I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

Cyber Security R&D: A Personal Perspective

Ravi Sandhu
Executive Director

Professor of Computer Science
Lutcher Brown Chair in Cyber Security

May 2019

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

World-Leading Research with Real-World Impact!

UTSA Computer Science

ICS Facts and Figures

MISSION

Excellence in graduate-level sponsored research

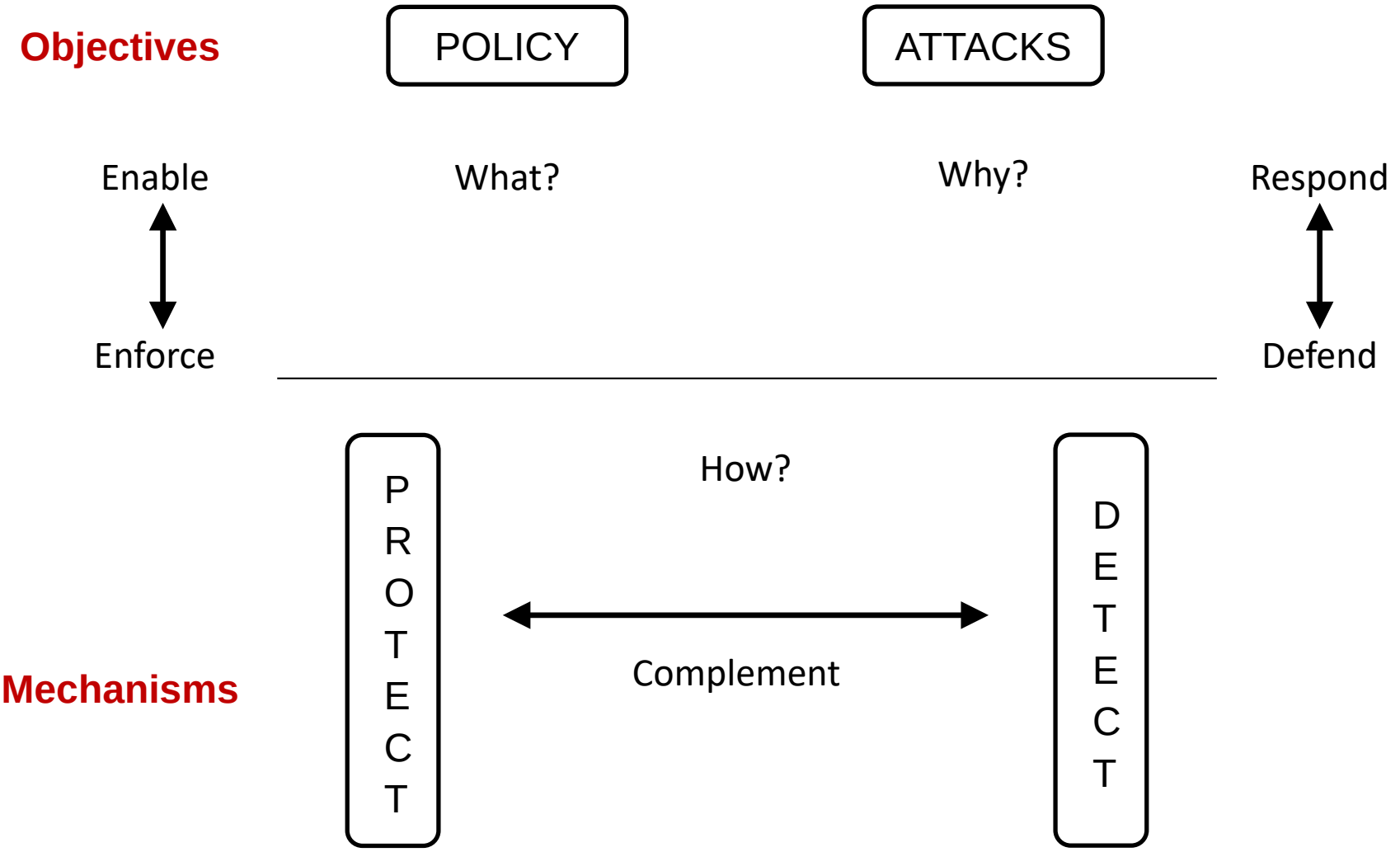
PAST SYNOPSIS

- Founded: 2007
- PhDs graduated: 25
- External funding raised: $22M

CURRENT STATUS

- Faculty affiliates: 20
  - College of Sciences: 8, Engineering: 5, Business: 5, Education: 2
  - Includes 6 with research fully managed through ICS
- Current PhD students: 32
  - College of Sciences: 22, Engineering: 7, Business: 2, Education: 1
  - Domestic: 17
  - Foreign: 15
- Current non-PhD students: 8
  - Domestic: 7
  - Foreign: 1

