Access Control
Evolution and Prospects

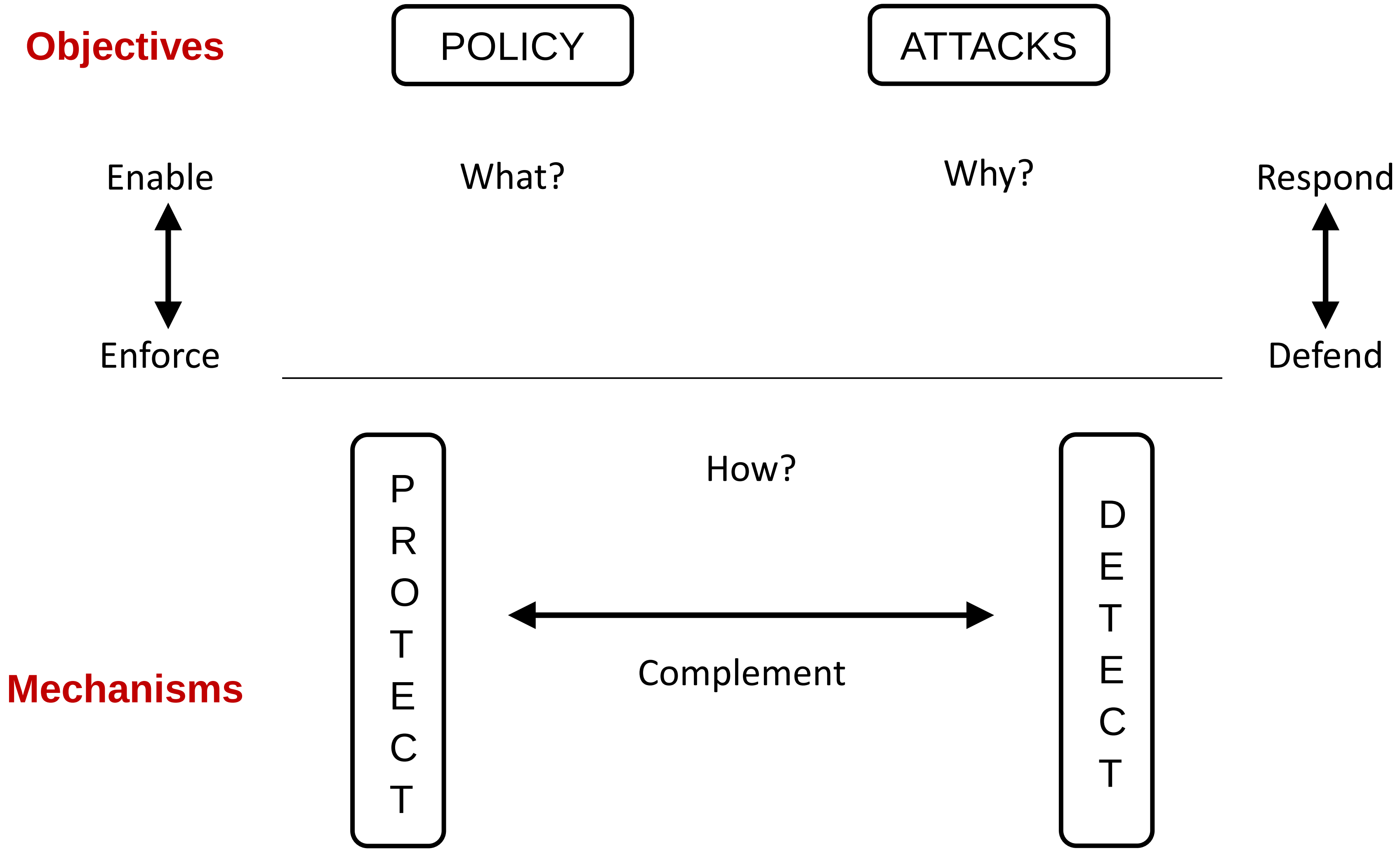
Ravi Sandhu
Executive Director

Professor of Computer Science
Lutcher Brown Chair in Cyber Security

December 2019

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

Holistic Cyber Security



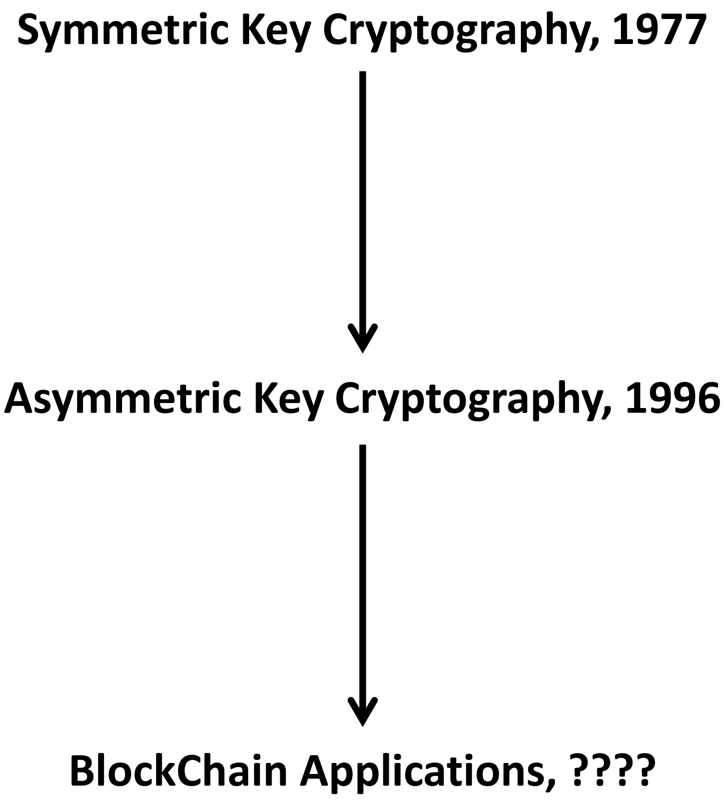
Cyber Security Fundamental Technologies

- Access Control: Authentication, Authorization
- Cryptography: Symmetric, Assymetric
- Detection: Signature, Zero Day
- Recovery/Recourse: Backups, Forensics
- Tolerance/Resilience: Mission Assurance
- ……….

Cyber Security Fundamental Limits

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

Cryptography



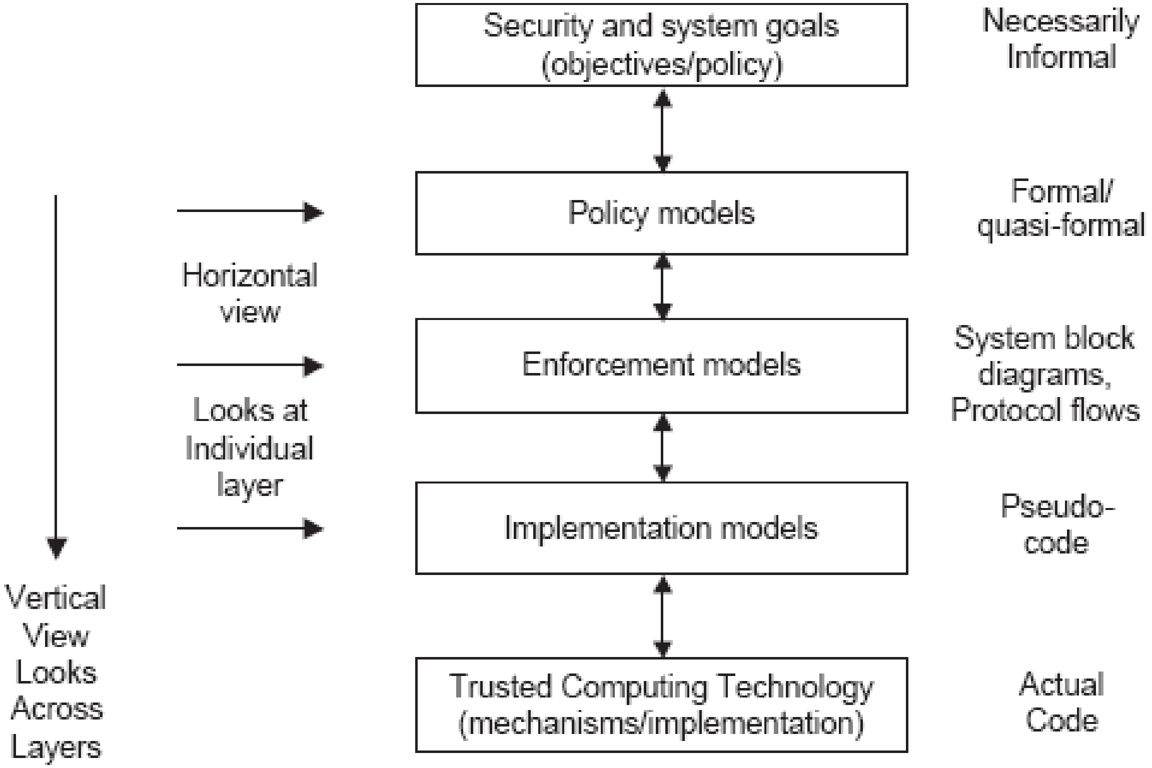
Symmetric Key Cryptography, 1977

Asymmetric Key Cryptography, 1996

BlockChain Applications, ????

