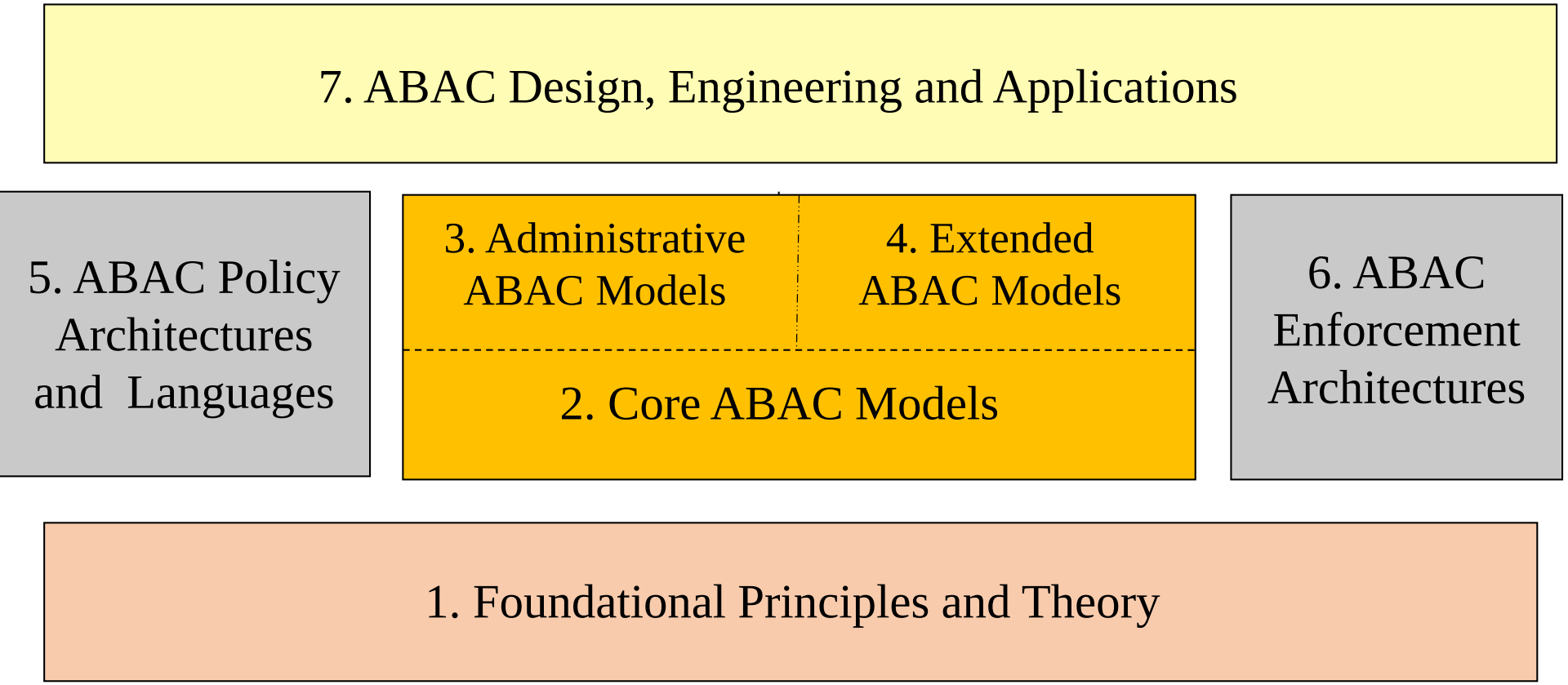
Attribute-Based Access Control (ABAC)

- Core concept:
  - Attributes determine everything
- Core drawback:
  - Flexibility at the cost of complexity
  - No fixed access decision rule
- Sophistication:
  - Chained attributes
  - Group attributes
  - Distributed decision rules
  - Automation
  - Adaptation