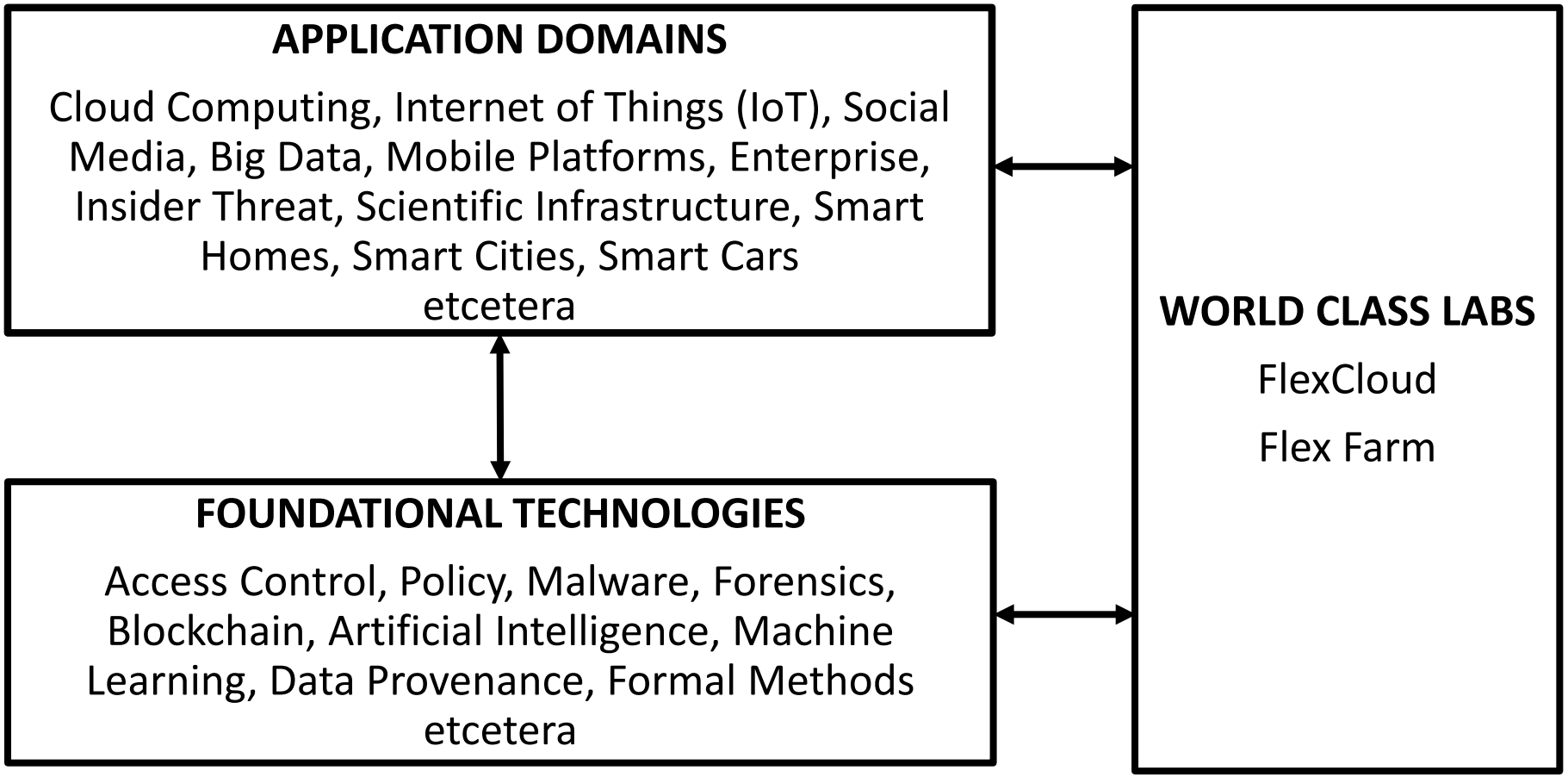
Holistic Cyber Security Research



Holistic Cyber Security Research

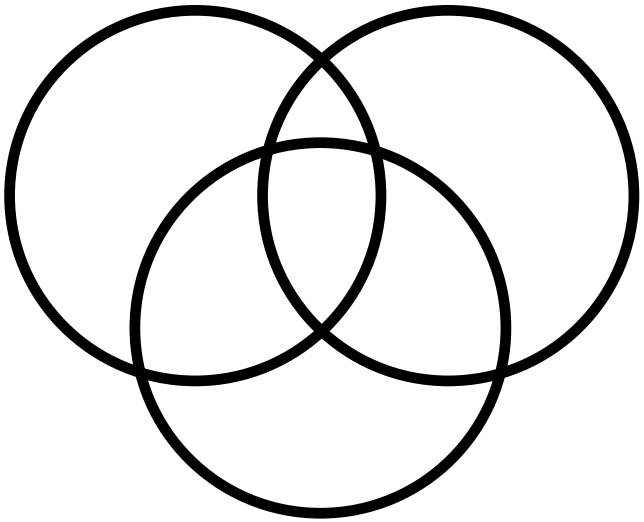
World-Leading Research with Real-World Impact!

ICS Major Research Thrusts



Goal: Broaden and Deepen

Security Objectives



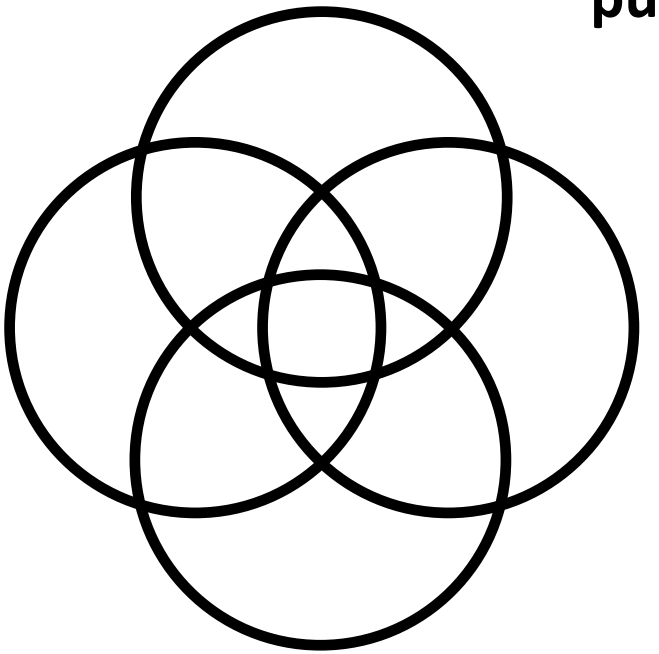
INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives

USAGE
purpose



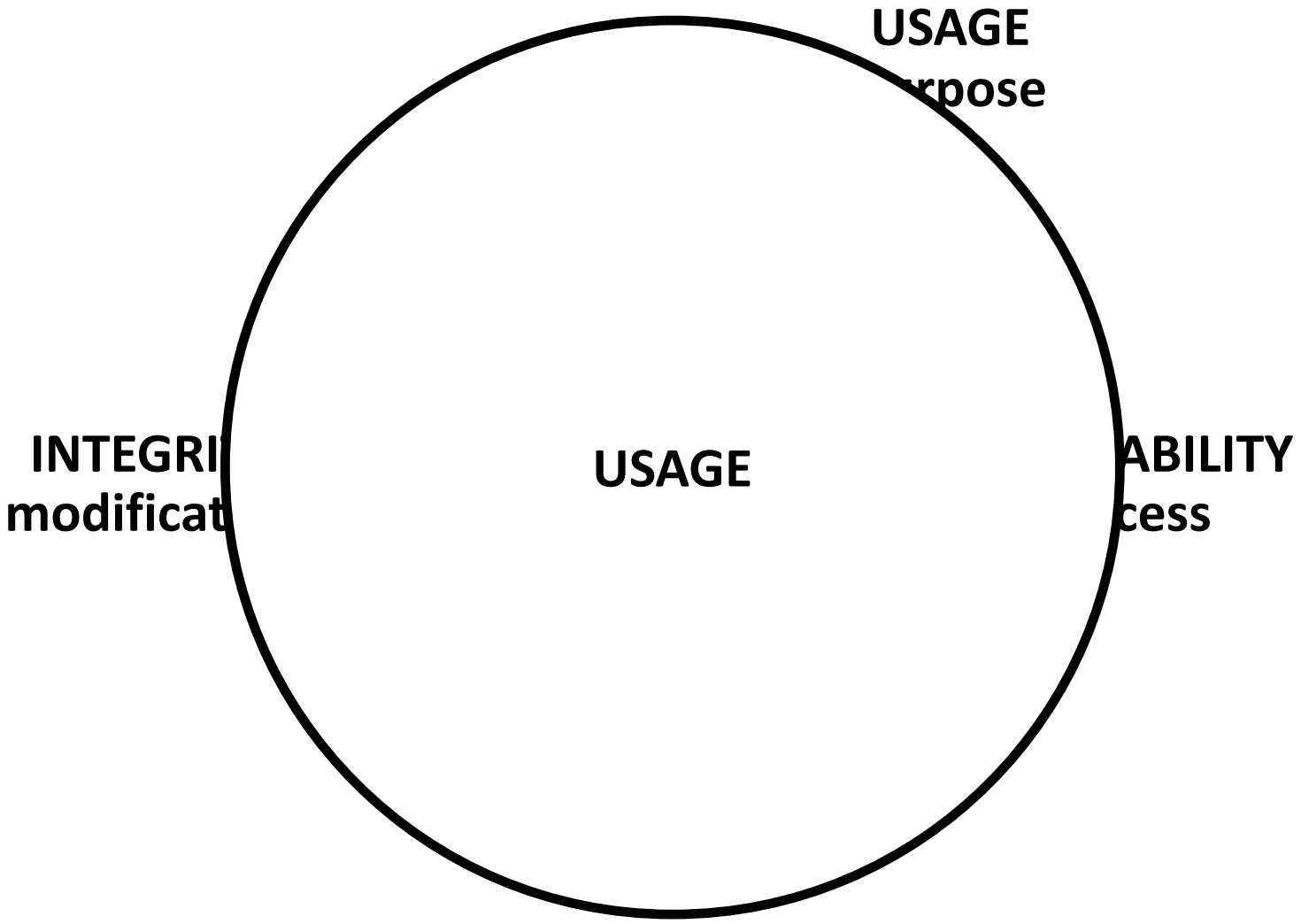
INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

