

Access Control Convergence: Challenges and Opportunities

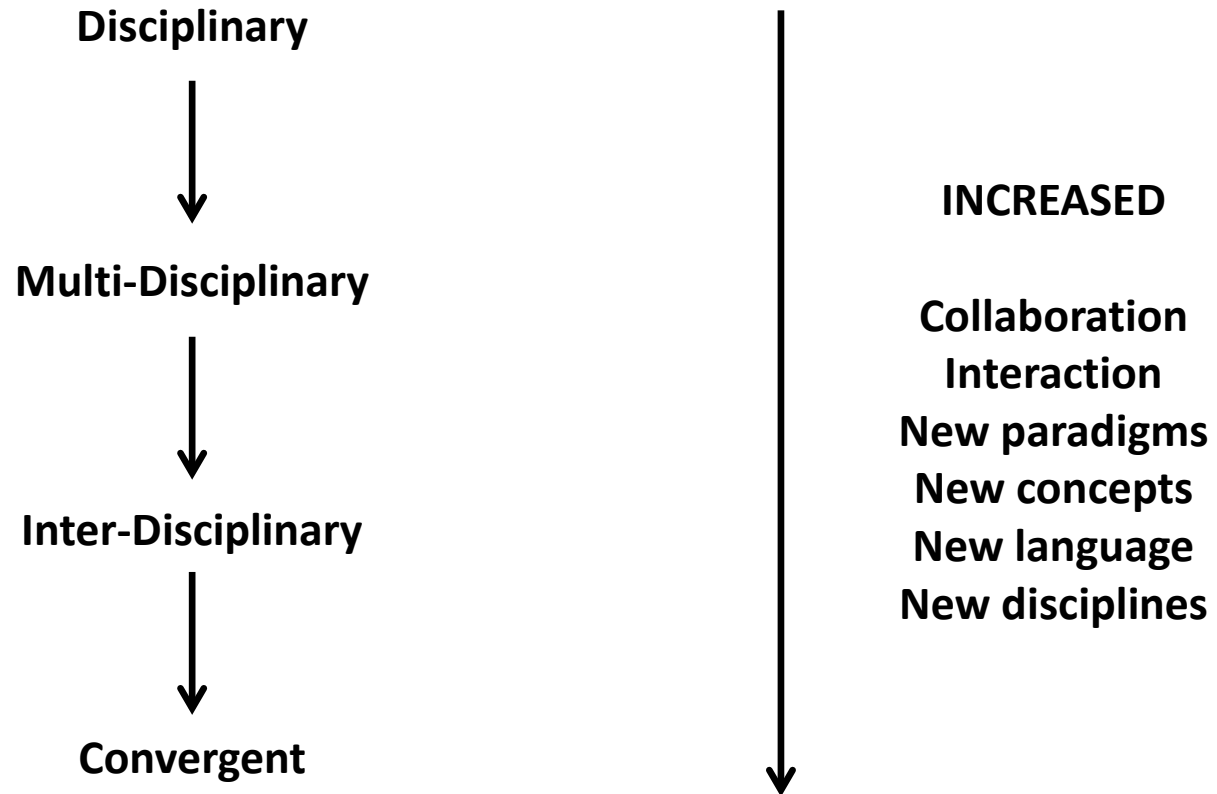
Ravi Sandhu

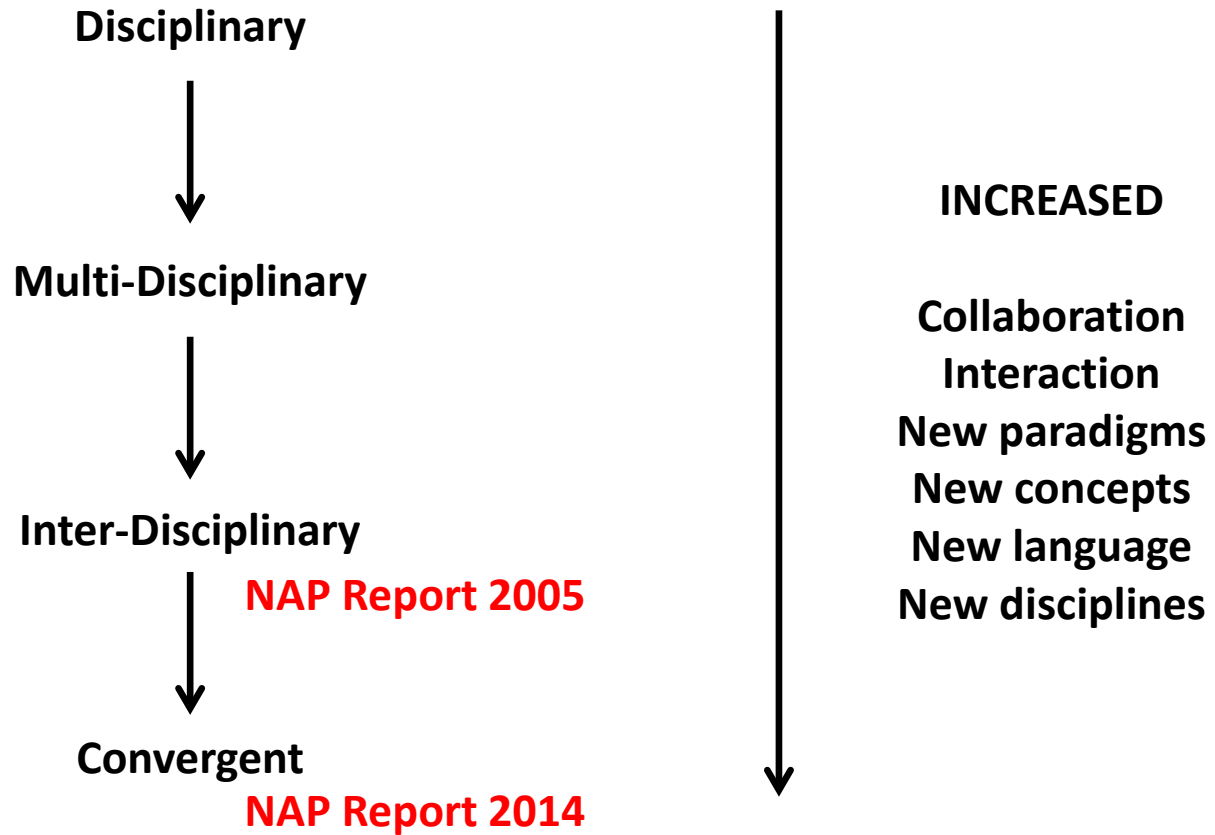
Executive Director and Chief Scientist

Professor of Computer Science
Lutcher Brown Chair in Cyber Security

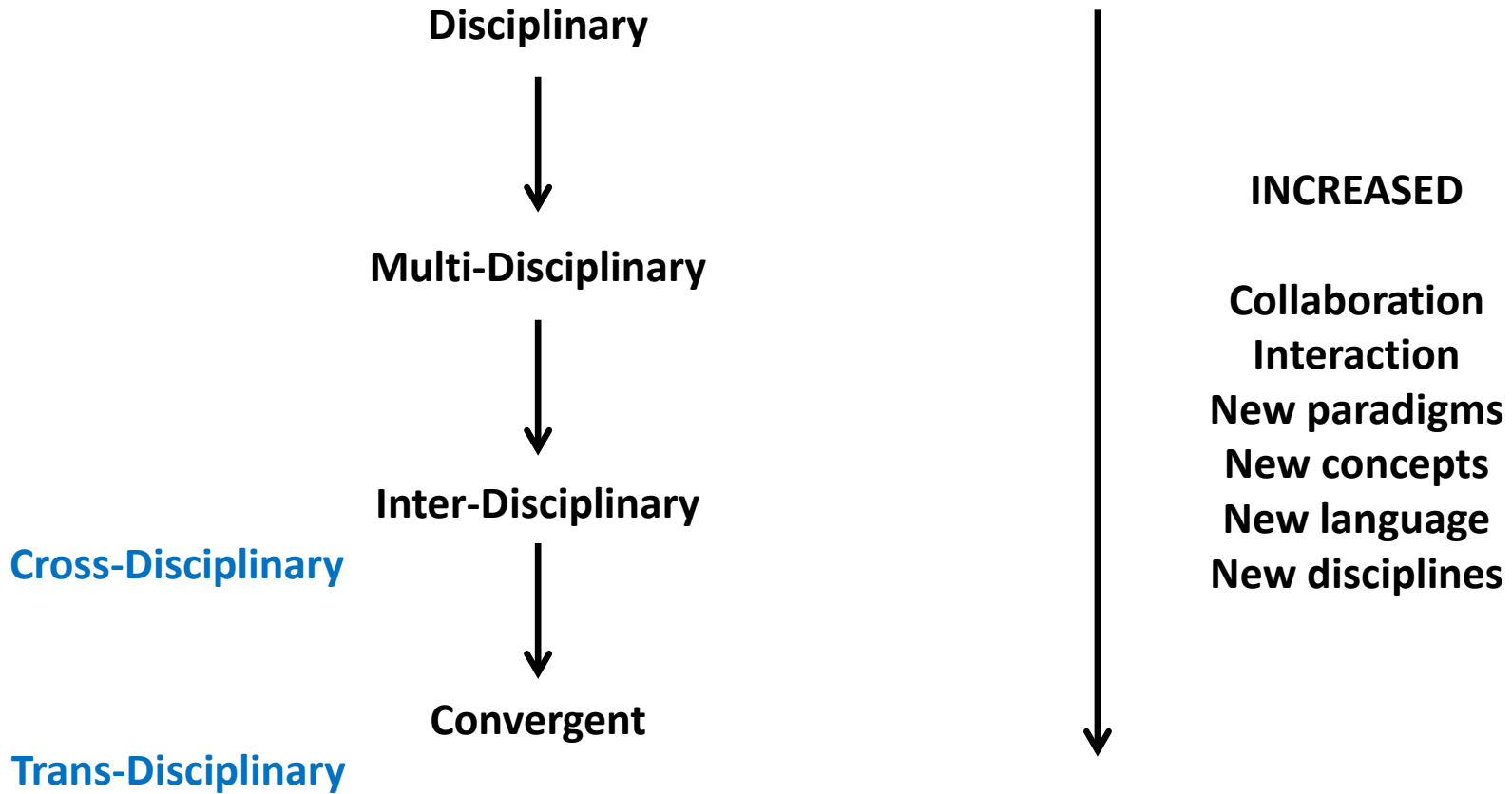
International Conference on Information Systems Security
December 2020

