An Access Control Perspective on the Science of Security
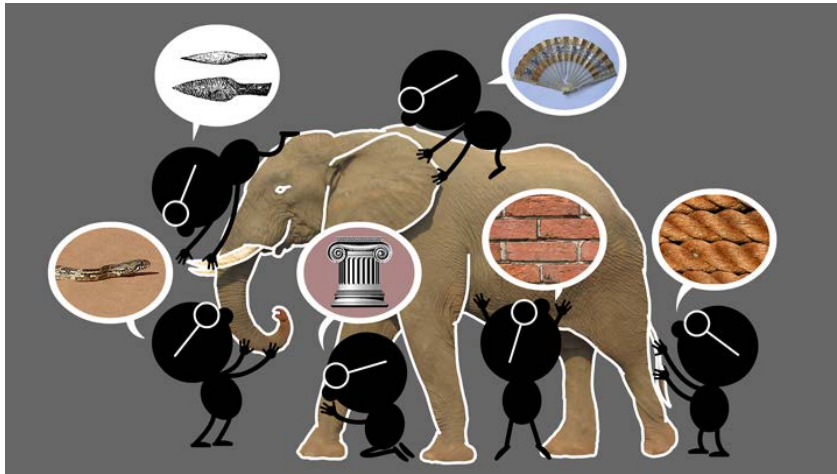
Ravi Sandhu

Executive Director and Chief Scientist

Professor of Computer Science
Lutcher Brown Chair in Cyber Security

Keynote Lecture
Hot Topics in the Science of Security
Raleigh, North Carolina
April 11, 2018

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

I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy
Enhanced Cloud Computing
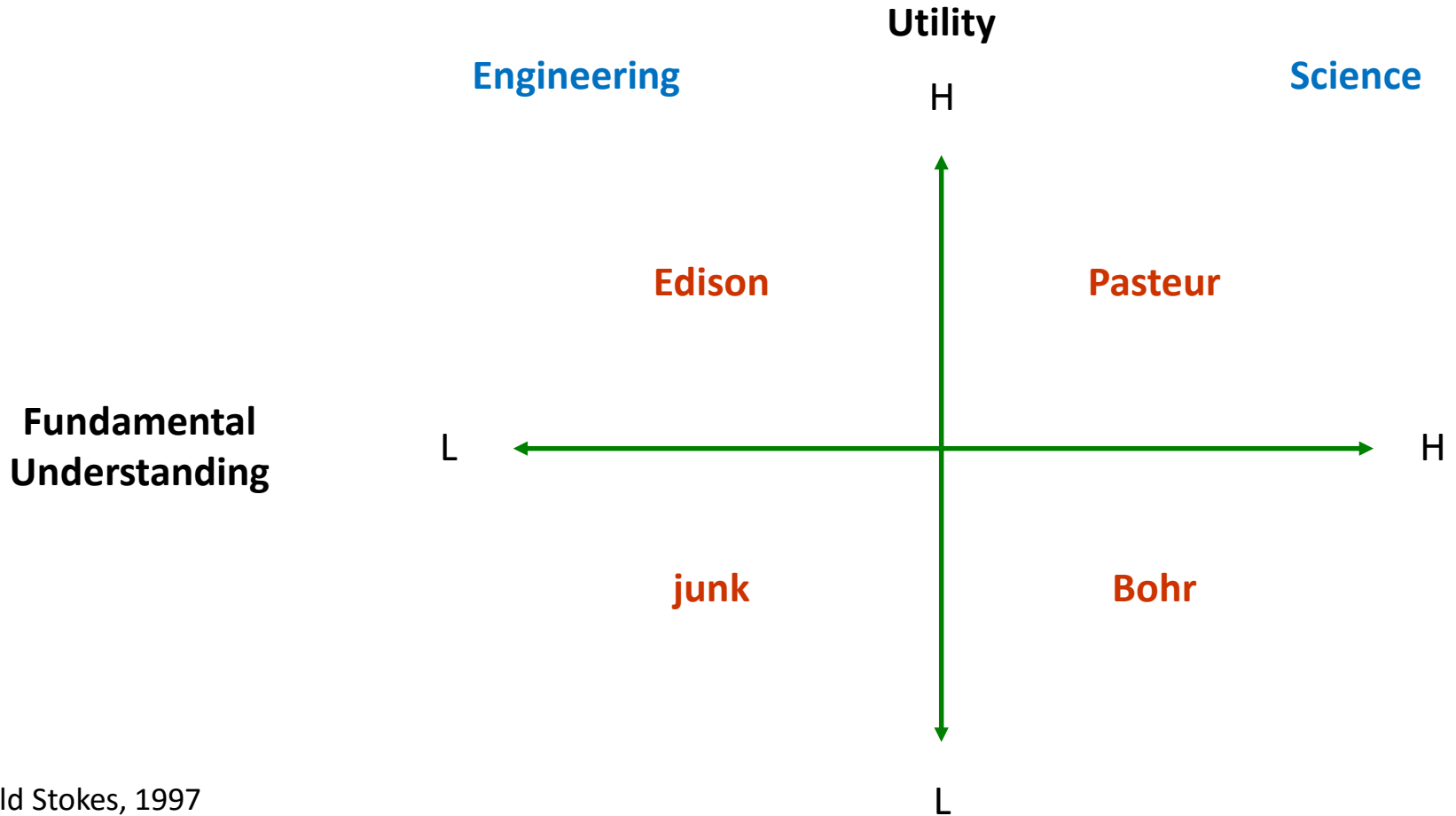
Elephant Problem