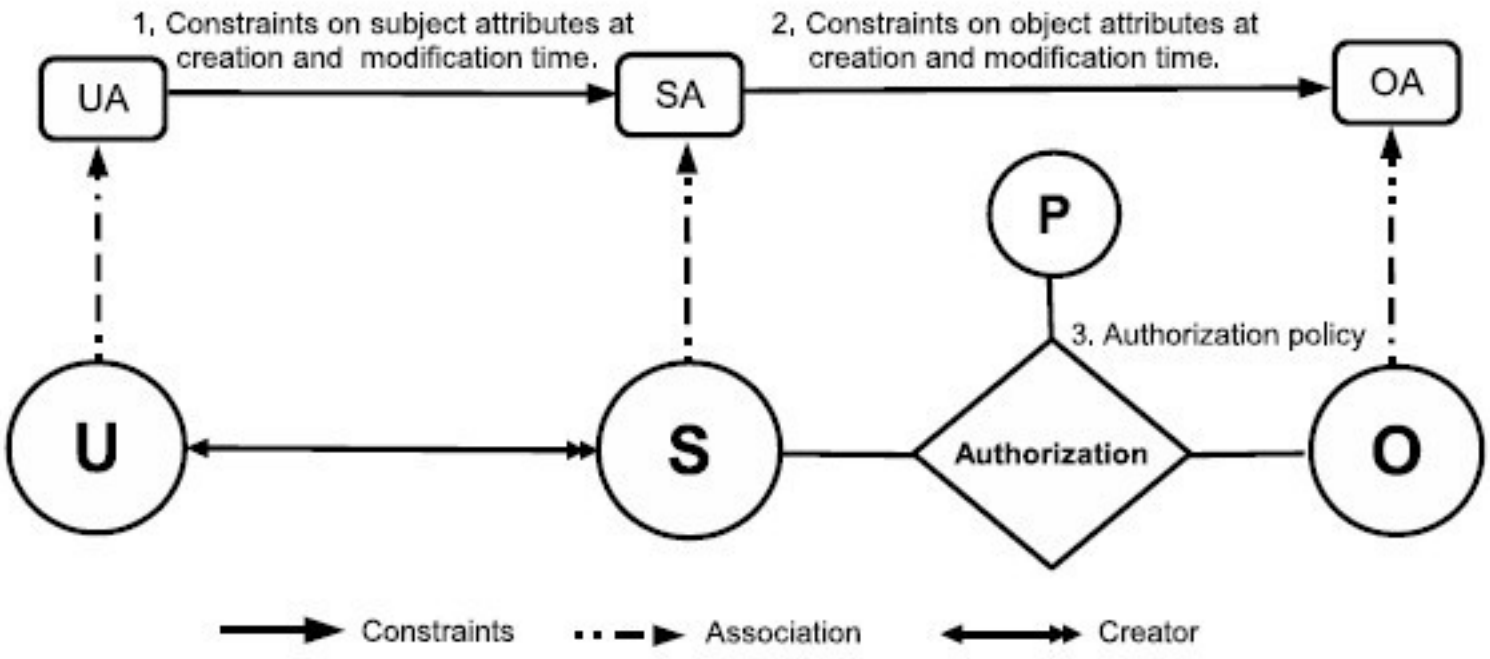
Access Control



ABAC Research Space



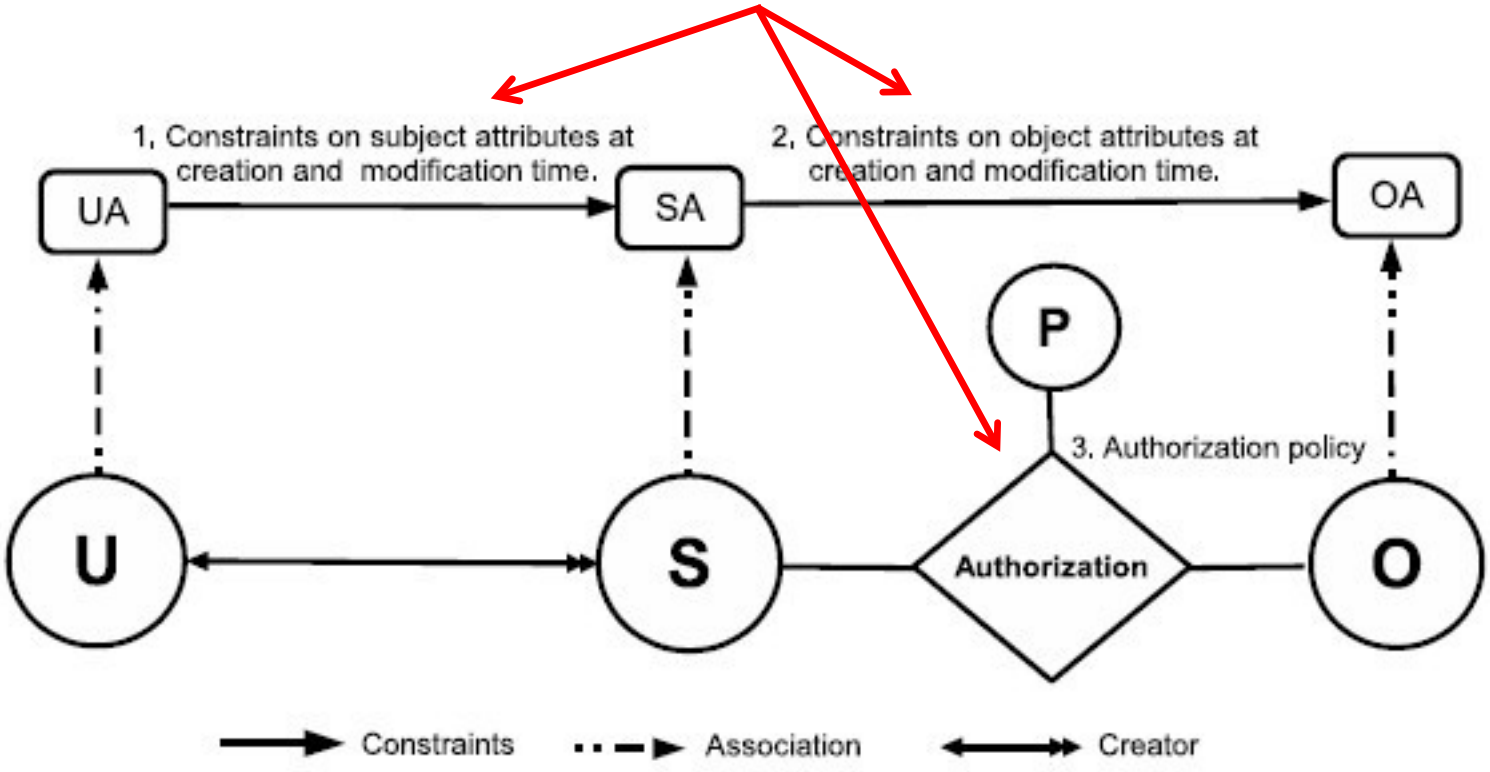
Core ABAC Models: $ABAC_{\alpha}$



Can be configured to do simple forms of DAC, MAC, RBAC (Jin, Krishnan, Sandhu 2012)