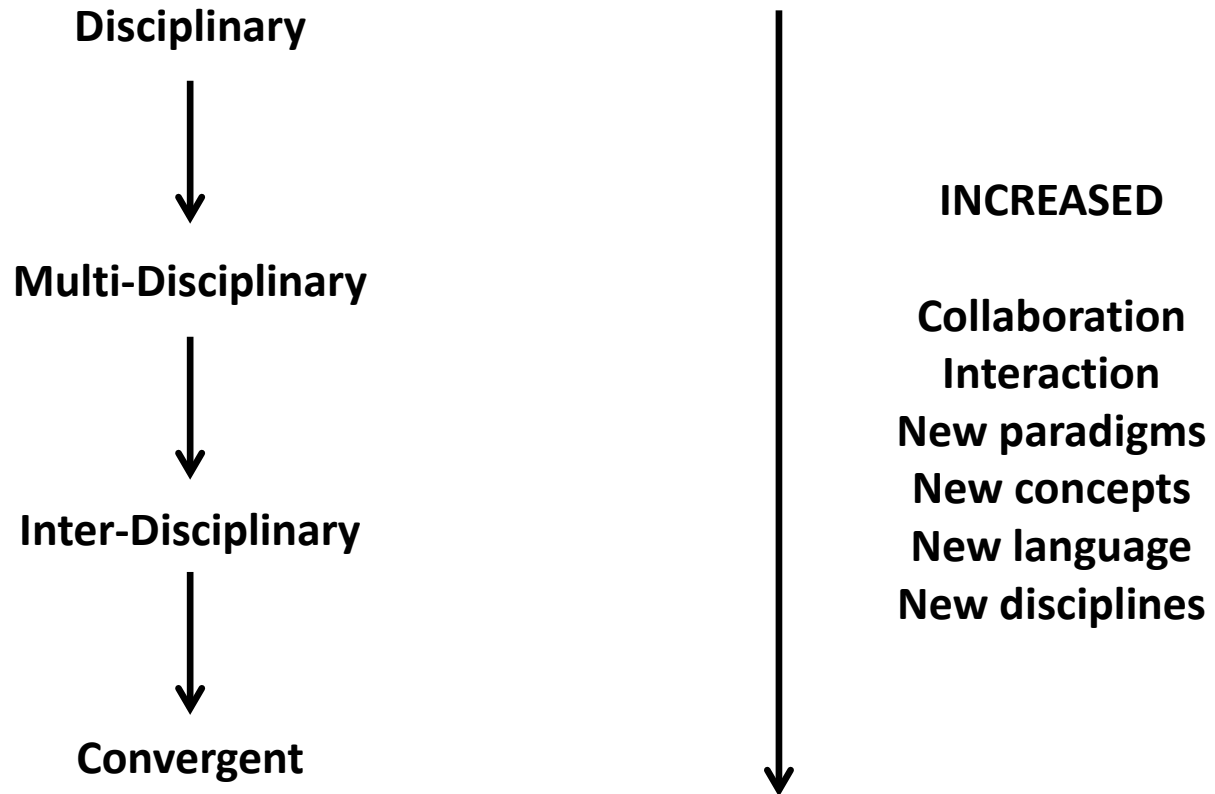
ravi.sandhu@utsa.edu www.ics.utsa.edu www.profsandhu.com