Cyber-Elephant Problem

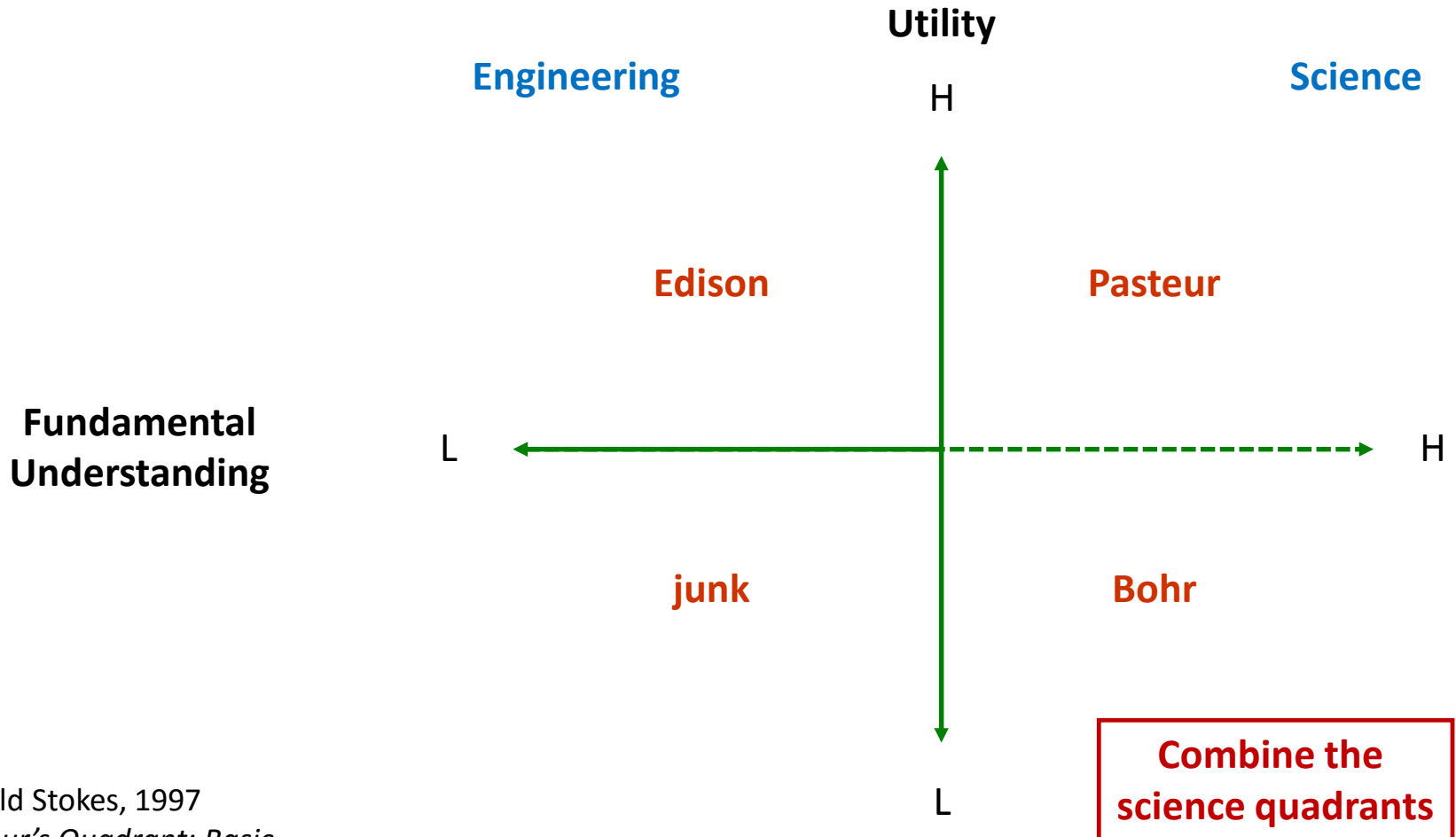**The cyber-elephant problem requires Applied and Basic research Combined (ABC)**
 ***The New ABCs of Research, Ben Schneiderman, 2016**

UTSA Computer Science

I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy
Enhanced Cloud Computing

Utility

Engineering

H

Science

Edison

Pasteur

**Fundamental
Understanding**

L ←————————————————→ H

junk

Bohr

L

Donald Stokes, 1997
*Pasteur's Quadrant: Basic
Science and Technological Innovation*

© Ravi Sandhu

World-Leading Research with Real-World Impact!