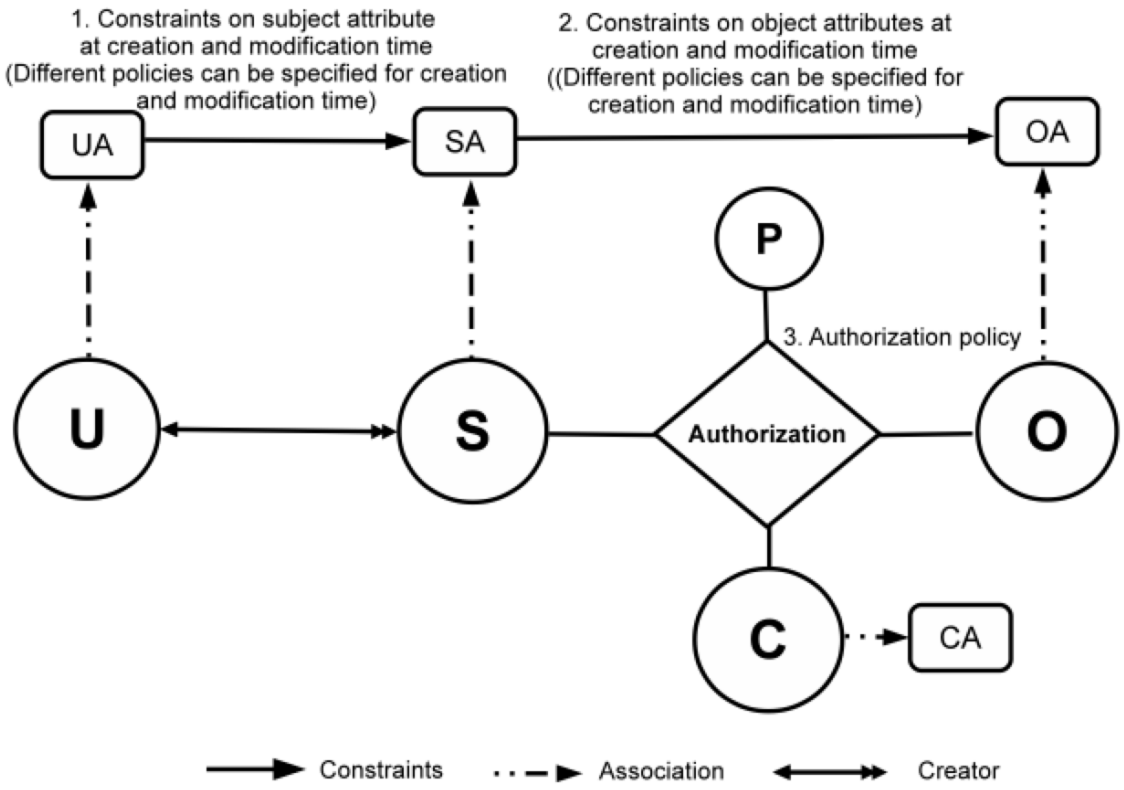
Core ABAC Models: $ABAC_{\alpha}$

Policy Configuration Points



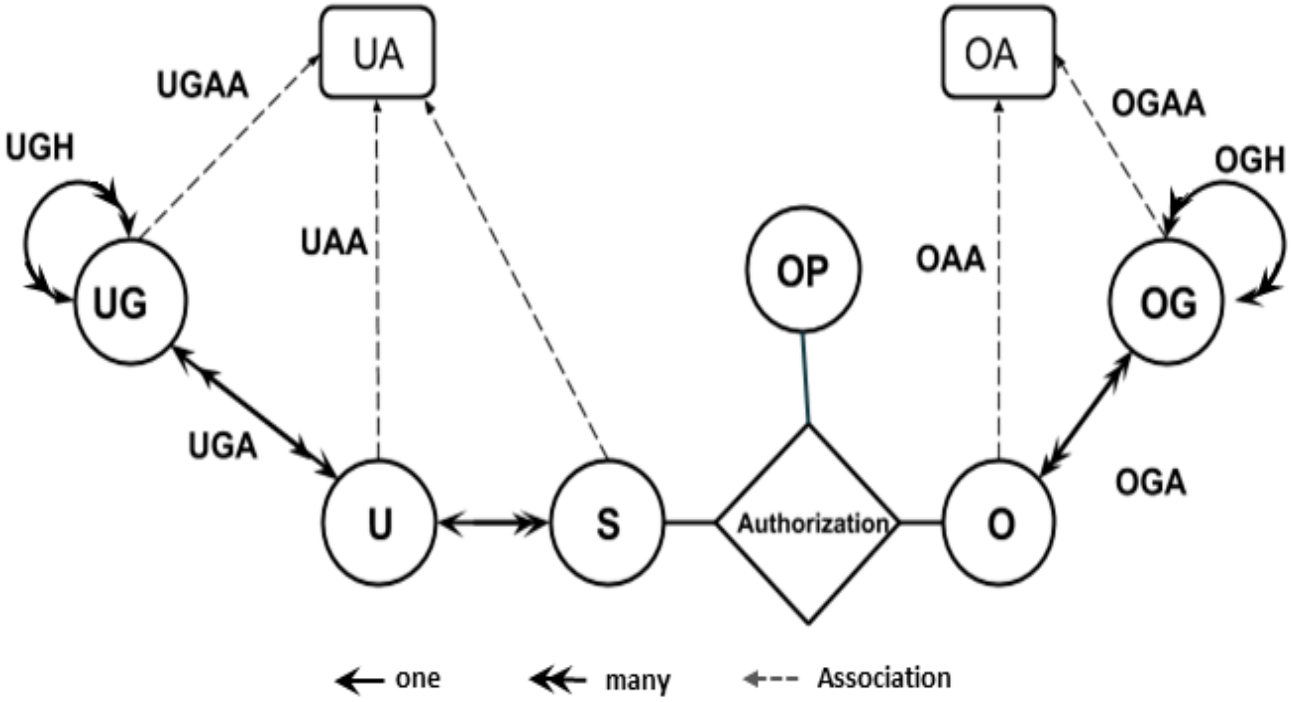
Can be configured to do simple forms of DAC, MAC, RBAC (Jin, Krishnan, Sandhu 2012)

Core ABAC Models: $ABAC_\beta$



Can further be configured to do many RBAC extensions (Jin, Krishnan, Sandhu 2014)