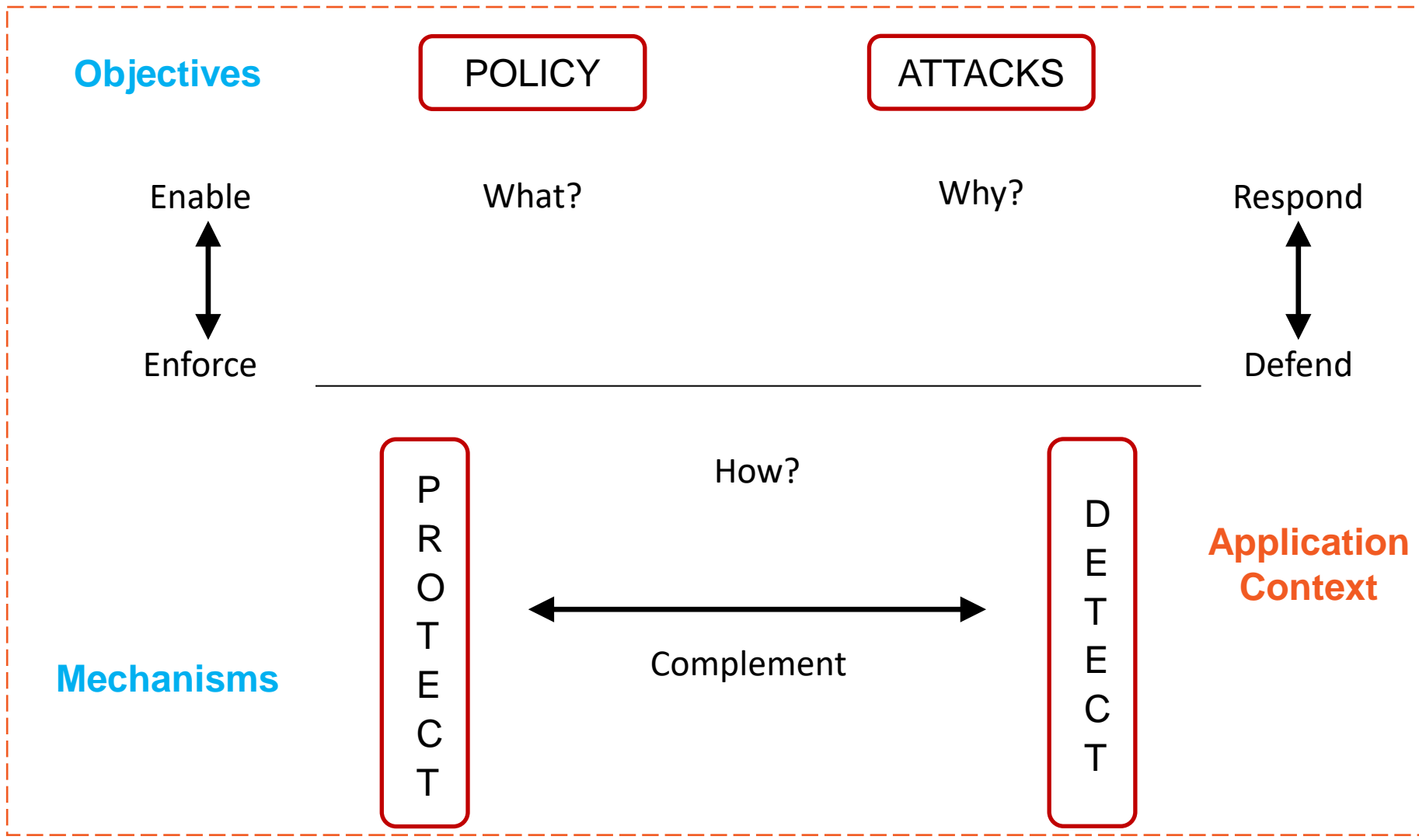
NAP = National Academies Press

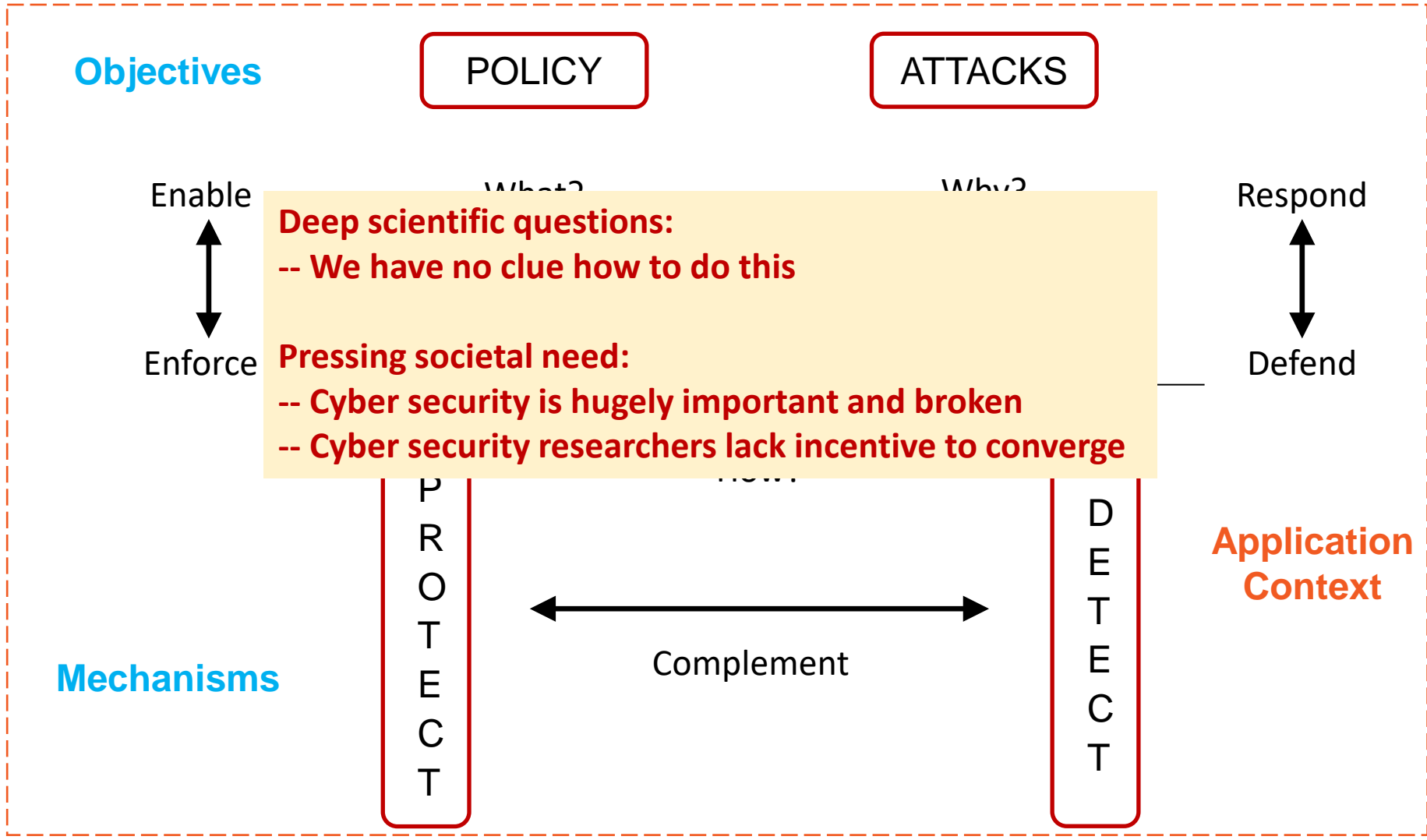


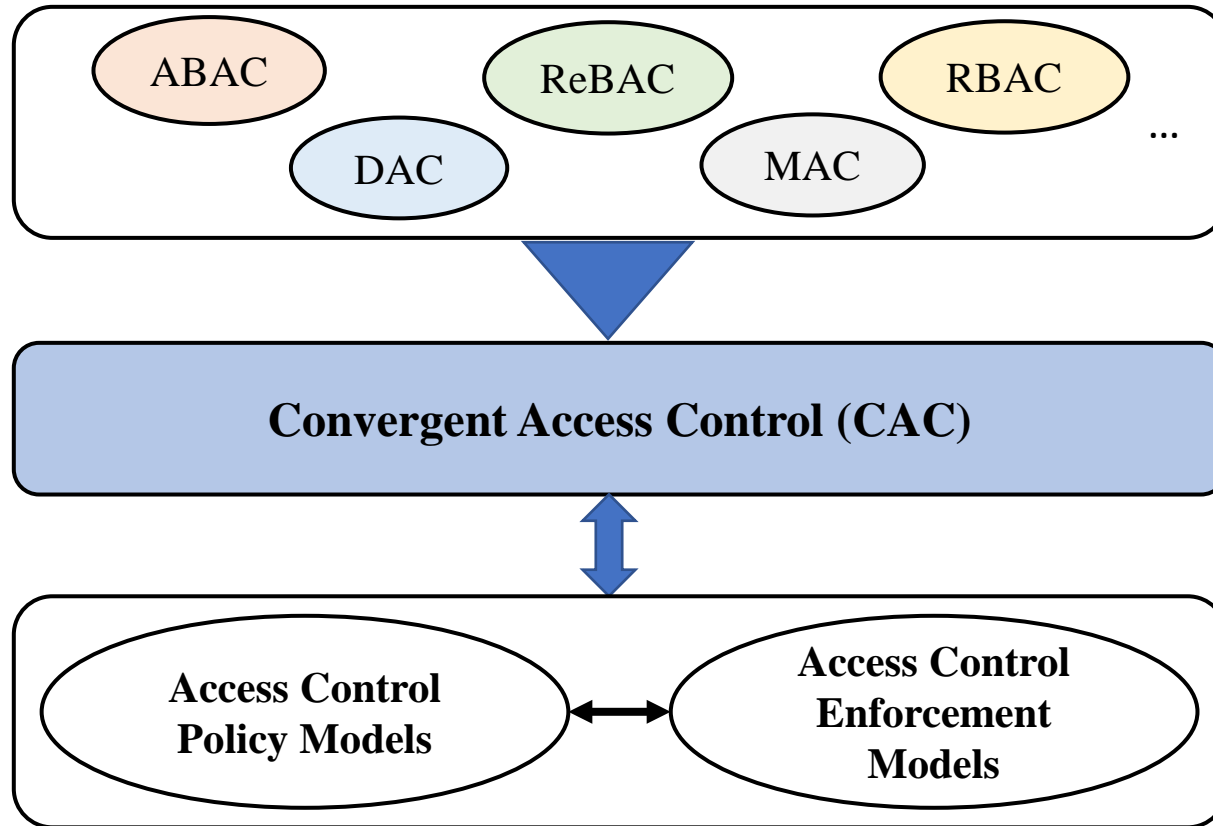