UTSA Computer Science

3

ICS
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy
Enhanced Cloud Computing

Utility

Engineering   H   **Science**

Edison   **Pasteur**

**Fundamental
Understanding**   L ←————————————→ H

junk   **Bohr**

L

Donald Stokes, 1997
*Pasteur's Quadrant: Basic
Science and Technological Innovation*

**Combine the
science quadrants**

I·C·S
The Institute for Cyber Security

Holistic Cyber Security

C·SPECC
Center for Security and Privacy
Enhanced Cloud Computing

Objectives

POLICY   ATTACKS

Enable   What?   Why?   Respond

Enforce   Defend

How?

P R O T E C T   Complement   D E T E C T

Mechanisms

Fixed policy

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Born 1990s

Flexible policy

World-Leading Research with Real-World Impact!

7. ABAC Design, Engineering and Applications

5. ABAC Policy Architectures and Languages
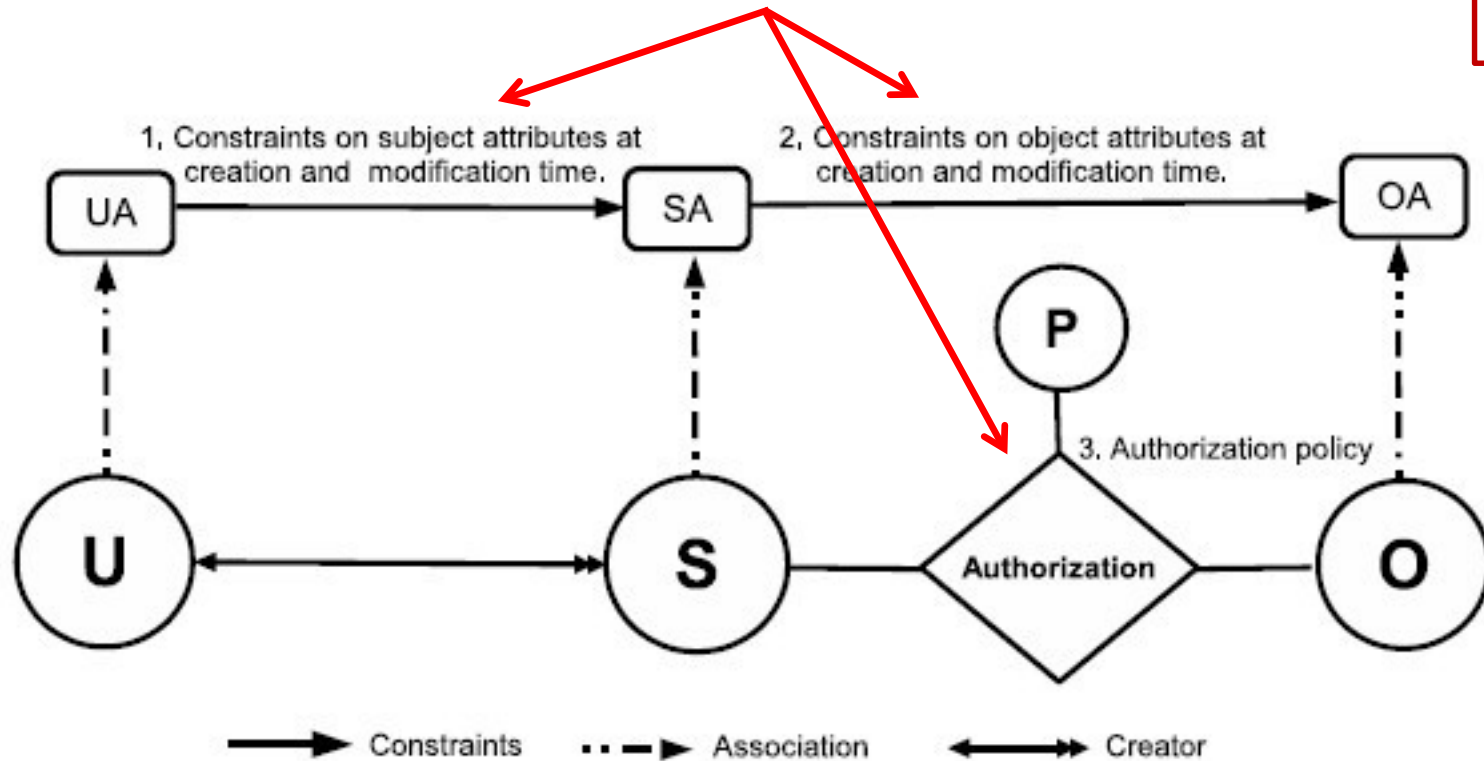
3. Administrative ABAC Models

4. Extended ABAC Models

2. Core ABAC Models

6. ABAC Enforcement Architectures
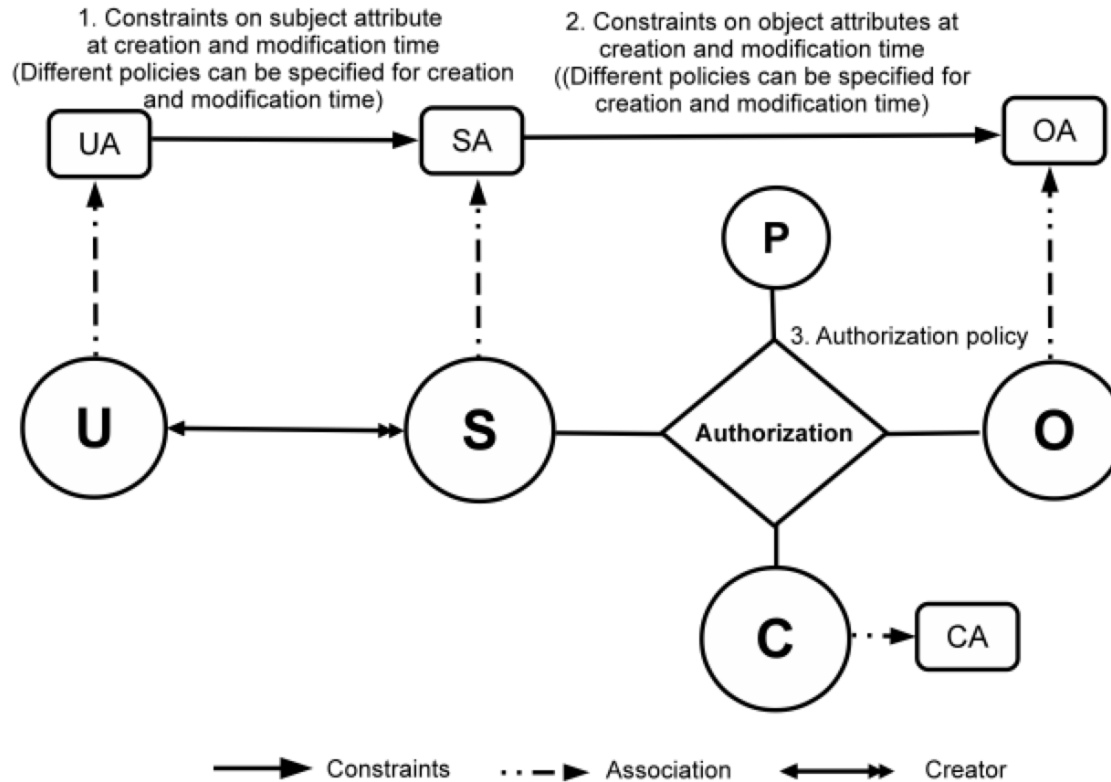
1. Foundational Principles and Theory

World-Leading Research with Real-World Impact!
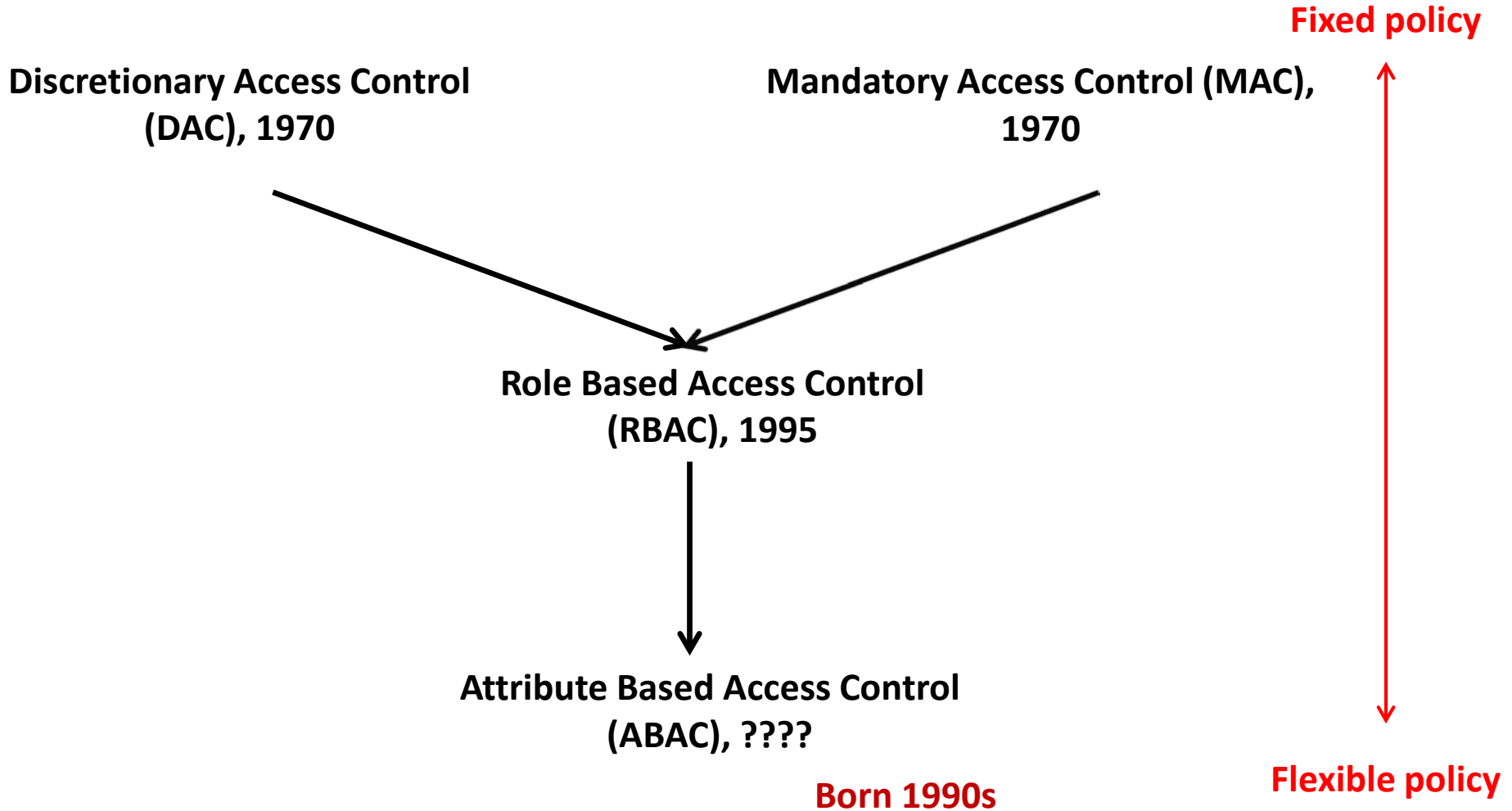
Policy Configuration Points