Access Control
PEI Layers

Assumes Successful Authentication

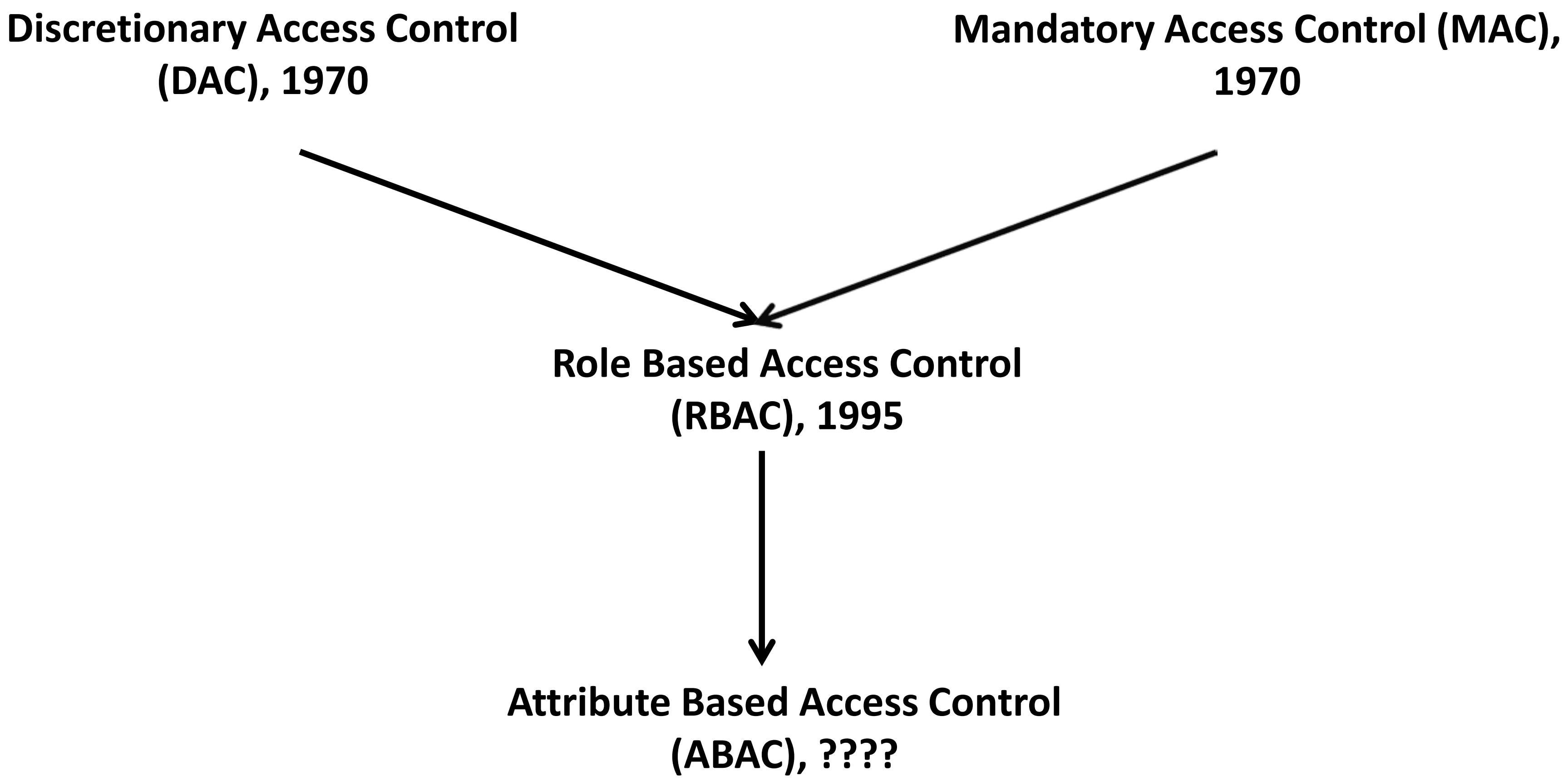

Security and system goals (objectives/policy)
Necessarily Informal
Policy models
Formal/ quasi-formal
Enforcement models
System block diagrams, Protocol flows
Implementation models
Pseudo-code
Trusted Computing Technology (mechanisms/implementation)
Actual Code
Horizontal view
Looks at Individual layer
Vertical View Looks Across Layers

Idealized

Enforceable (Approximate)

Codeable

Access Control



Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Discretionary Access Control (DAC)

- Core concept:

  Custodian of information determines access

- Core drawback:

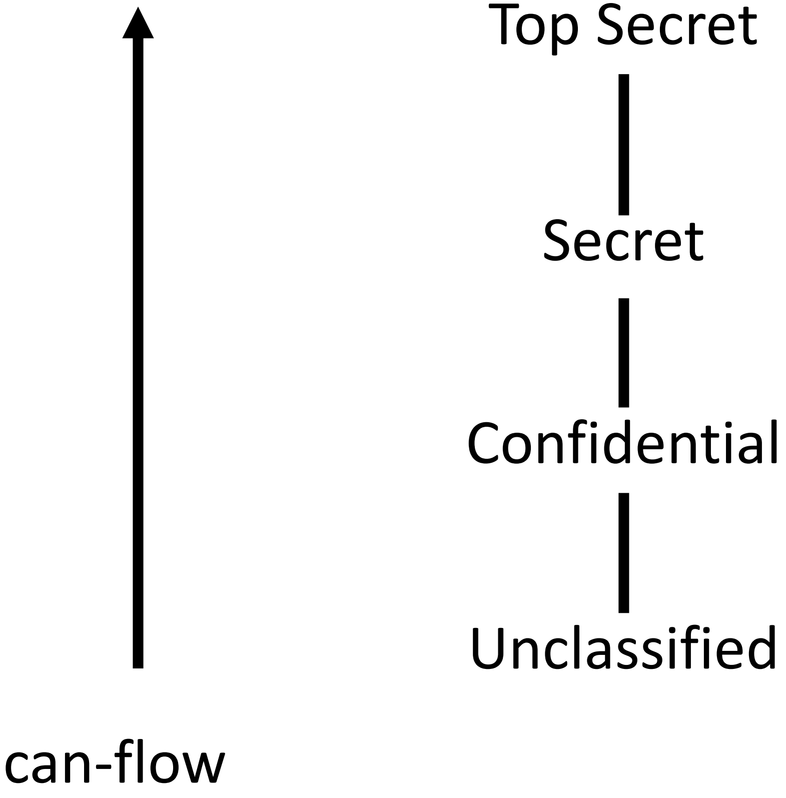
  Does not protect copies
  Therefore OK for integrity but not for confidentiality

- Sophistication:

  Delegation of custody

  Denials or negative rights

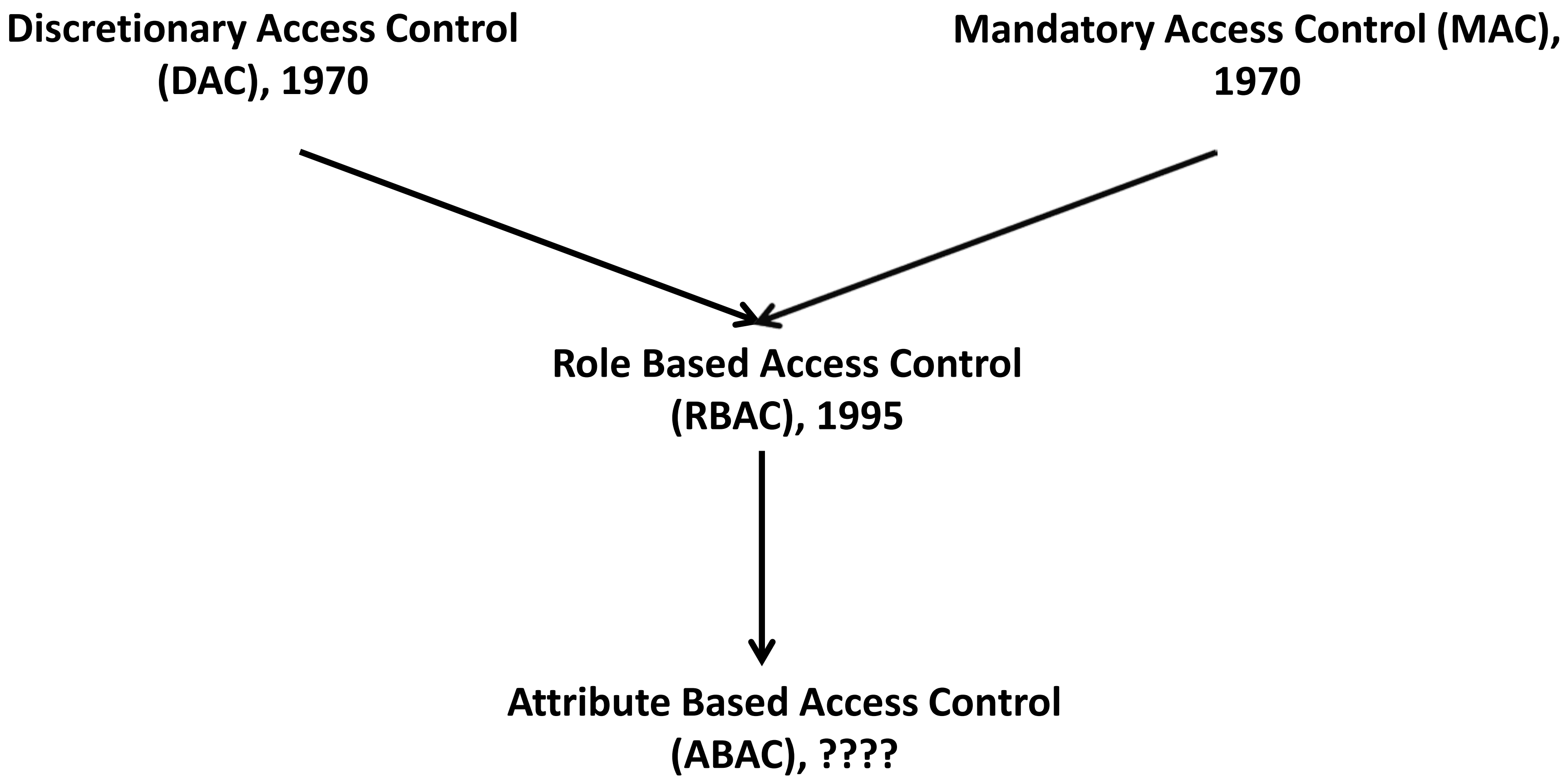
Mandatory Access Control (MAC)



Mandatory Access Control (MAC)

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

Access Control



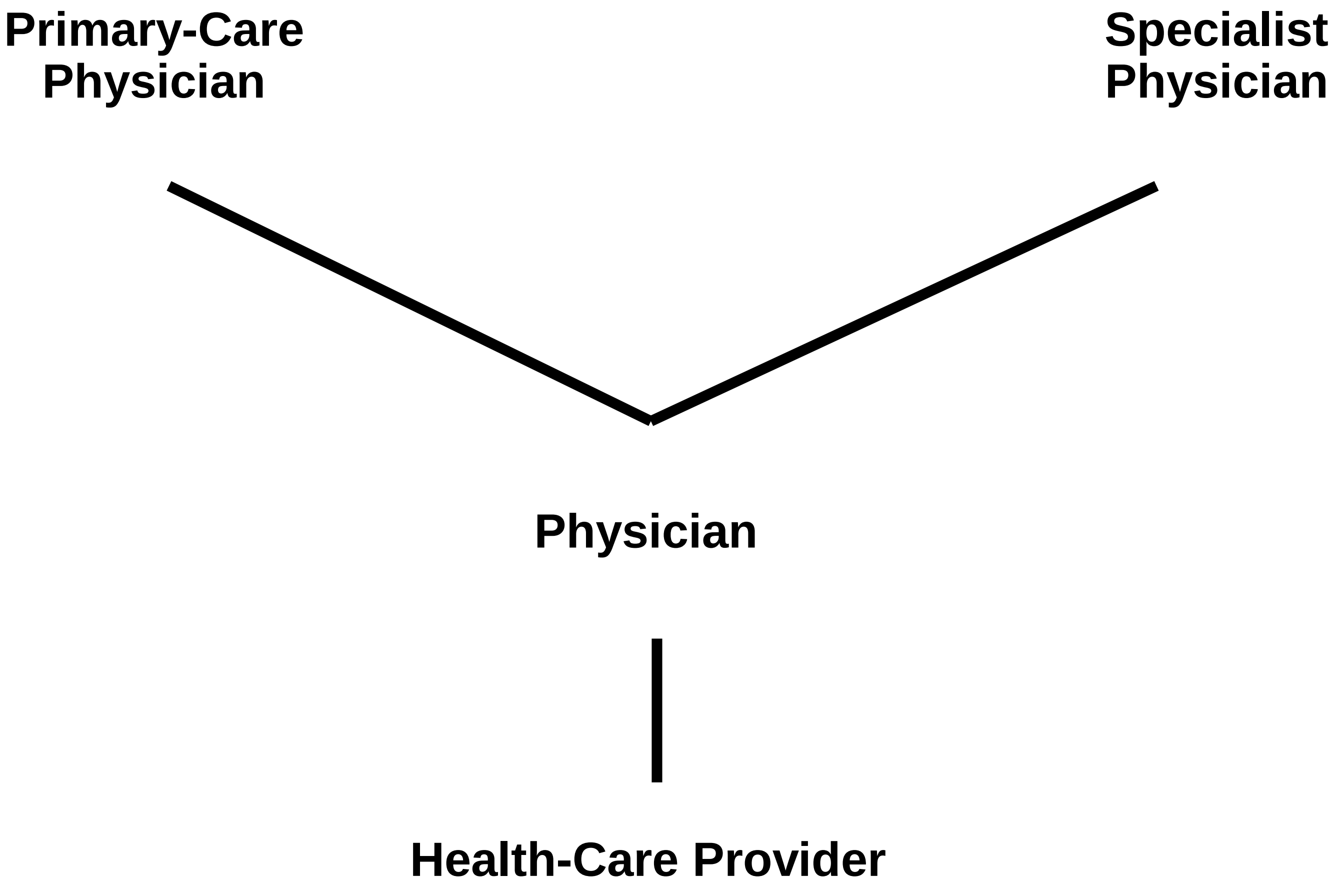
Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Role-Based Access Control (RBAC)