DRIVERS

- **Deep scientific questions**
- **Pressing societal needs**







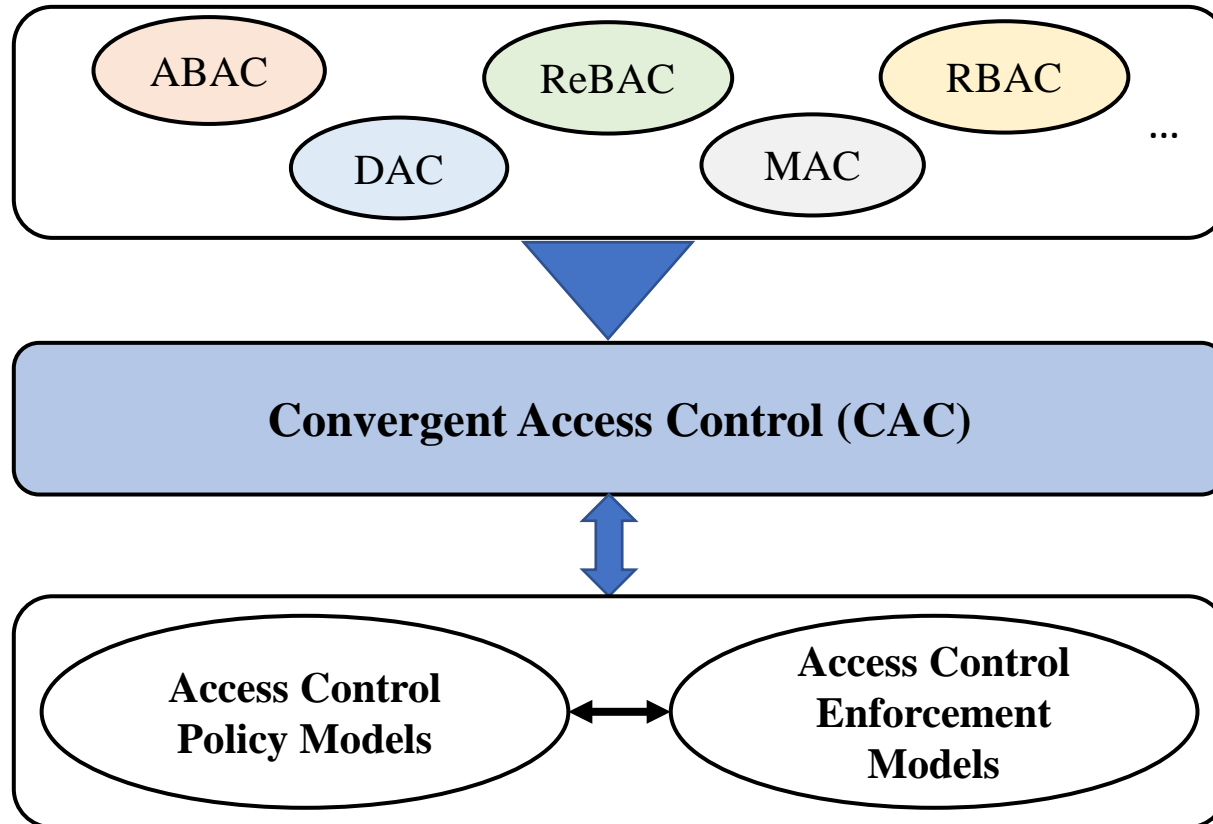