ABAC$_\alpha$

1, Constraints on subject attributes at creation and modification time.

2, Constraints on object attributes at creation and modification time.

3. Authorization policy

UA → SA → OA

P

U → S → Authorization → O

➜ Constraints ·····➤ Association ⬌ Creator

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

World-Leading Research with Real-World Impact!

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

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

World-Leading Research with Real-World Impact!

ICS The Institute for Cyber Security

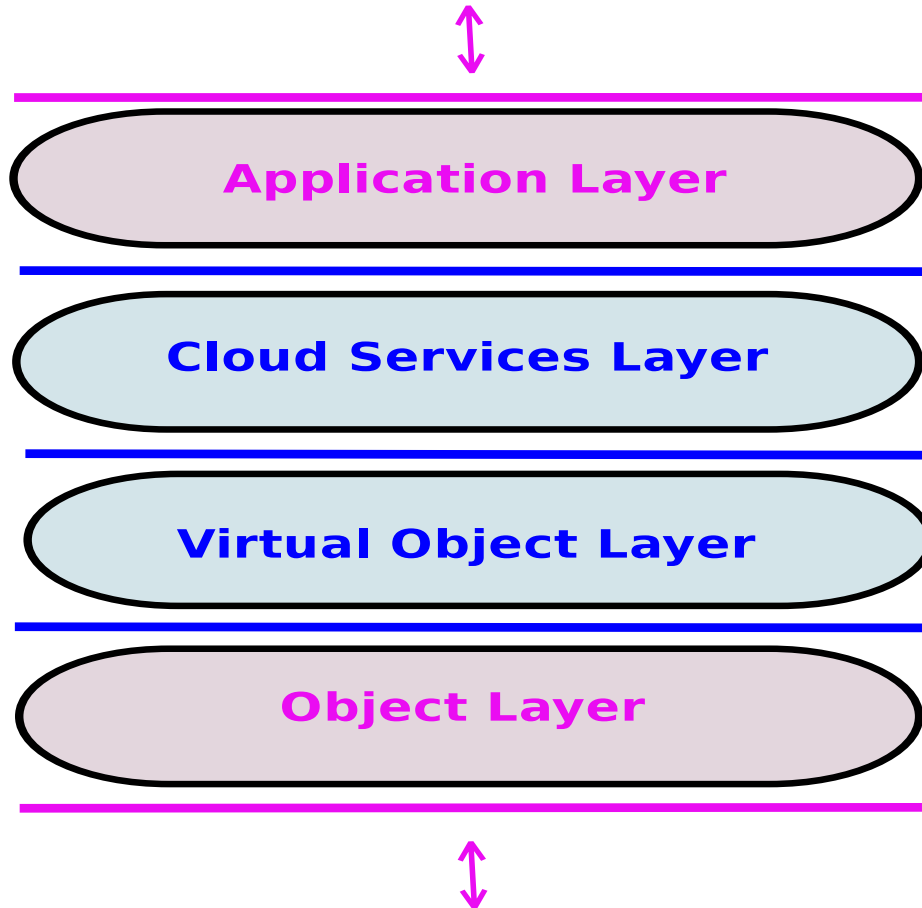**C·SPECC** Center for Security and Privacy Enhanced Cloud Computing
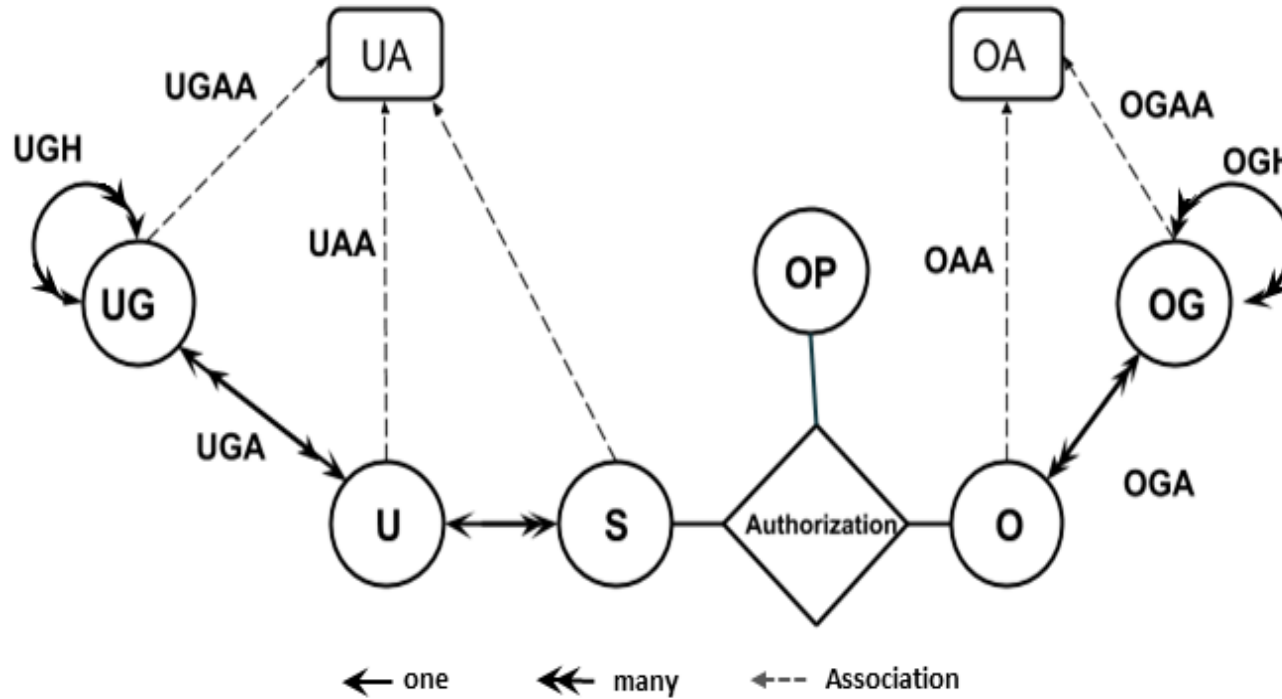
HGABAC