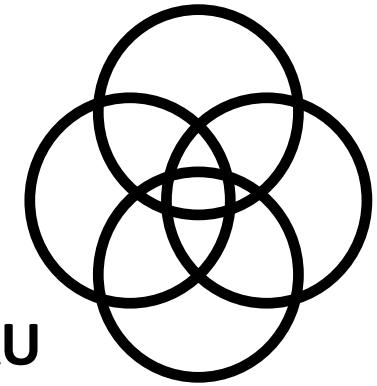
Covers privacy and intellectual property protection

Security Objectives

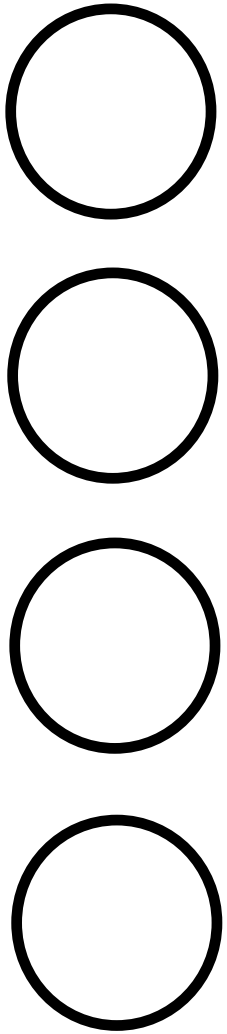


Security Objectives

Cannot have it all
Need to reconcile
with non-Security Objectives



CIAU



Cost

Convenience

Growth

Safety

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure

  Not attainable

- Enable system designers and operators to say:

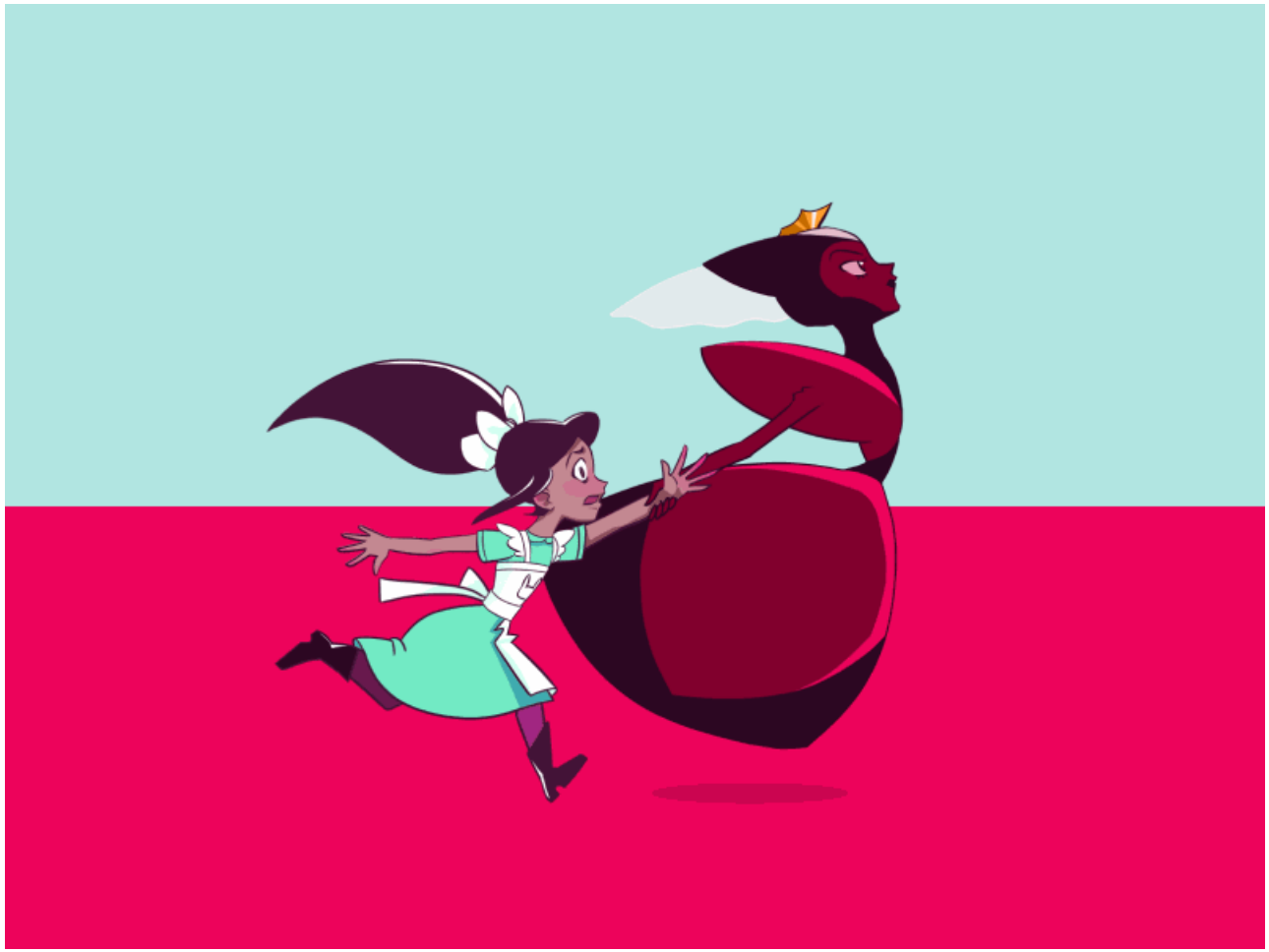
  This system is as secure as it needs to be and no more

  Many successful examples

Cyber Security is Dynamic

"My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that."

— Lewis Carroll, Alice in Wonderland



Cyber Security Big Trends

Single enterprise	**Multiple interacting parties**
Cyber only	**Cyber physical**
Configured	**Automated**
Static	**Adaptive**
Experts	**Naïve users**
Fractured	**Seamless**