Primary-Care Physician

Specialist Physician

Physician

Health-Care Provider

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

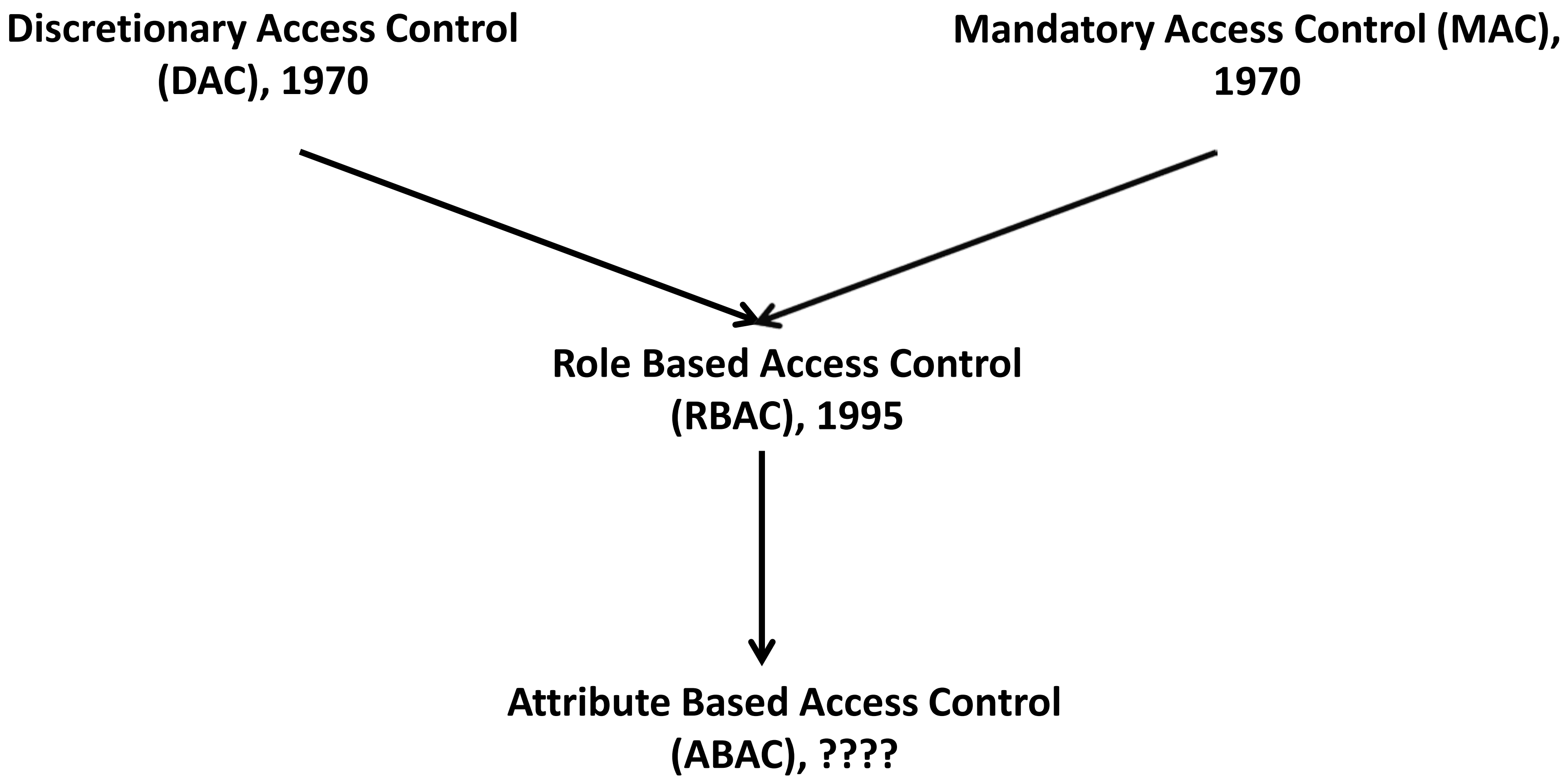
Role-Based Access Control (RBAC)

- Fundamental theorem of RBAC:

  RBAC can be configured to do DAC

  RBAC can be configured to do MAC

Access Control



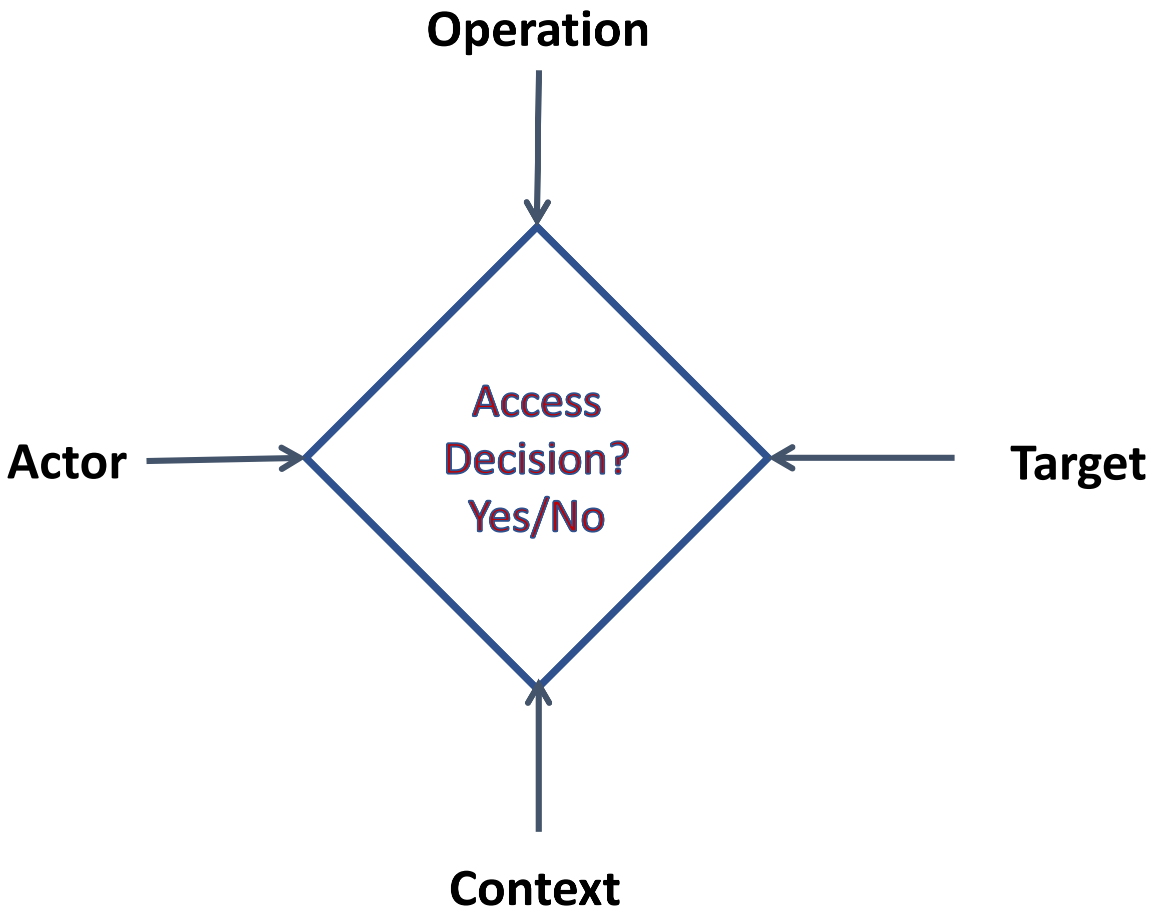
Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

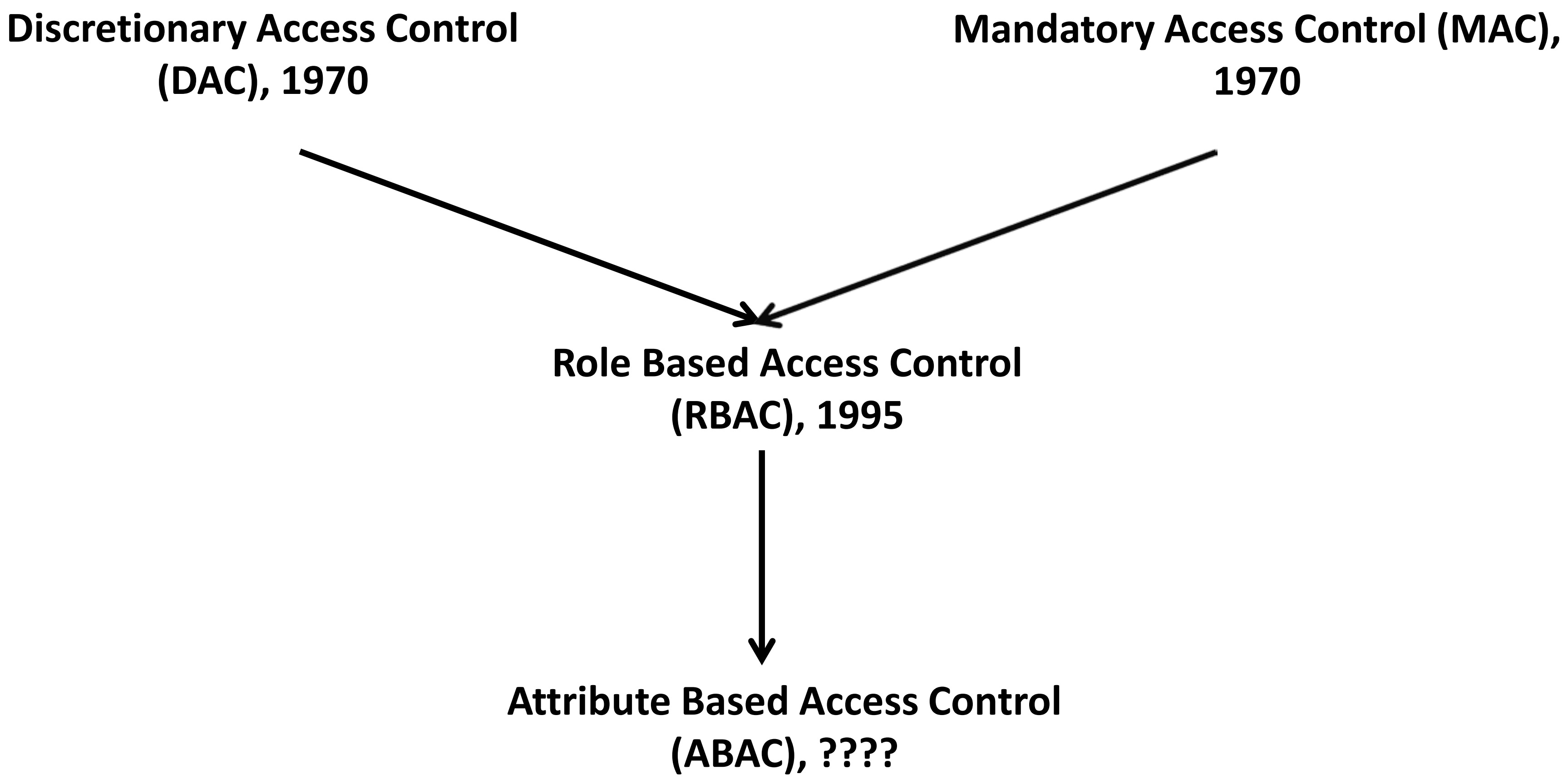
Attribute-Based Access Control (ABAC)