➤ Hierarchical Group and Attribute Based Access Control (HGABAC)
  ❖ Introduces User and Object Groups
  ❖ Simplifies administration of attributes
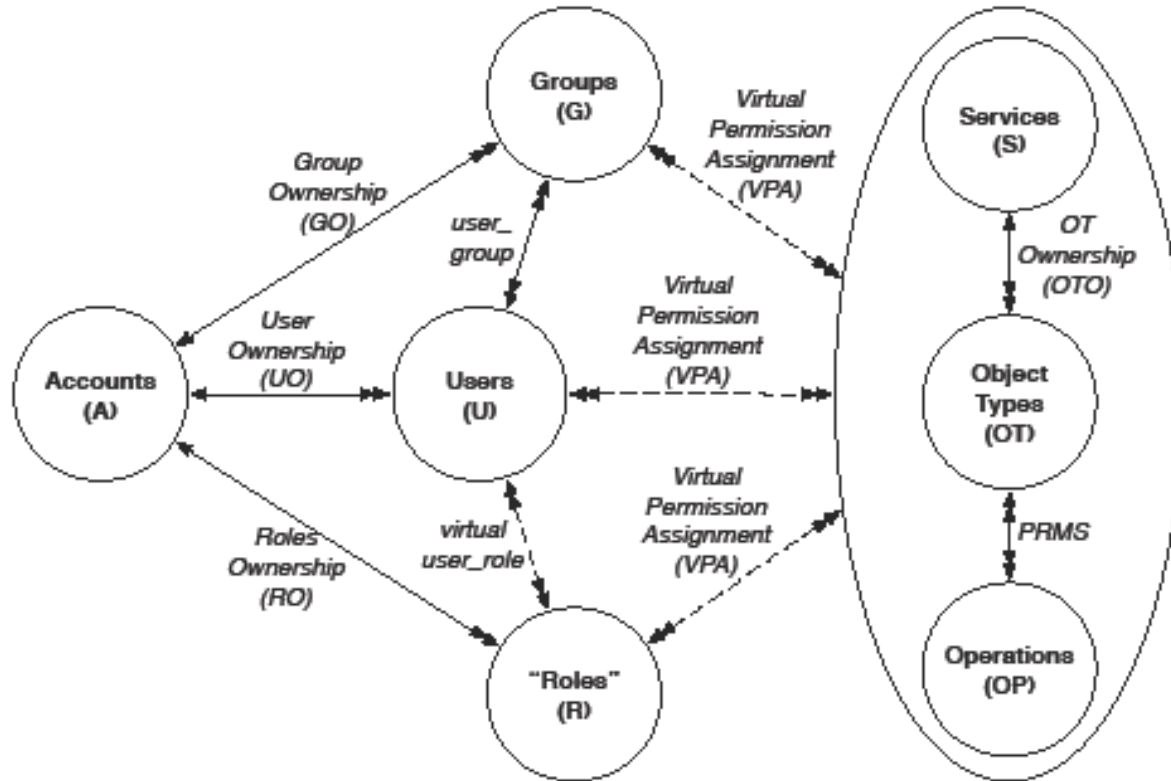
Servos and Osborn, 2015