Deep scientific questions:

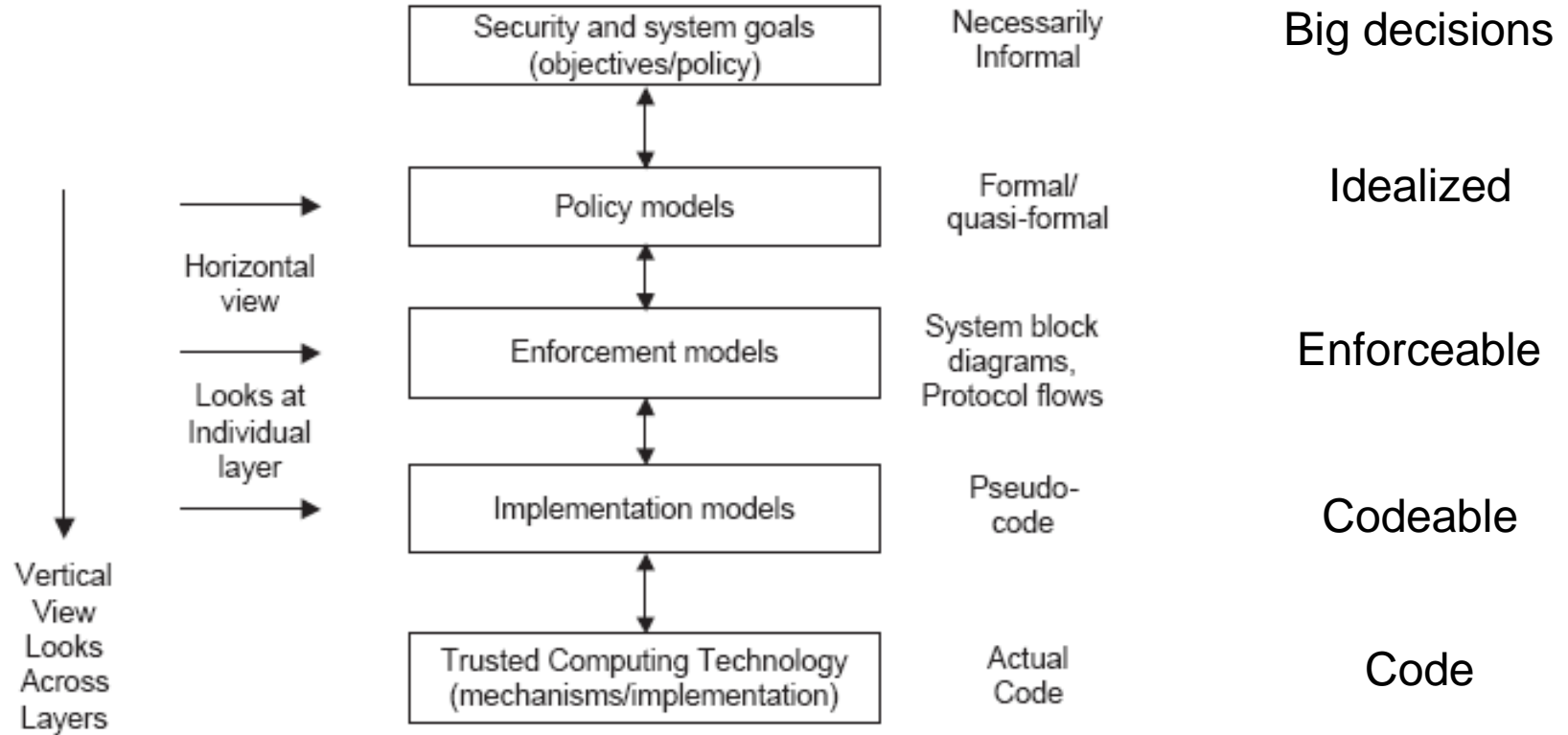
- We have no clue how to do this
- Will revisit at end of talk