Attribute-Based Access Control (ABAC)

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

Access Control



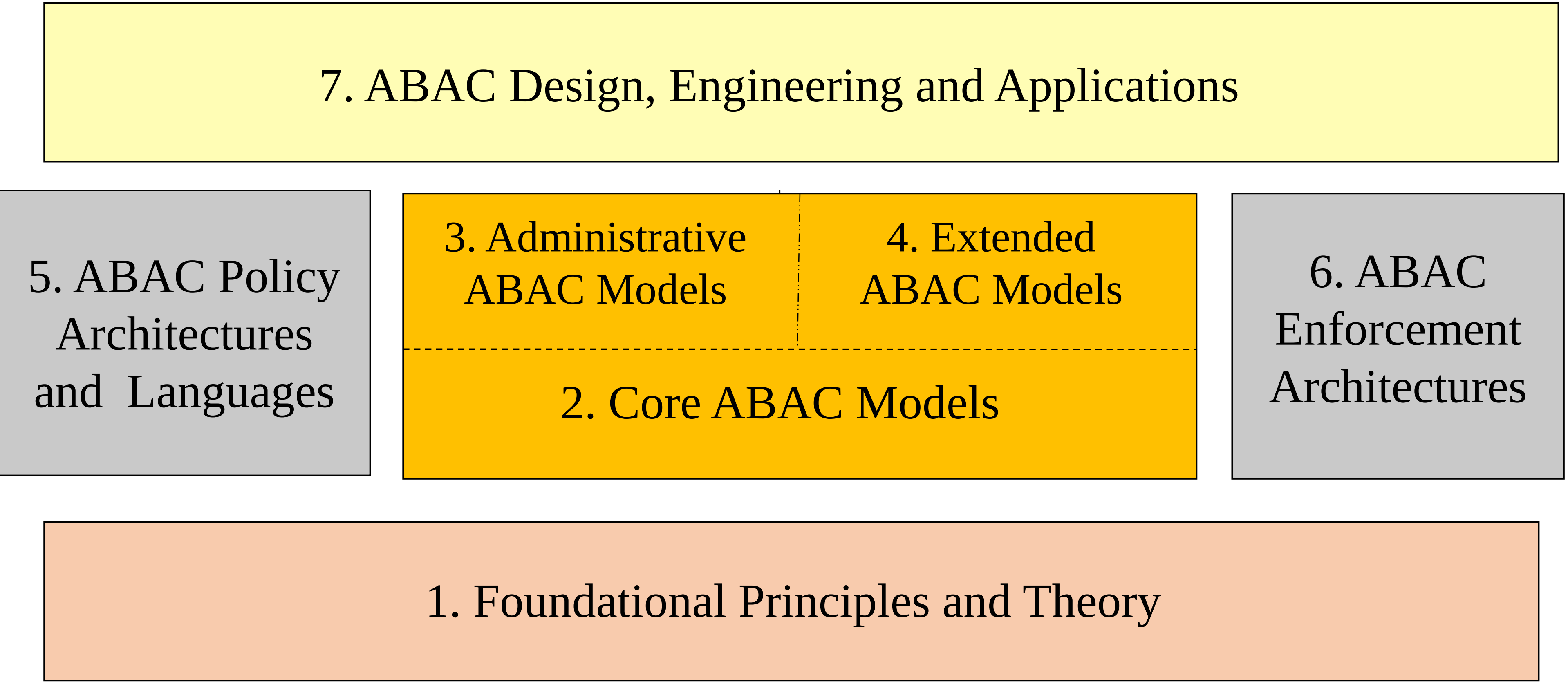
Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