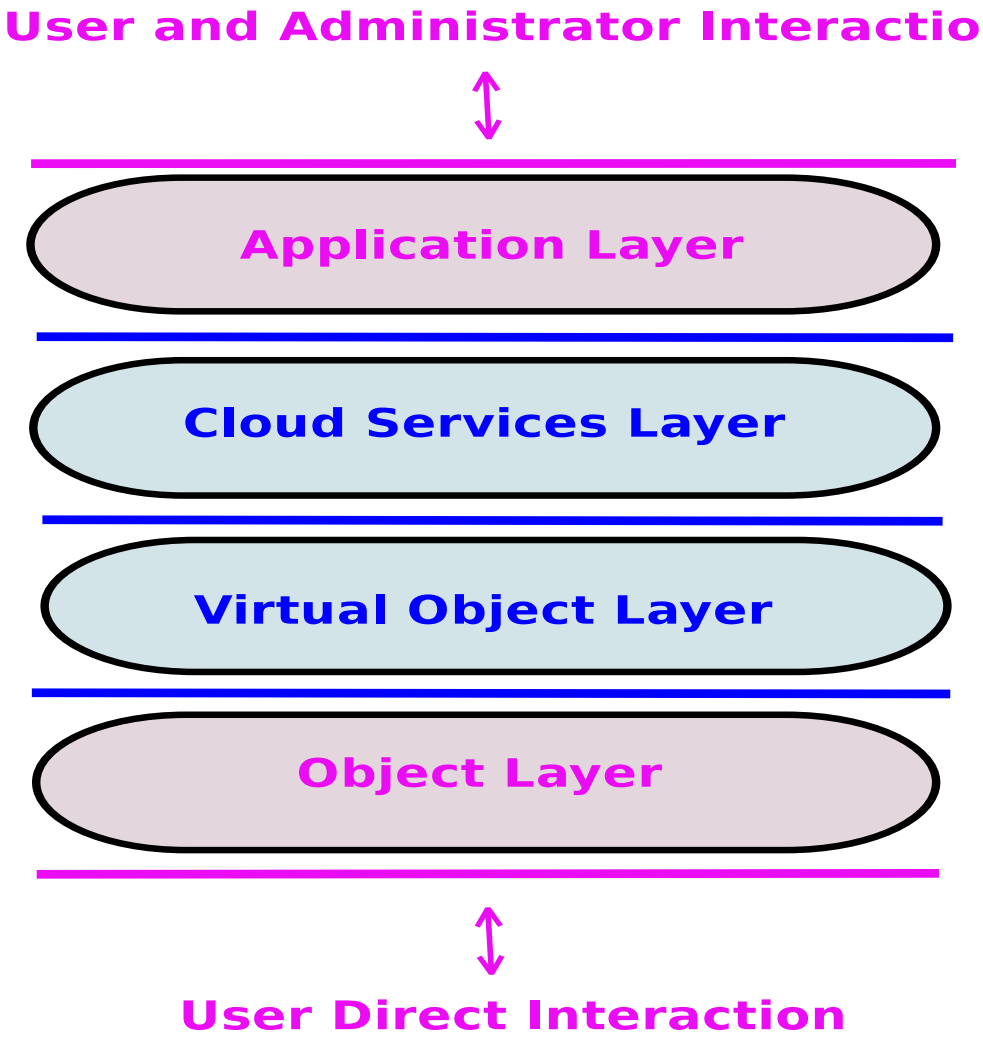
Administrative ABAC Models: HGABAC



- Hierarchical Group and Attribute Based Access Control (HGABAC)
  - Introduces User and Object Groups
  - Simplifies administration of attributes