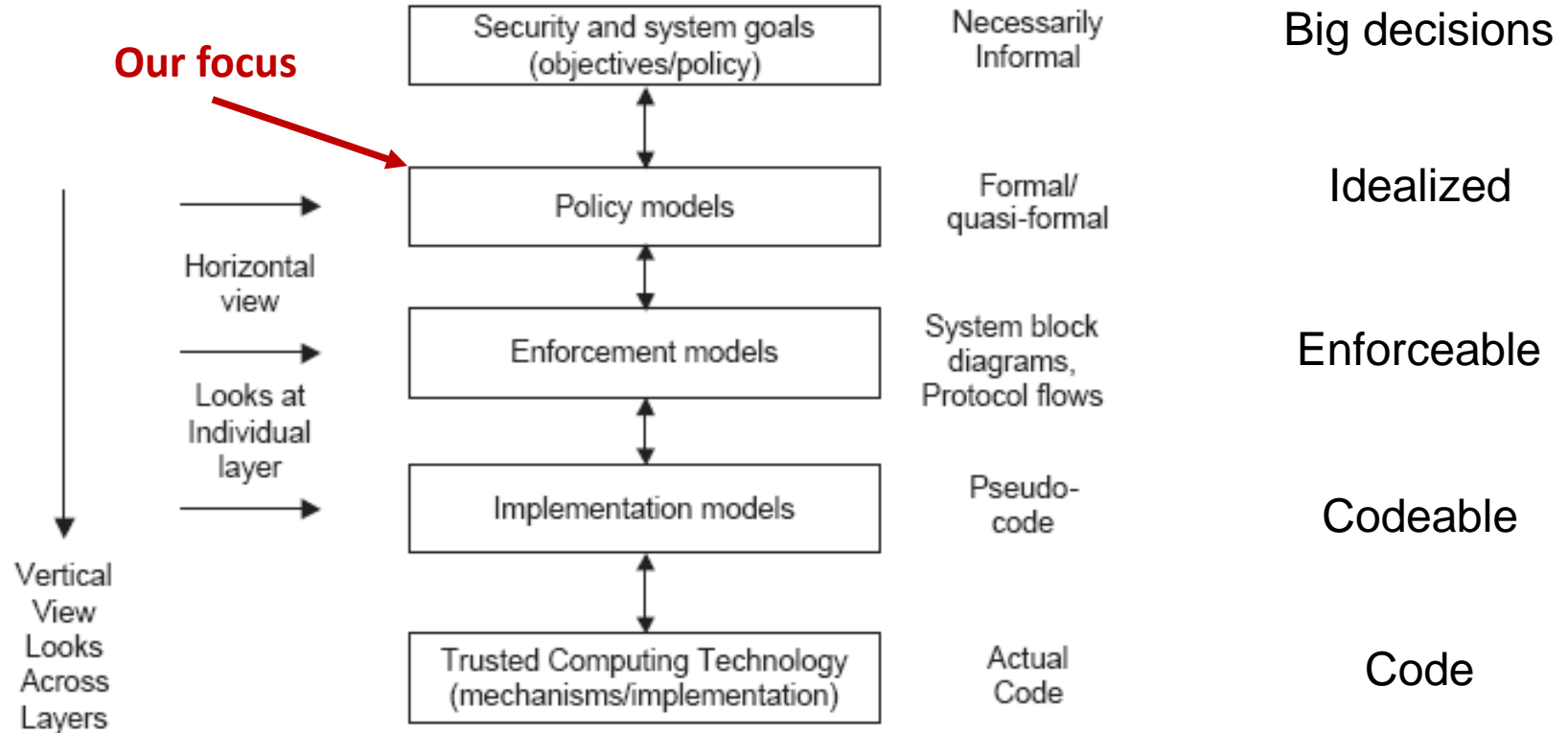
Pressing societal need:

- Cyber security is hugely important and broken
- Access control is an essential piece to secure modern cyber applications: IoT, CPS, smart communities, ...
- Cyber security researchers have no incentive to converge
- Convergence may be easier in Access Control vs all of cyber security