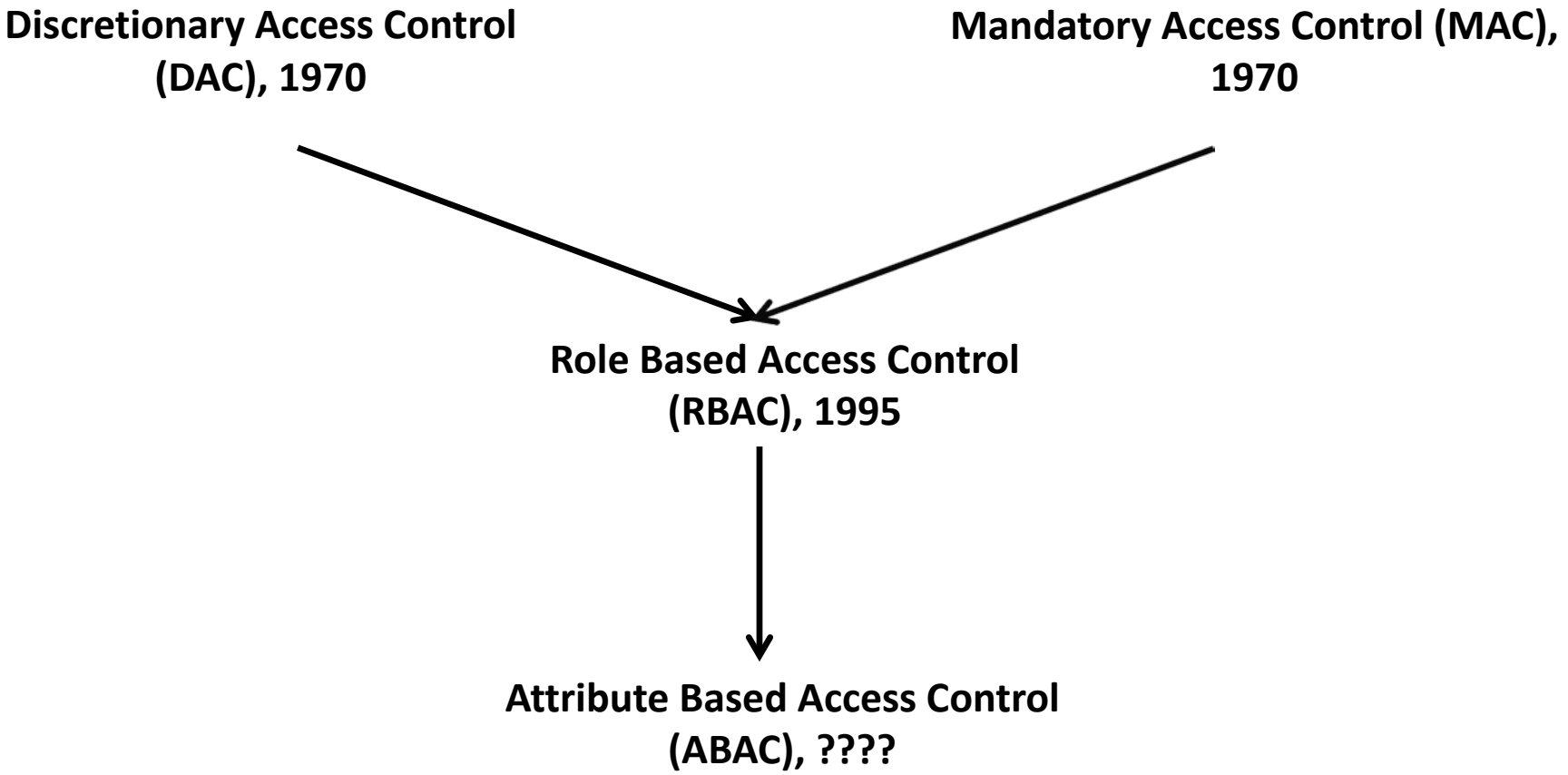
Cryptography

Symmetric Key Cryptography, 1977

Asymmetric Key Cryptography, 1996

BlockChain Applications, ????

Access Control



Discretionary Access Control (DAC)

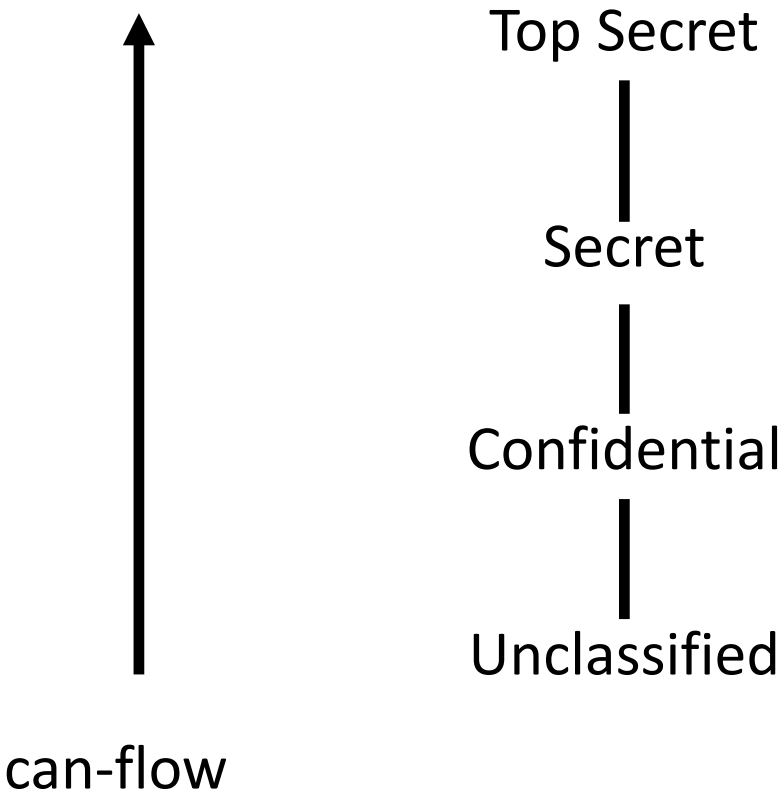
- Core concept:

  Custodian of information determines access

- Core drawback:

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

Mandatory Access Control (MAC)



Mandatory Access Control (MAC)

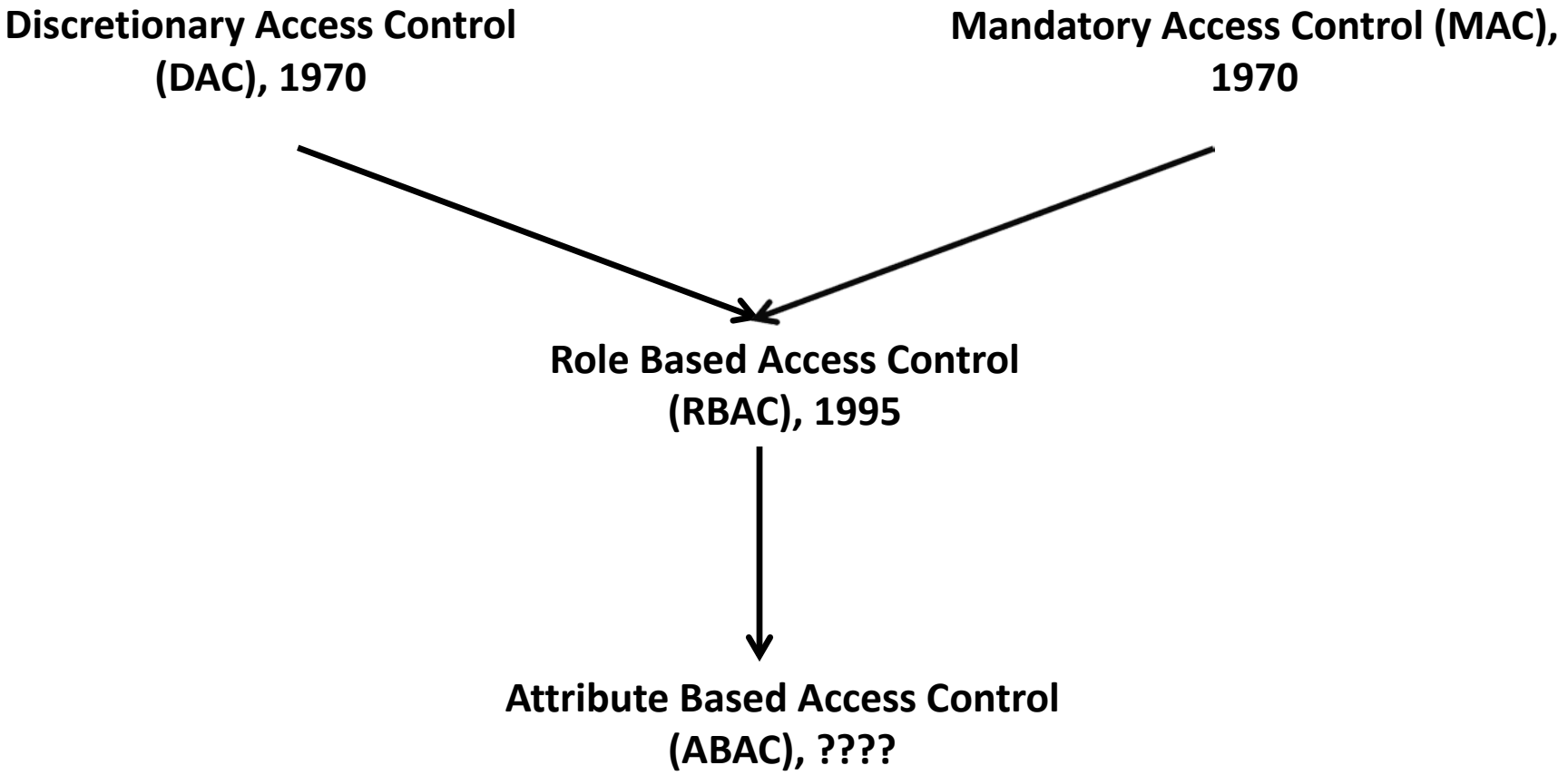
- Core concept:

  Extend control to copies by means of security labels

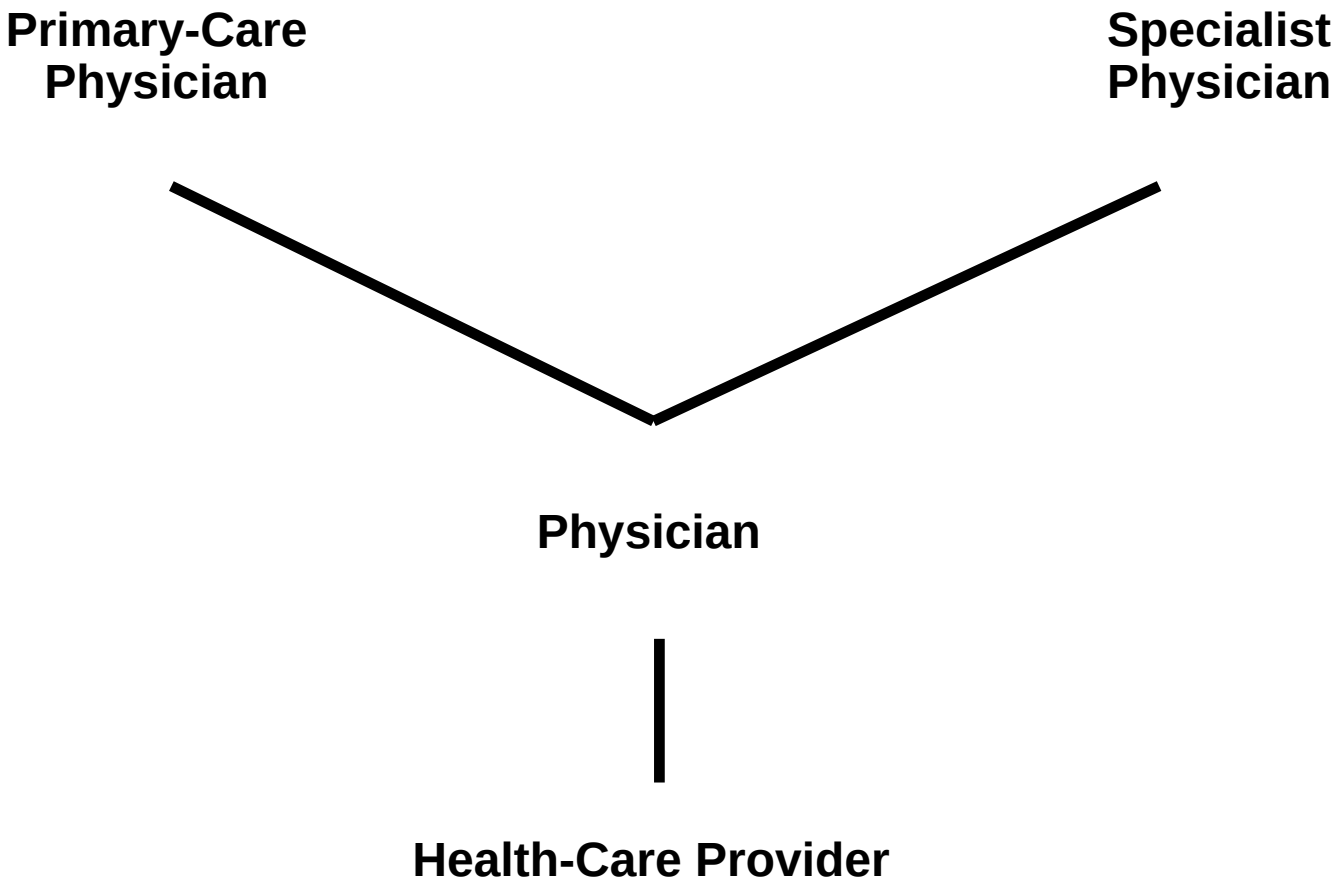
- Core drawback:

  Covert channels can make copies that bypass this control

Access Control



Role-Based Access Control (RBAC)



Role-Based Access Control (RBAC)

- Core concept:

  Roles determine everything

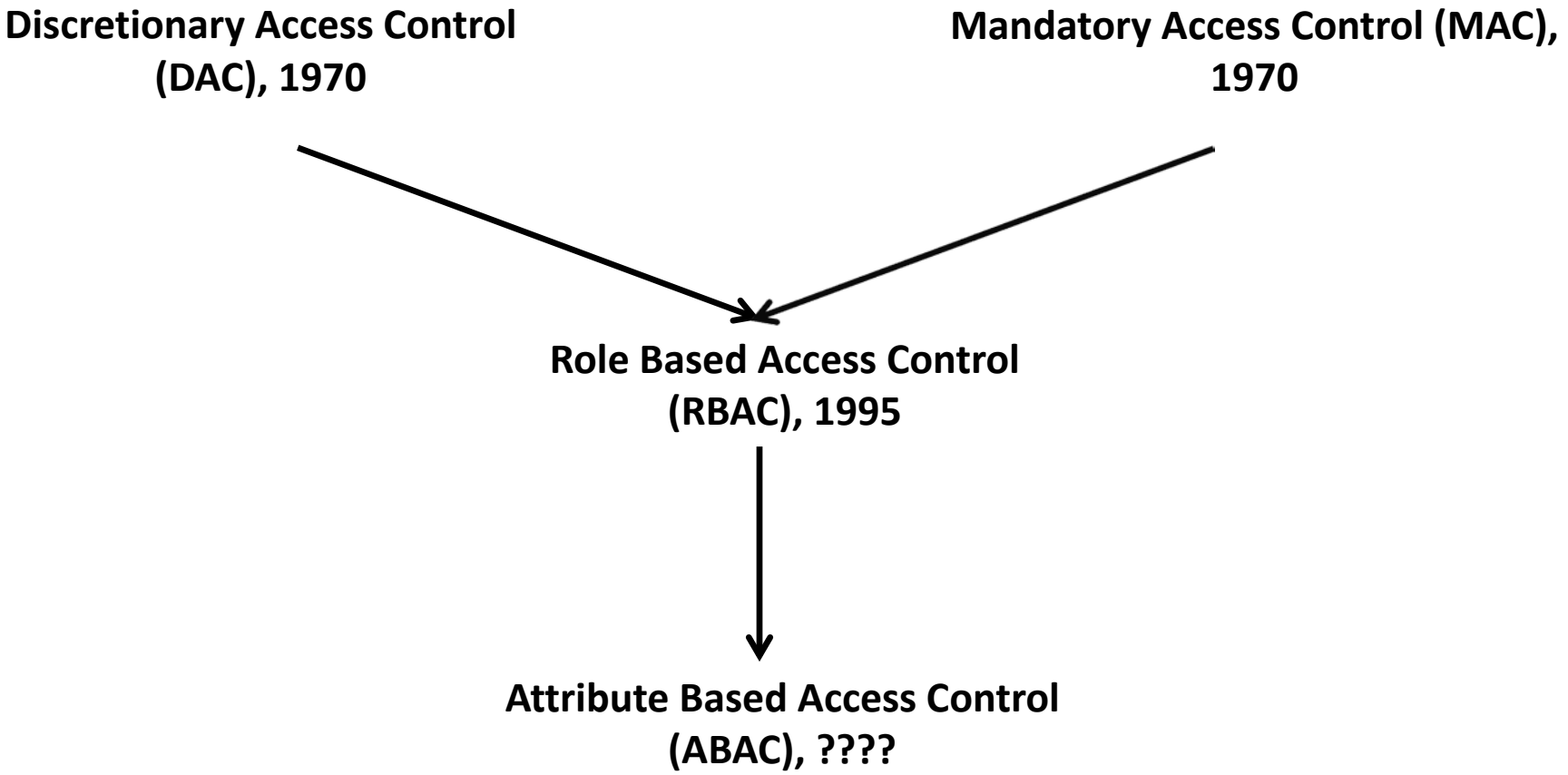
- Core drawback:

  Roles are a natural concept for human users
  But not so natural for:
  Information objects
  IoT things
  Contextual attributes

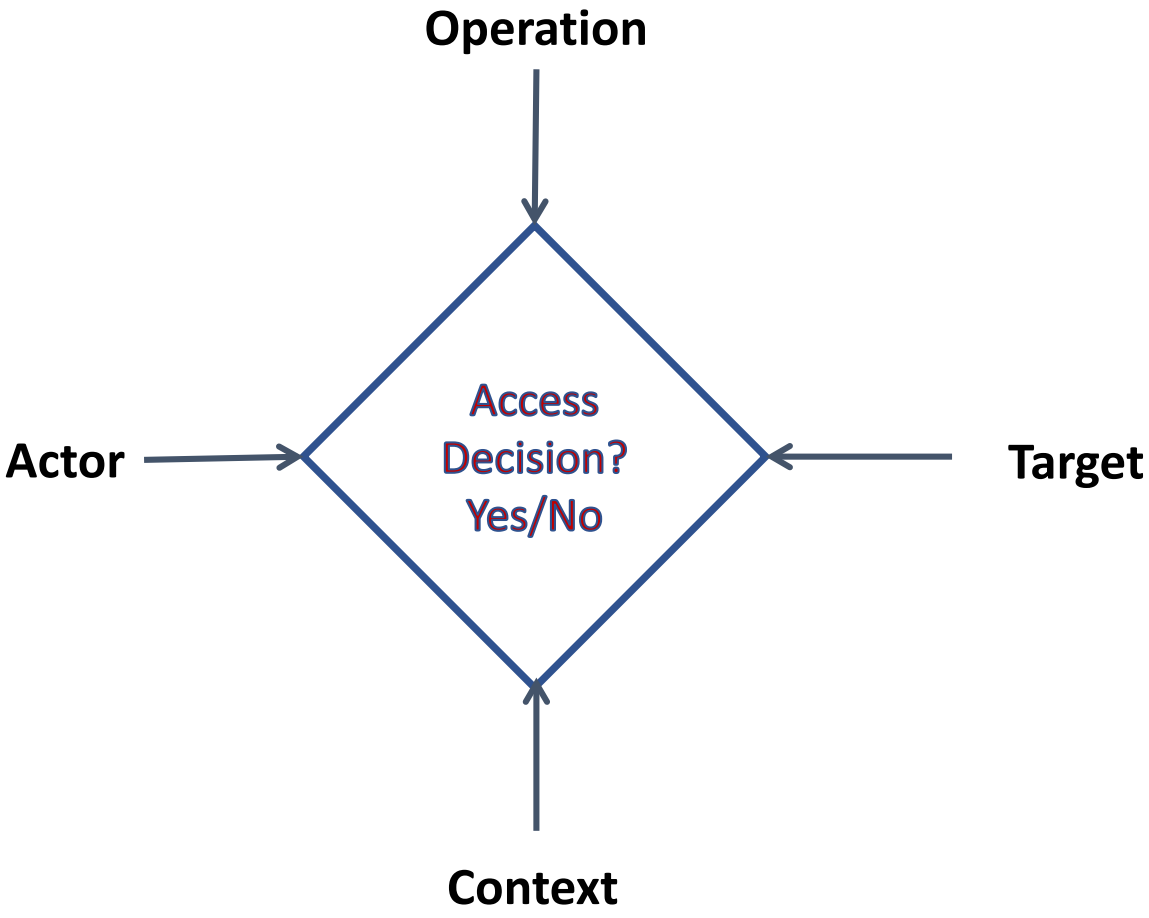
Role-Based Access Control (RBAC)

- 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:

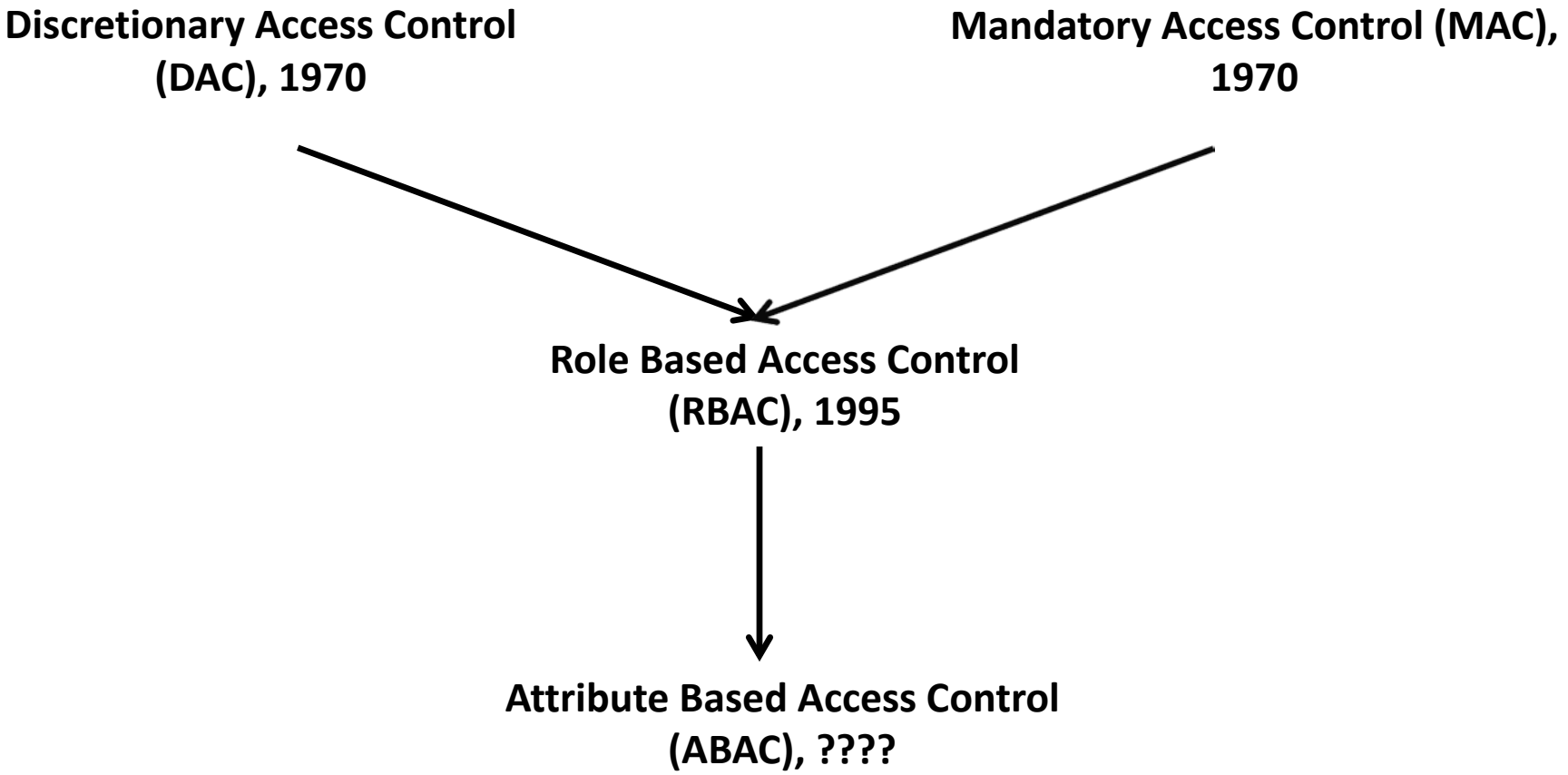
  Attributes determine everything

- Core drawback:

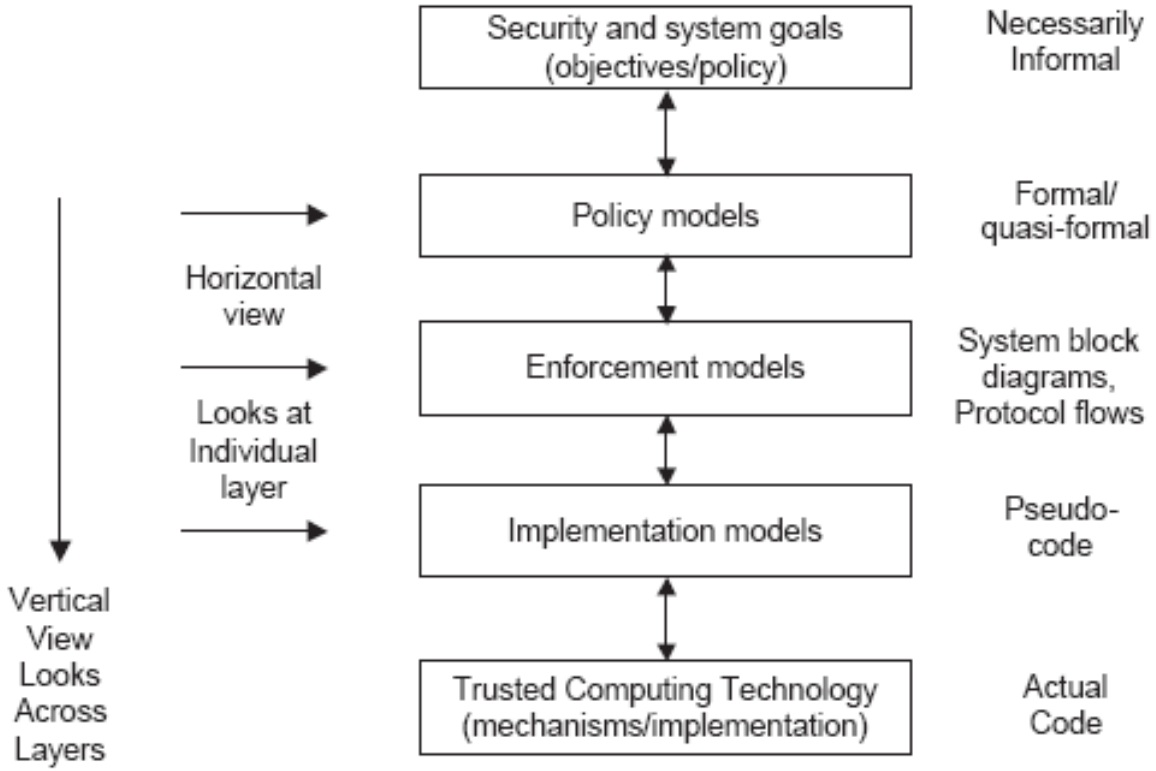
  Flexibility at the cost of complexity

  No fixed access decision rule

Access Control



Access Control PEI Layers

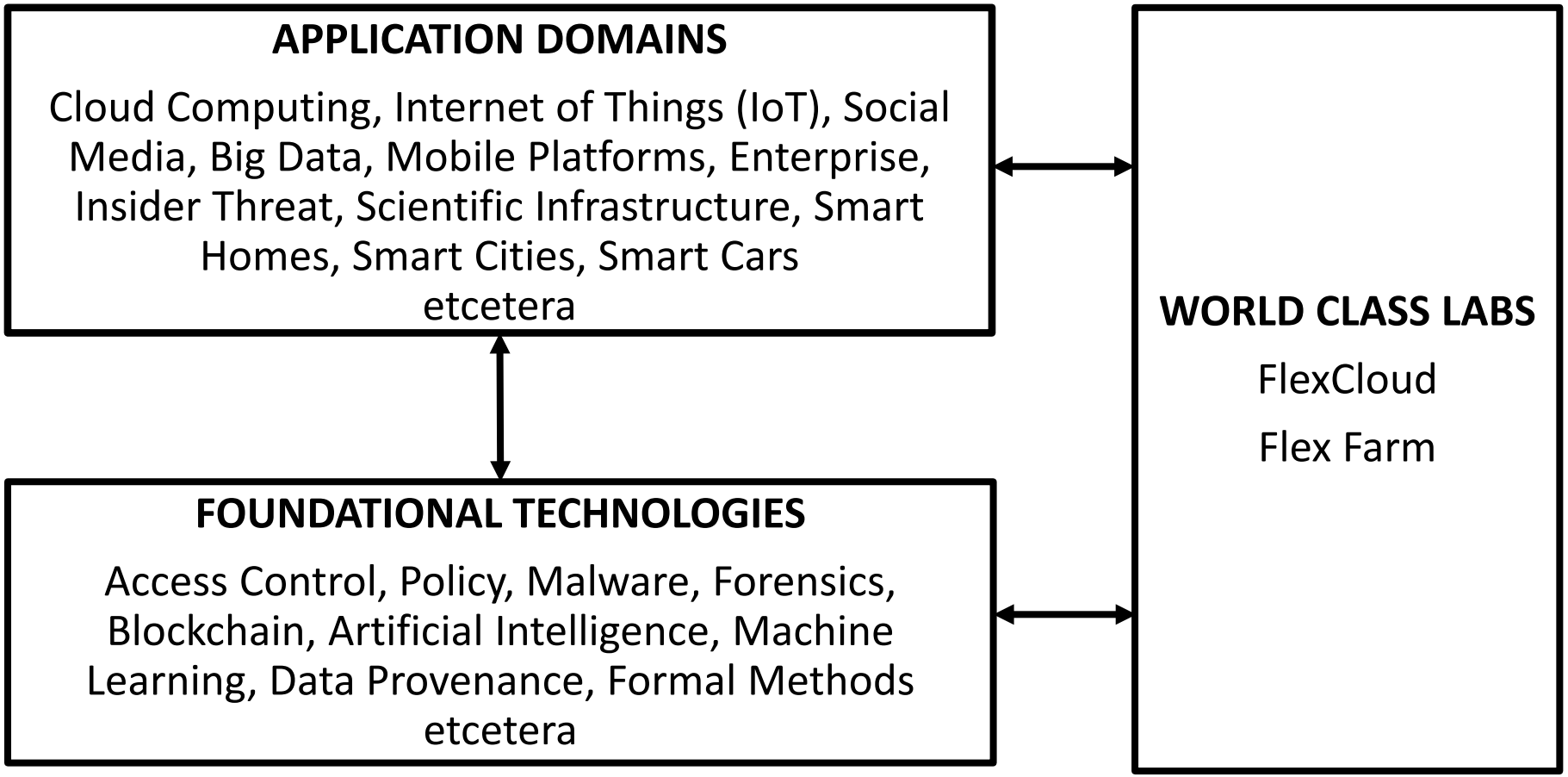


Idealized

Enforceable (Approximate)