ABAC Research Space



7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages

3. Administrative ABAC Models

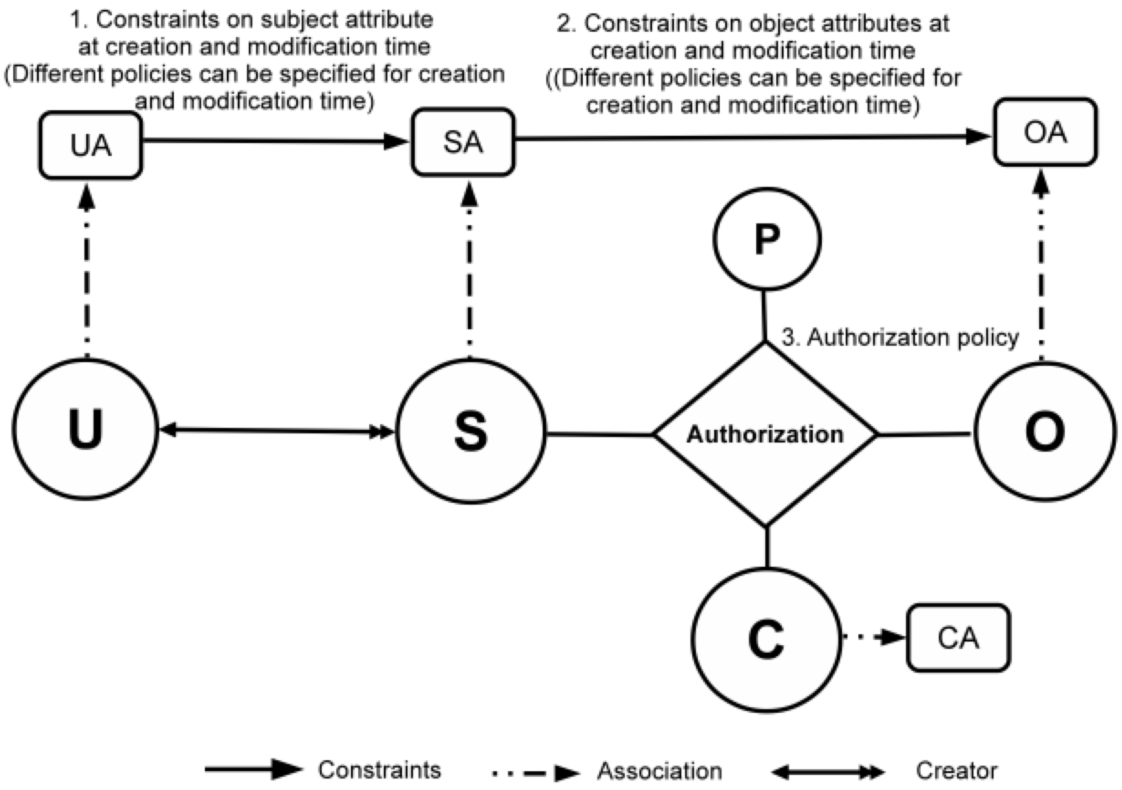
4. Extended ABAC Models

2. Core ABAC Models

6. ABAC Enforcement Architectures

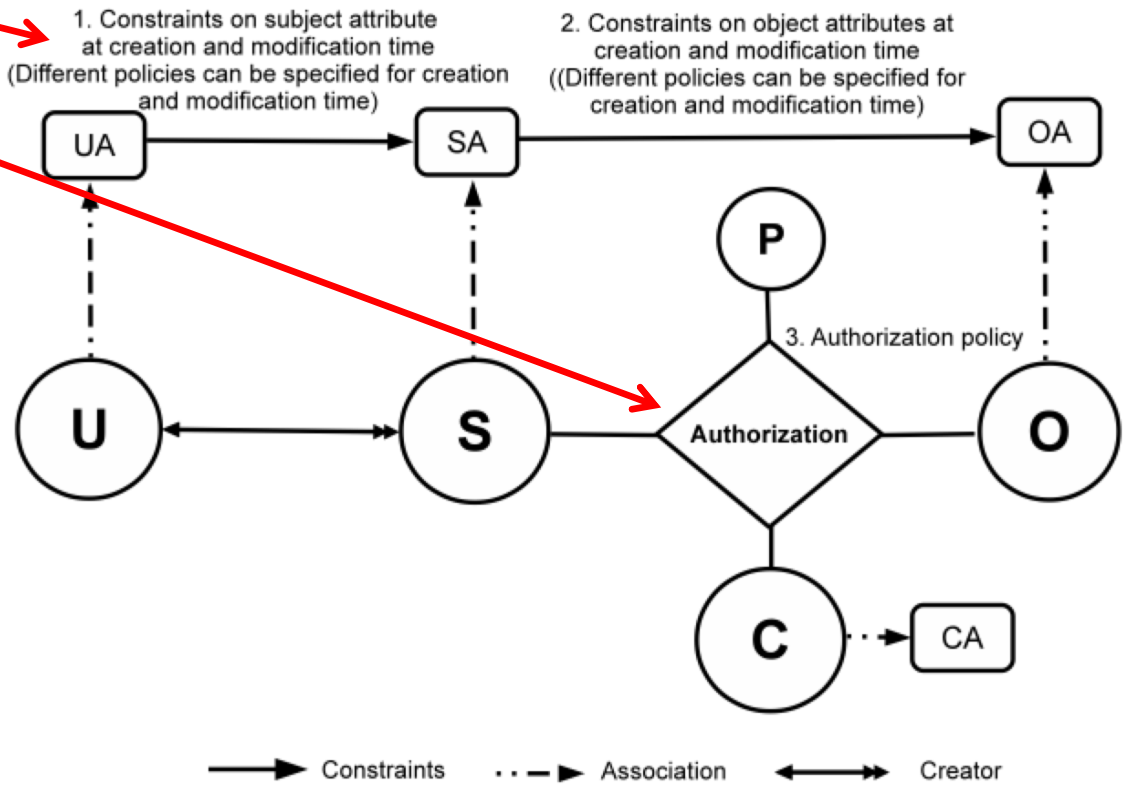
1. Foundational Principles and Theory

Core ABAC Models: ABAC$_\beta$


1. Constraints on subject attribute at creation and modification time (Different policies can be specified for creation and modification time)
2. Constraints on object attributes at creation and modification time ((Different policies can be specified for creation and modification time)
UA
SA
OA
P
3. Authorization policy
U
S
Authorization
O
C
CA
Constraints
Association
Creator

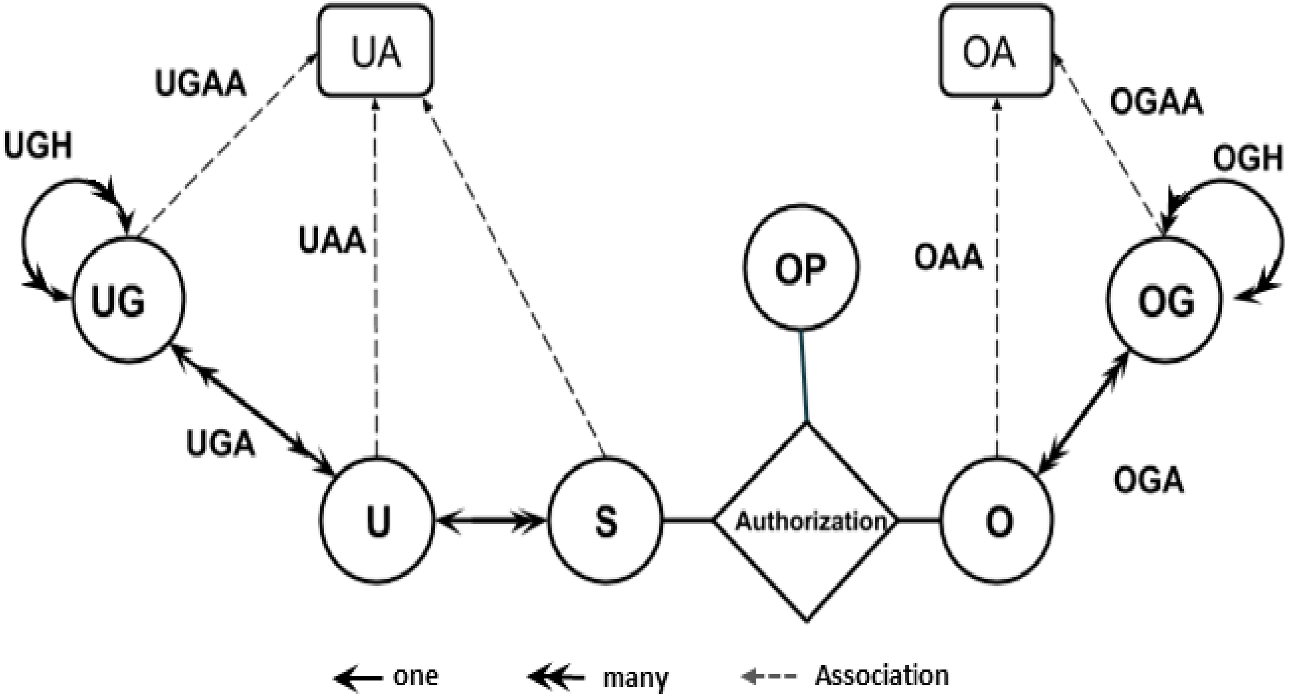
Core ABAC Models: ABAC$_\beta$

Policy Configuration Points


1. Constraints on subject attribute at creation and modification time (Different policies can be specified for creation and modification time)
2. Constraints on object attributes at creation and modification time ((Different policies can be specified for creation and modification time)
UA
SA
OA
P
3. Authorization policy
U
S
Authorization
O
C
CA
Constraints
Association
Creator