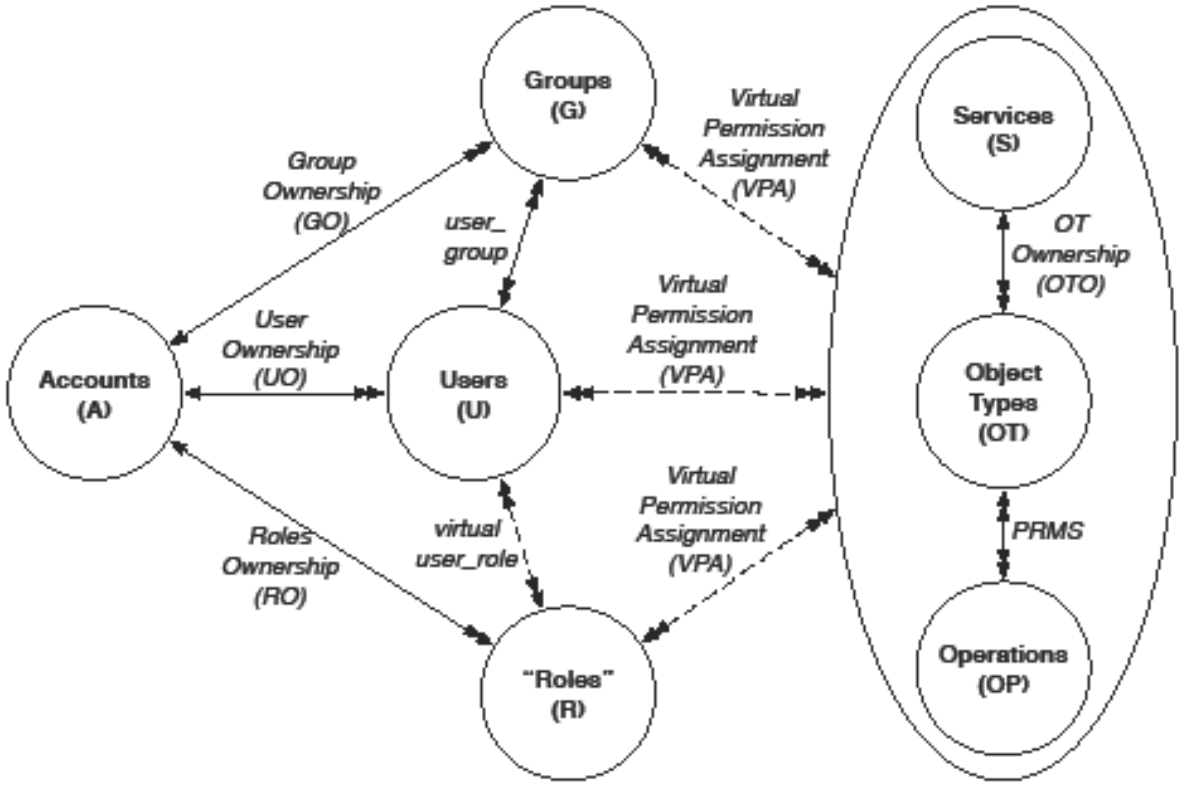
Servos and Osborn, 2015

ABAC Applications: Cloud Enabled IoT



Alsheri, Bhatt, Patwa, Benson, Sandhu 2016 onwards

Policy Architecture: Amazon AWS style



ABAC Research Space

* 7. ABAC Design, Engineering and Applications

* 5. ABAC Policy Architectures and Languages