World-Leading Research with Real-World Impact!

UTSA Computer Science

The Institute for Cyber Security

C·SPECC
Center for Security and Privacy
Enhanced Cloud Computing

User and Administrator Interaction

Cloud Enabled IoT

↕

Application Layer

Cloud Services Layer

Virtual Object Layer

Object Layer

↕

User Direct Interaction

Alsheri, Bhatt, Patwa,
Benson, Sandhu
2016 onwards

World-Leading Research with Real-World Impact!

UTSA Computer Science

The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

Amazon AWS Style

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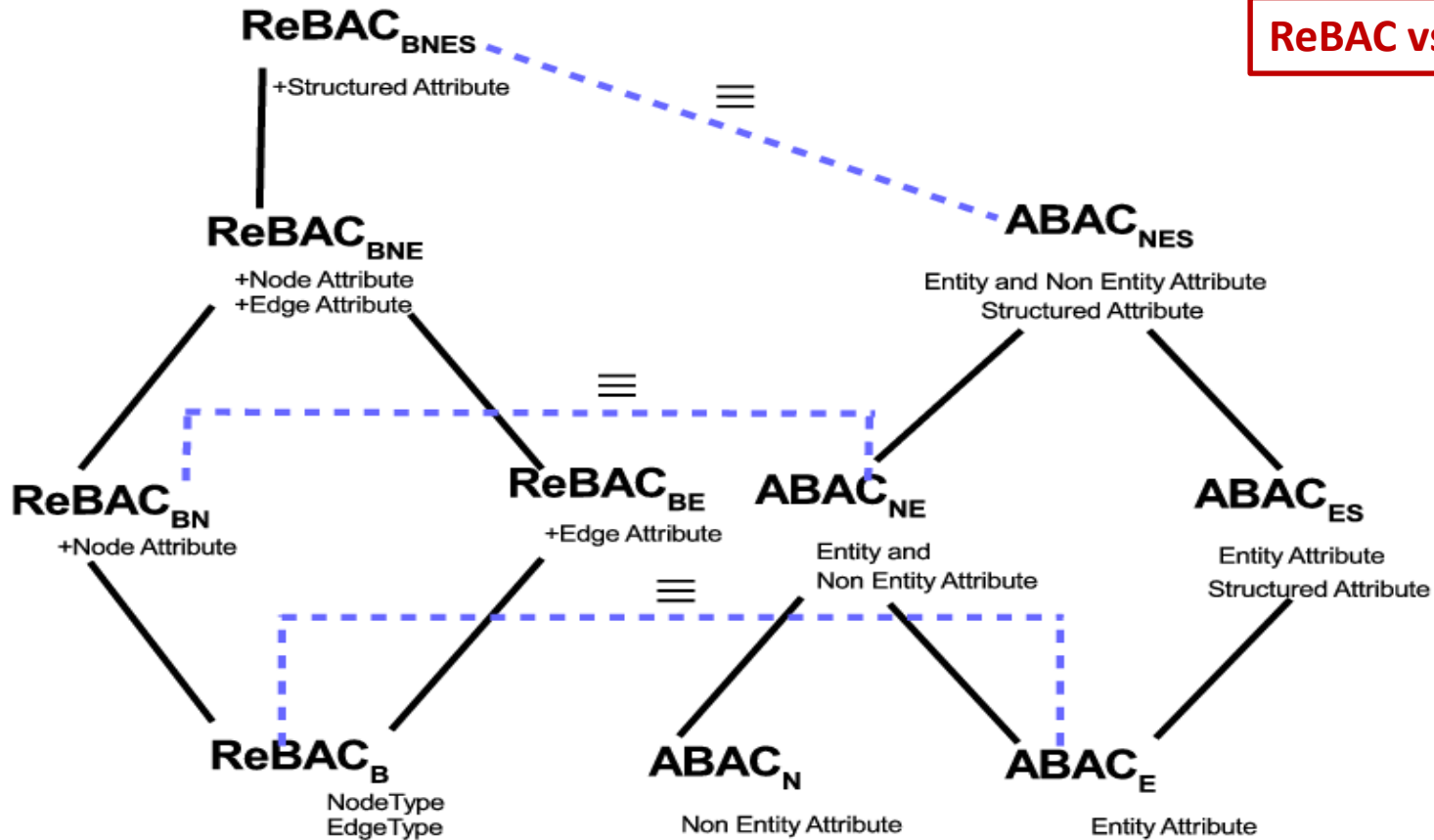
**ReBAC and ABAC are not that different
(Tahmina, Sandhu 2017)**

World-Leading Research with Real-World Impact!