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

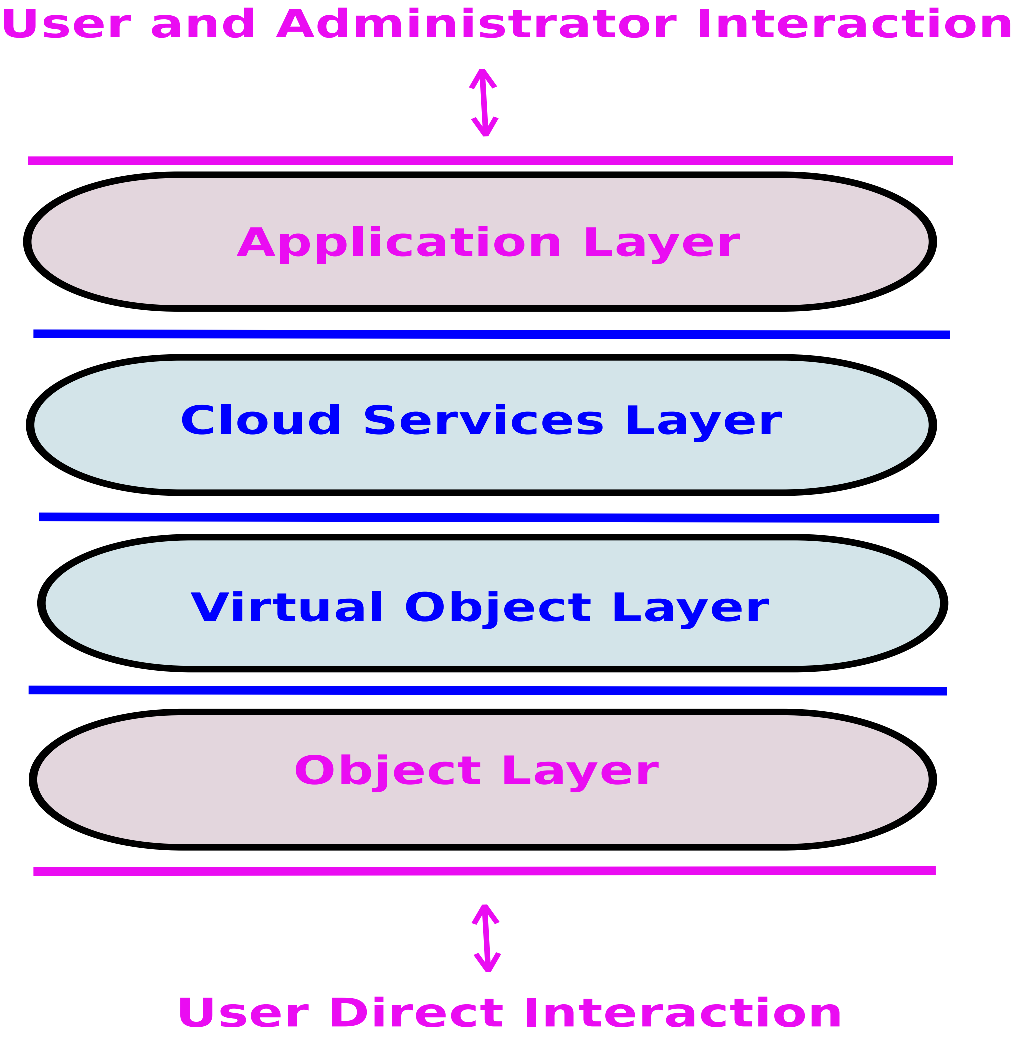
Administrative ABAC Models: HGABAC



- 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



User and Administrator Interaction

Application Layer

Cloud Services Layer

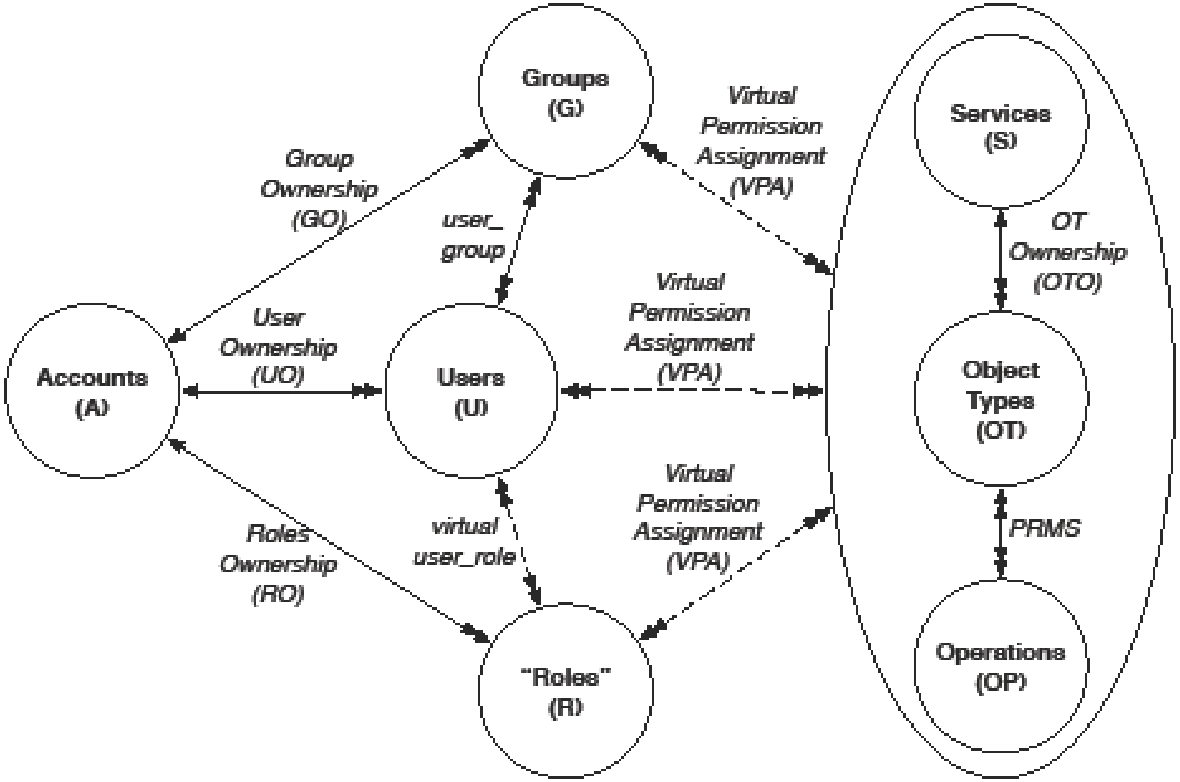
Virtual Object Layer

Object Layer

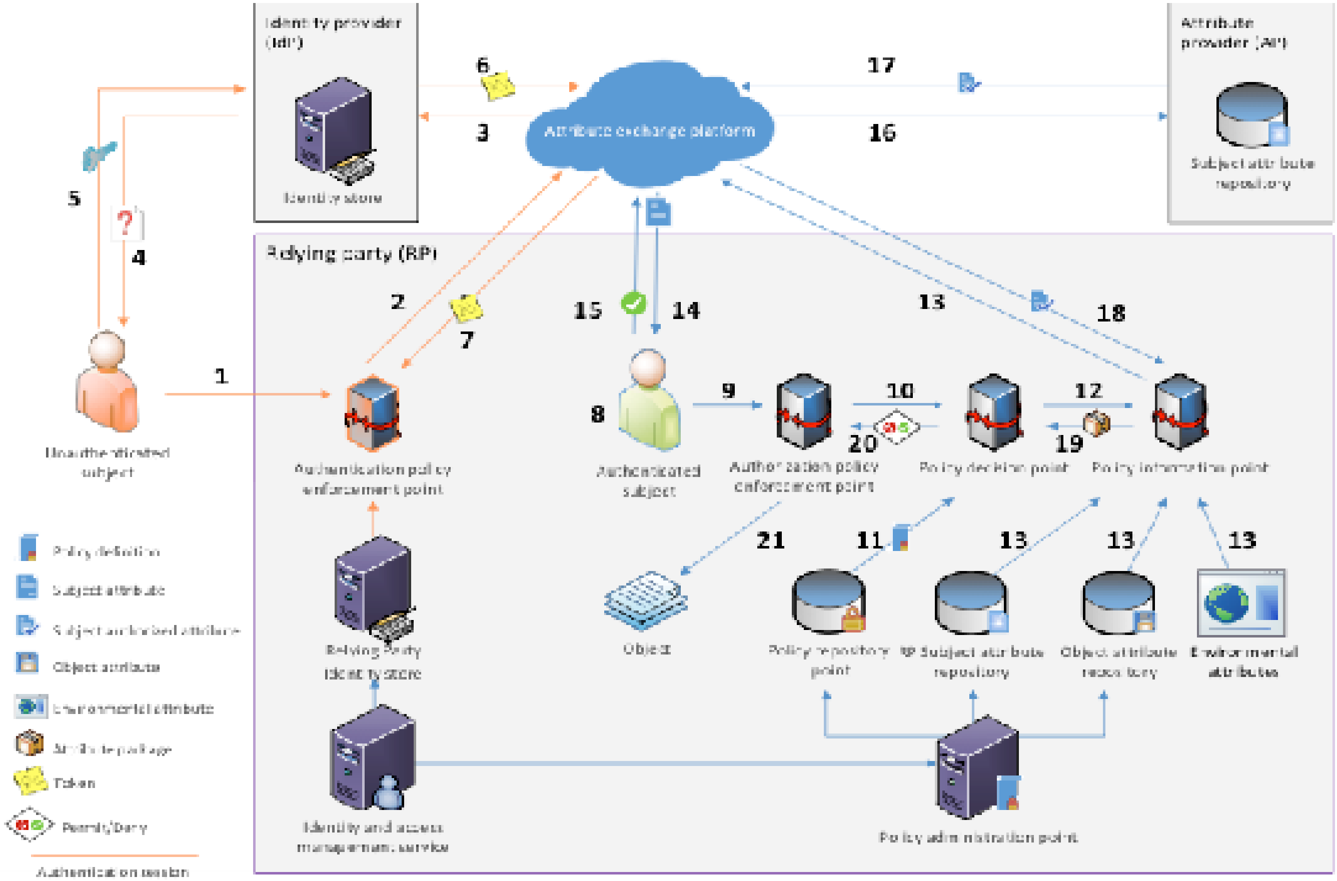
User Direct Interaction

Alsheri, Bhatt, Patwa,
Benson, Sandhu
2016 onwards

Policy Architecture: Amazon AWS style