3. Administrative * ABAC Models

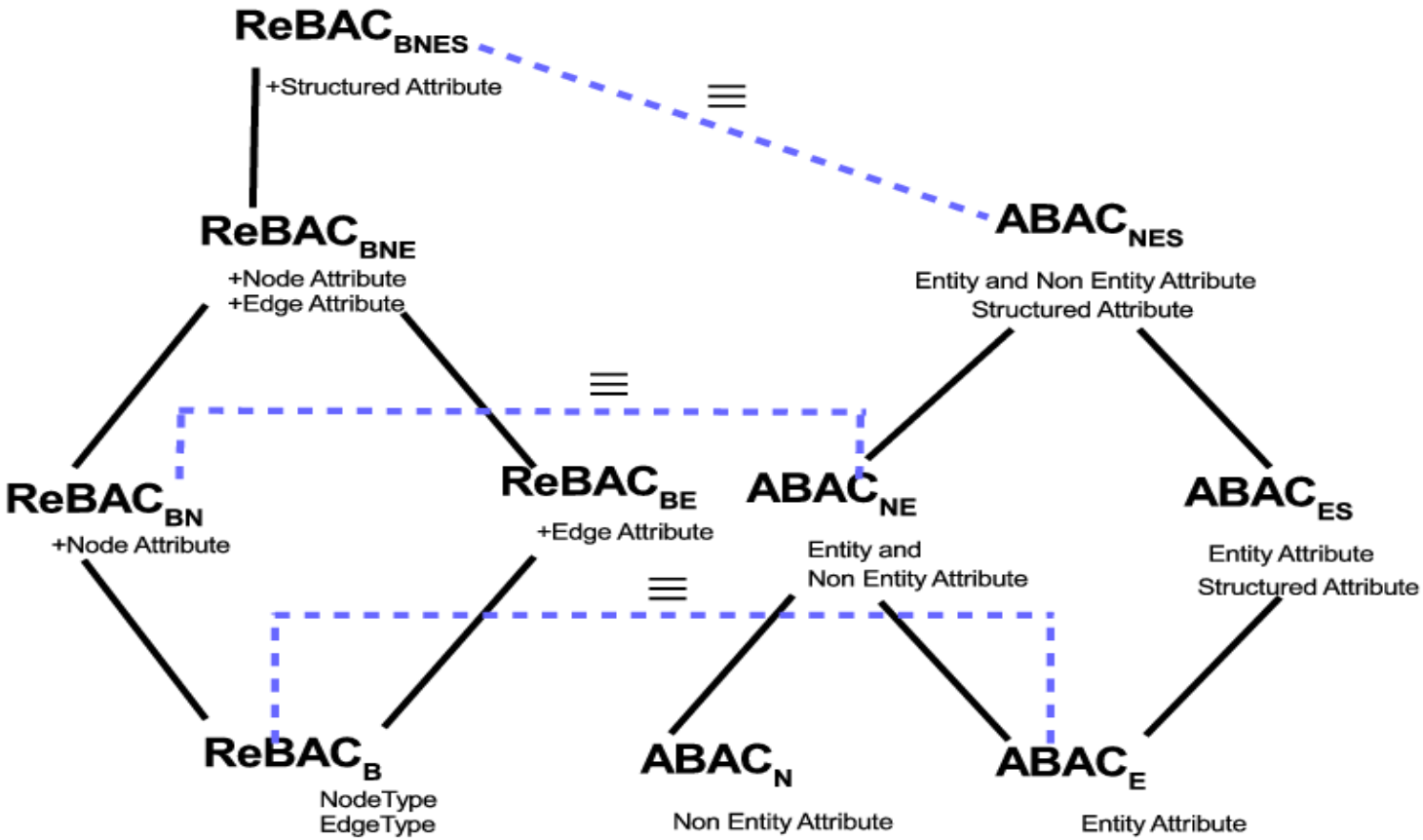
4. Extended ABAC Models

* 2. Core ABAC Models

6. ABAC Enforcement Architectures

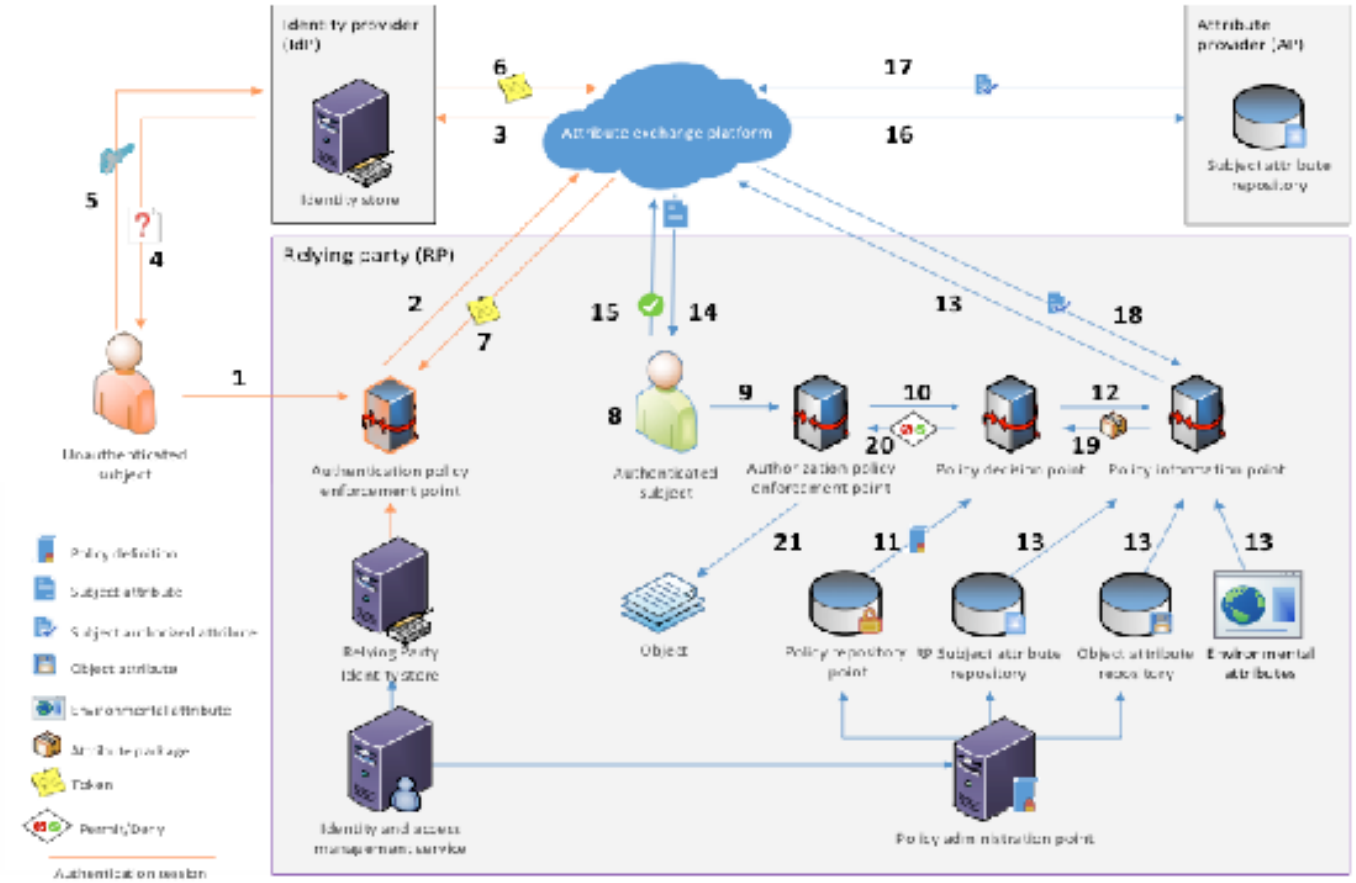
1. Foundational Principles and Theory

Extended ABAC Models: ReBAC versus ABAC



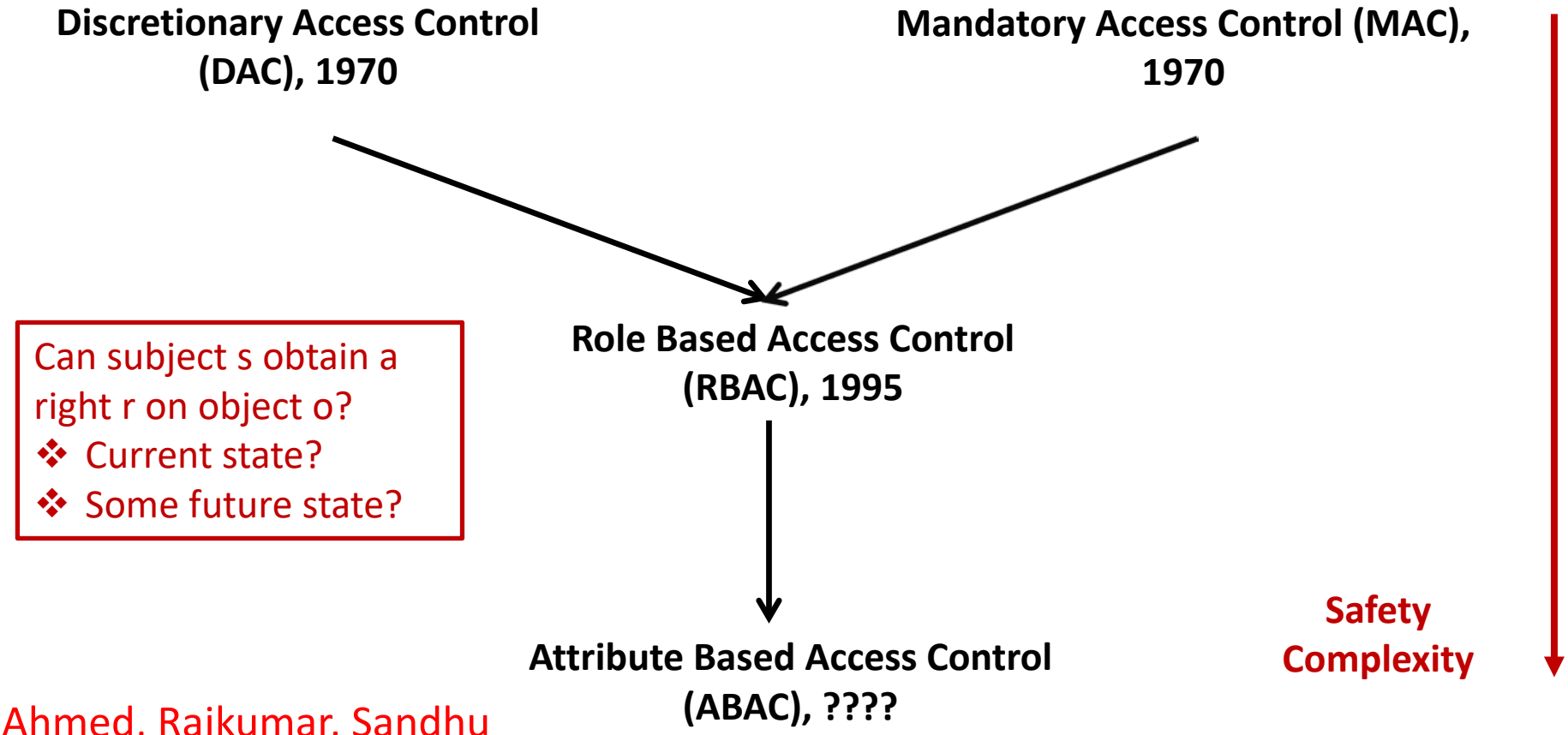
ReBAC and ABAC are not that different (Tahmina, Sandhu 2017)

ABAC Enforcement Architecture: Federated ABAC



Fisher 2015
NCCOE, NIST, Building Block

Foundations: Safety Analysis



Can subject s obtain a right r on object o?

- Current state?
- Some future state?

Ahmed, Rajkumar, Sandhu 2016 onwards