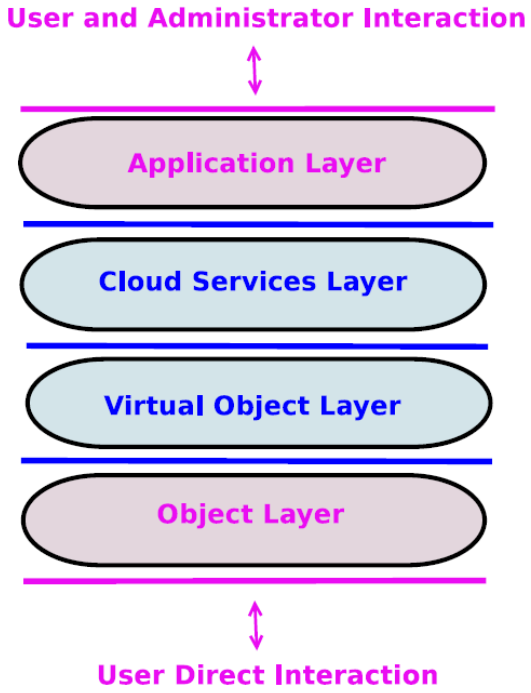
Codeable

ICS Major Research Thrusts

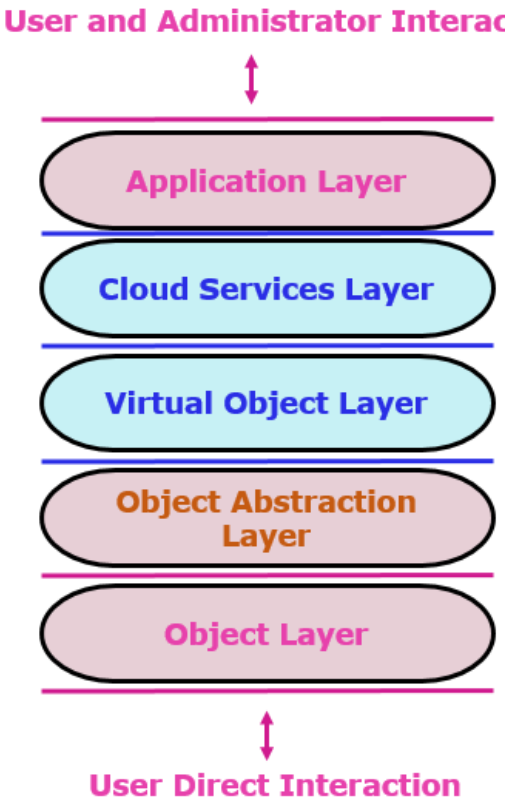


Goal: Broaden and Deepen

Cloud-Enabled IoT (CE-IoT)

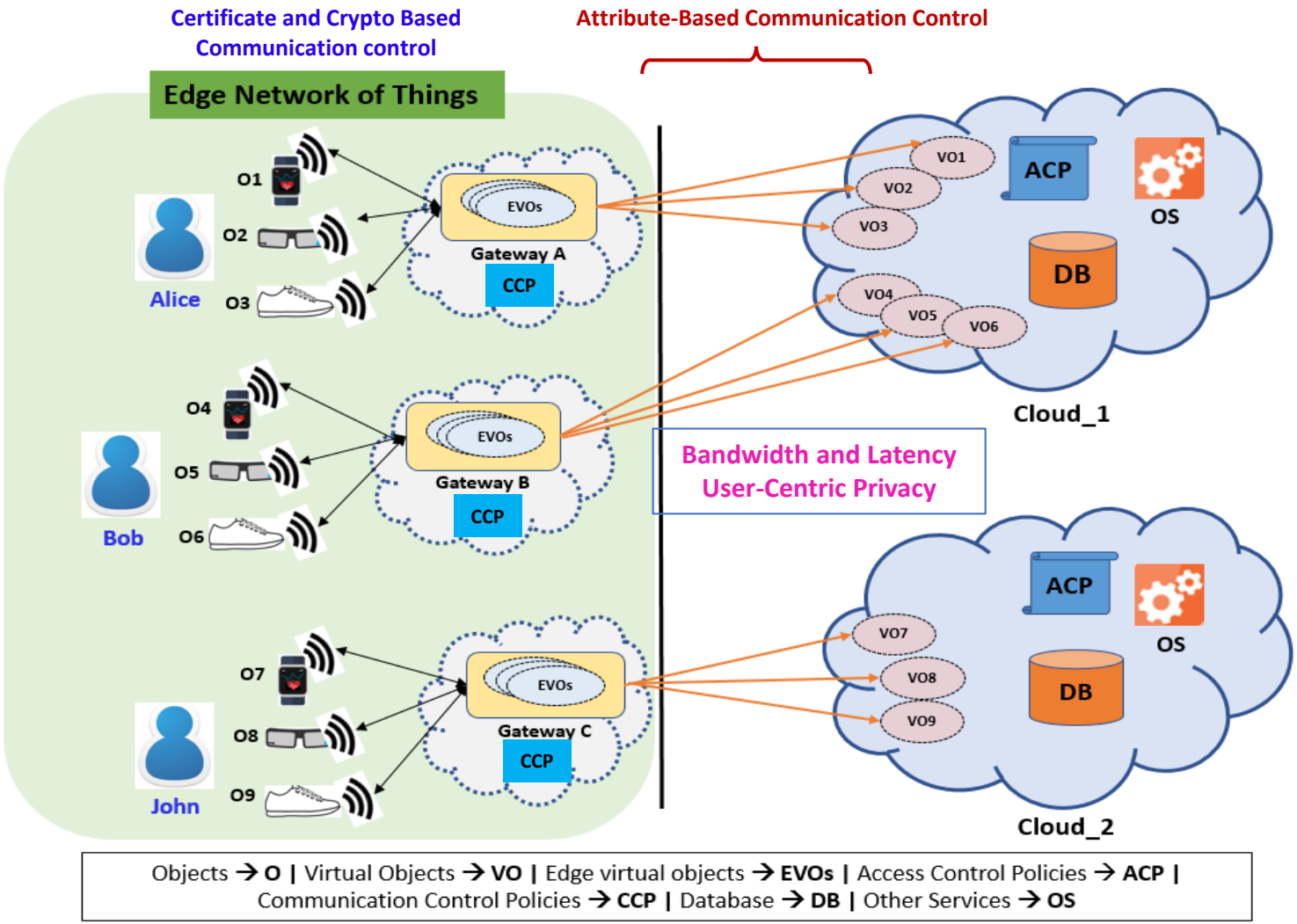


a) Access Control Oriented (ACO) Architecture



b) Enhanced ACO (E-ACO) Architecture

CE-IoT Enforcement Model



Objects → **O** | Virtual Objects → **VO** | Edge virtual objects → **EVOs** | Access Control Policies → **ACP** | Communication Control Policies → **CCP** | Database → **DB** | Other Services → **OS**