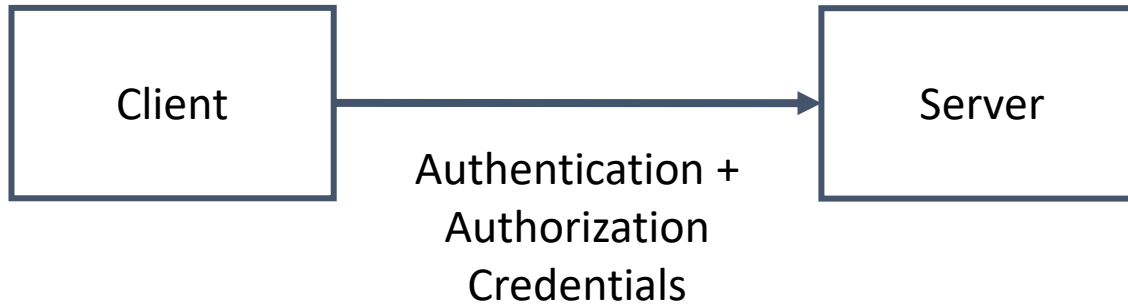




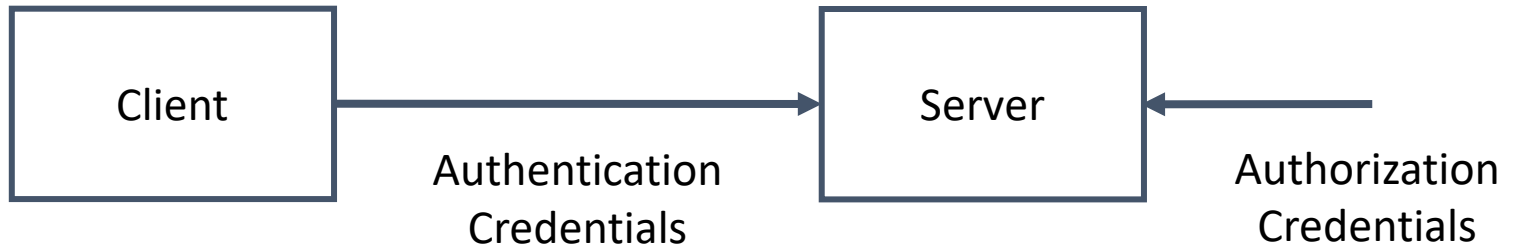


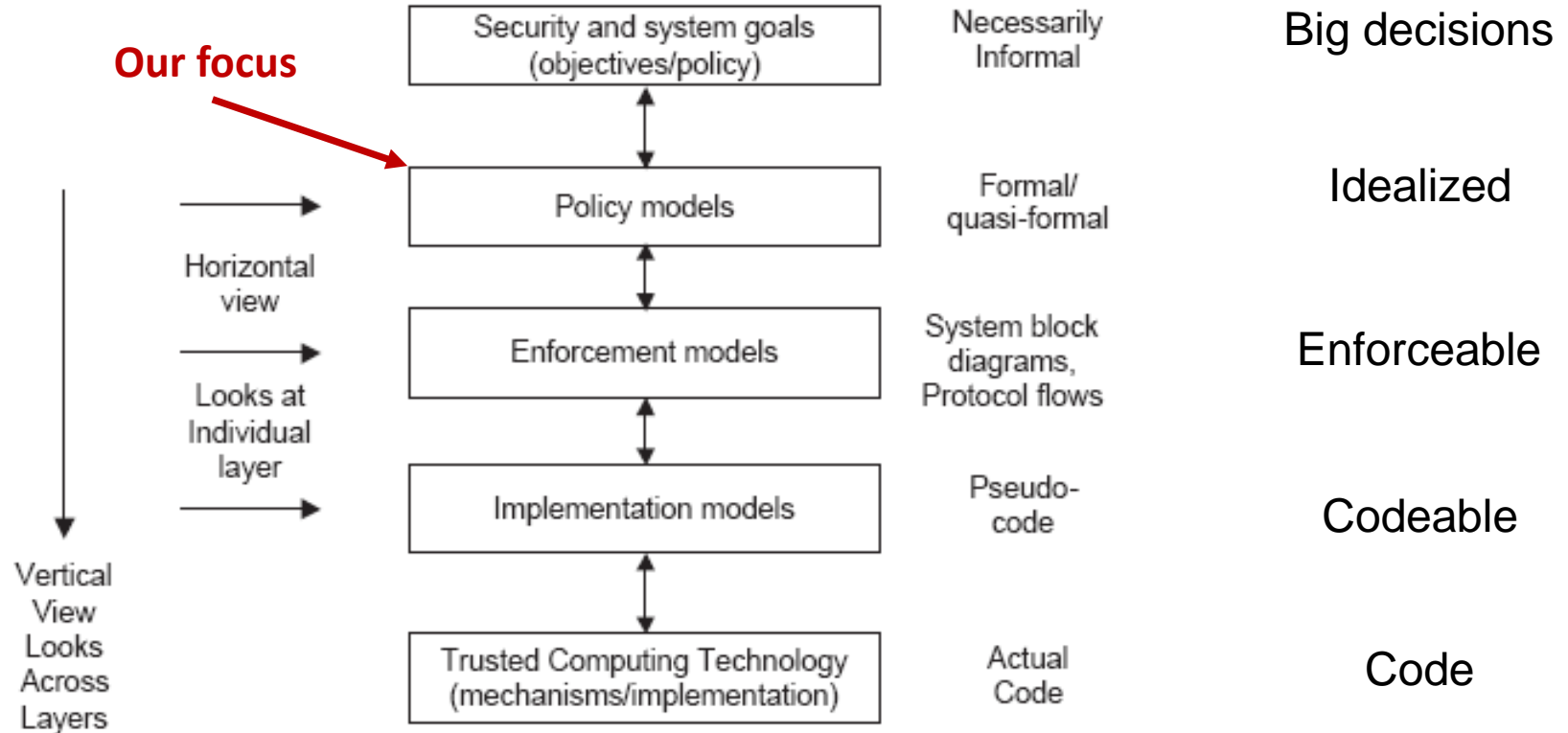


**PUSH
MODEL**



**PULL
MODEL**





Discretionary Access Control (DAC)

1970

Mandatory Access Control (MAC)

1970



Role Based Access Control (RBAC)