Federated ABAC
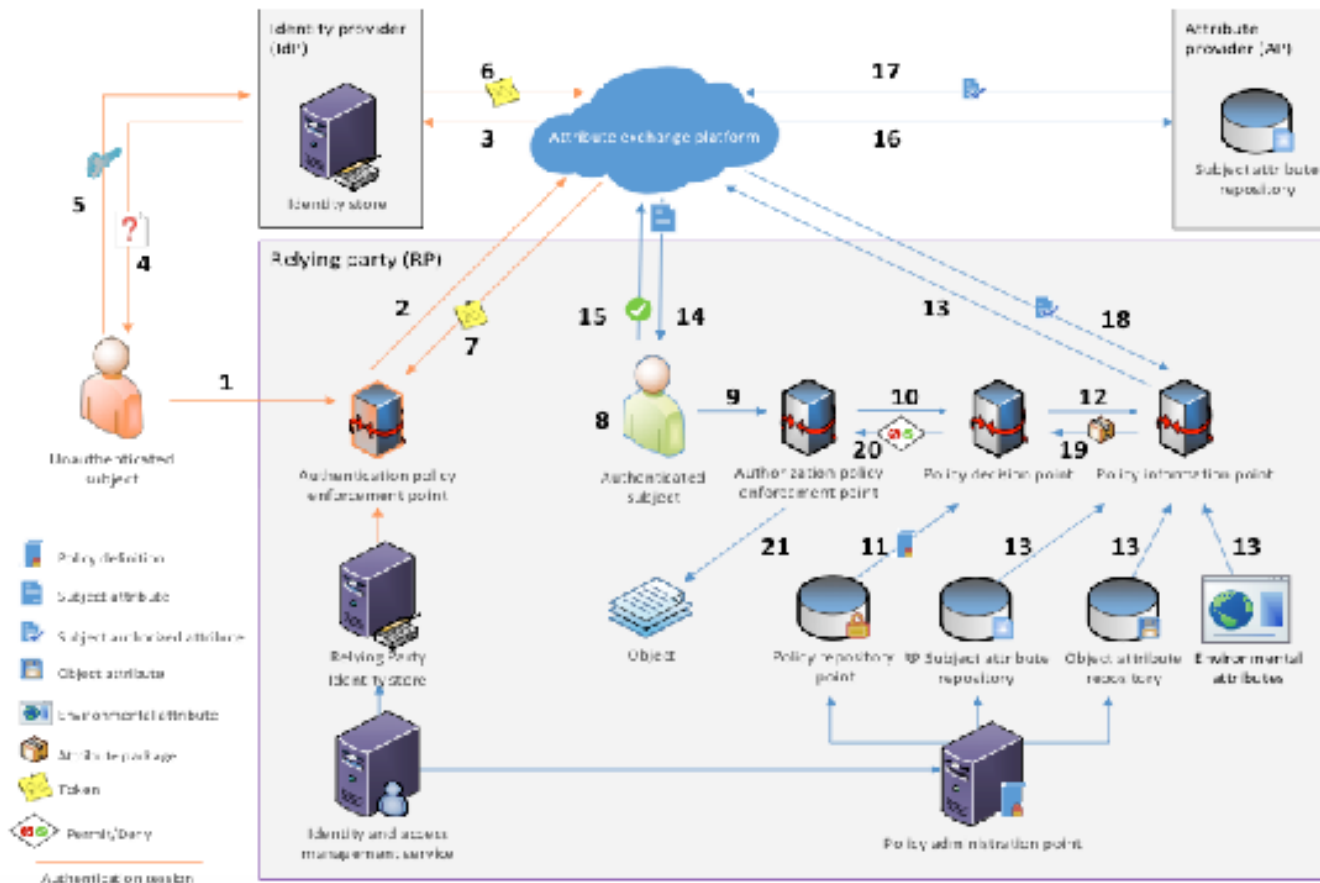
Fisher 2015
NCCOE, NIST, Building Block

ICS — The Institute for Cyber Security

C·SPECC — Center for Security and Privacy Enhanced Cloud Computing

Safety Analysis

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

Can subject s obtain a right r on object o?
- ❖ Current state?
- ❖ Some future state?

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

Safety Complexity

Ahmed, Rajkumar, Sandhu 2016 onwards

World-Leading Research with Real-World Impact!

UTSA Computer Science

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

World-Leading Research with Real-World Impact!

Take-Aways for Science of Security

➢ Applied and Basic Combined

➢ Holistic