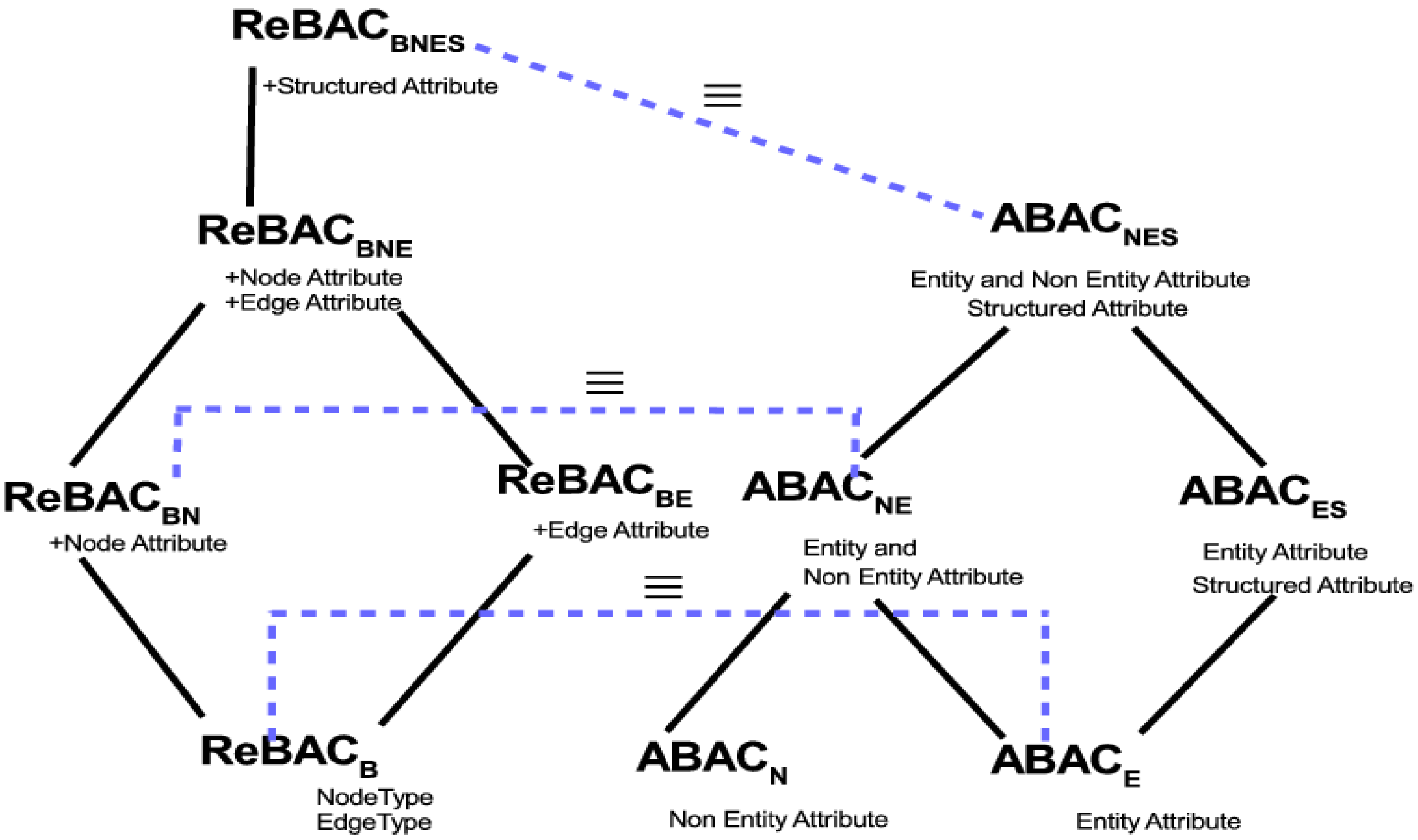
ABAC Enforcement Architecture: Federated ABAC



Fisher 2015

NCCOE, NIST, Building Block

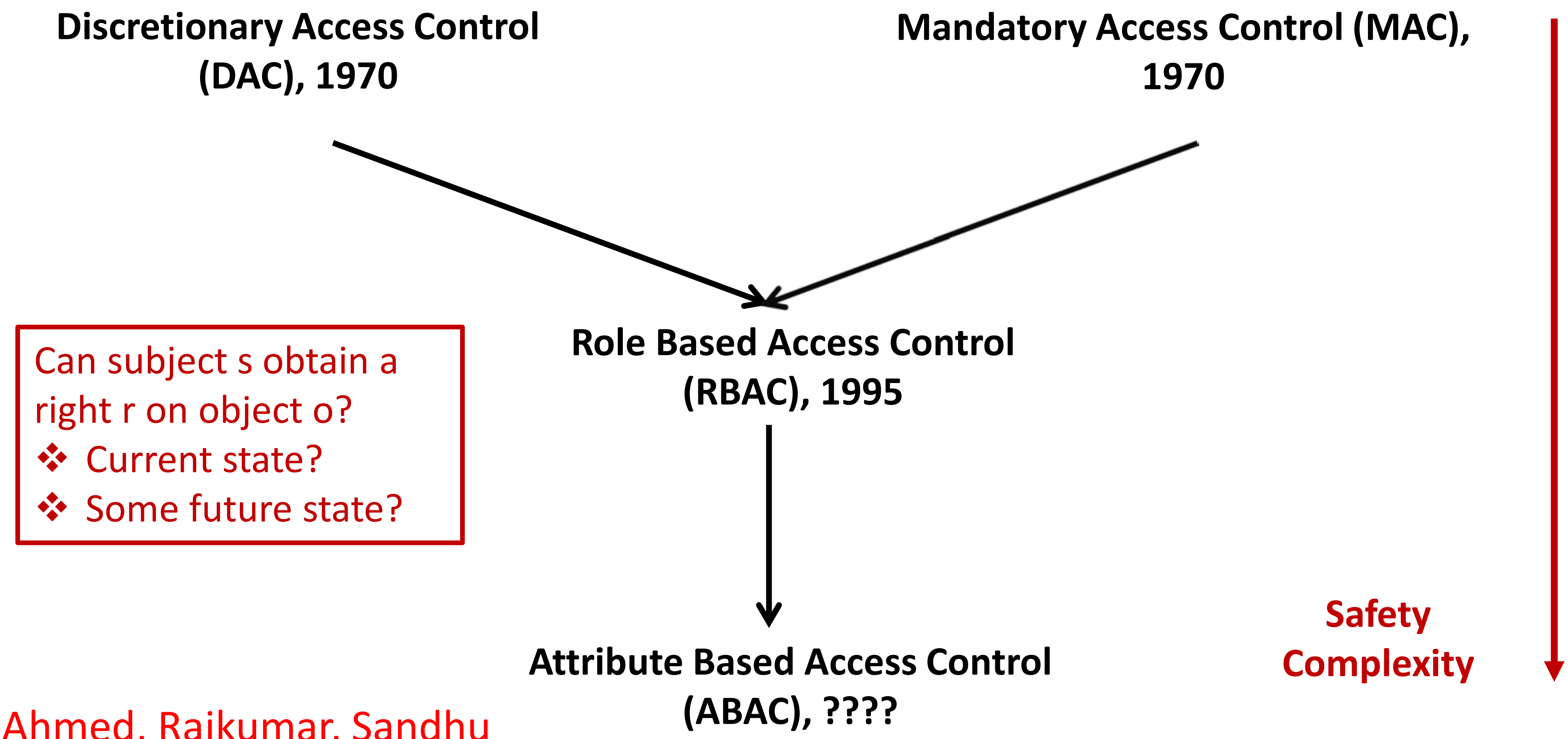
Extended ABAC Models: ReBAC versus ABAC



ReBAC and ABAC are not that different

(Tahmina, Sandhu 2017)

Foundations: Safety Analysis



Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Safety Complexity

Can subject s obtain a right r on object o?

- Current state?
- Some future state?

Ahmed, Rajkumar, Sandhu
2016 onwards