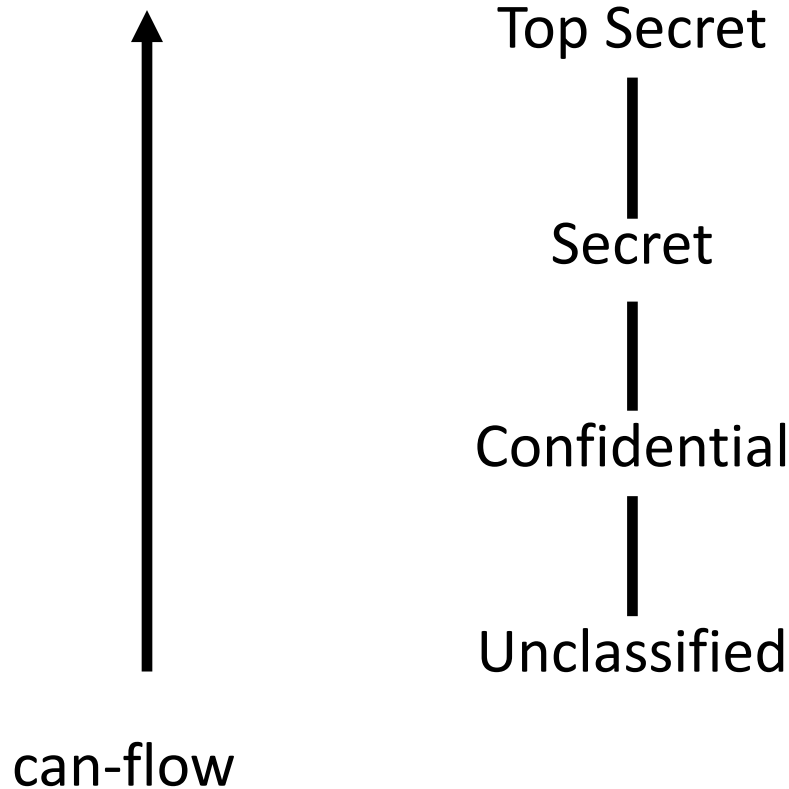
1995



**Attribute Based Access Control (ABAC)
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)**

2020s (Hopefully)

- 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



- 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

Discretionary Access Control (DAC)

1970

Mandatory Access Control (MAC)

1970



Role Based Access Control (RBAC)

1995



**Attribute Based Access Control (ABAC)
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)**

2020s (Hopefully)

- 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

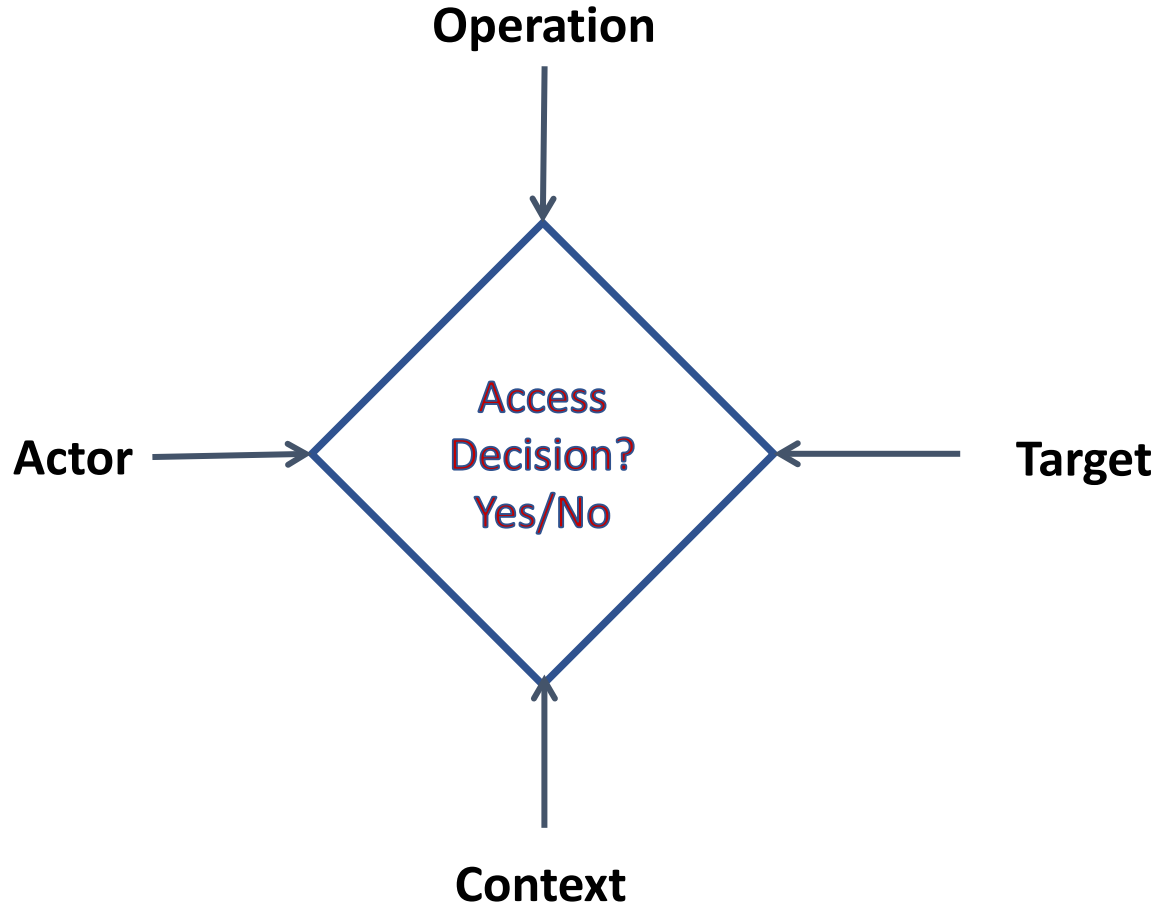
Discretionary Access Control (DAC)
1970

Mandatory Access Control (MAC)
1970



Role Based Access Control (RBAC)
1995

Attribute Based Access Control (ABAC)
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)
2020s (Hopefully)



- 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

Discretionary Access Control (DAC)

1970

Mandatory Access Control (MAC)

1970



Role Based Access Control (RBAC)

1995



Attribute Based Access Control (ABAC)
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)

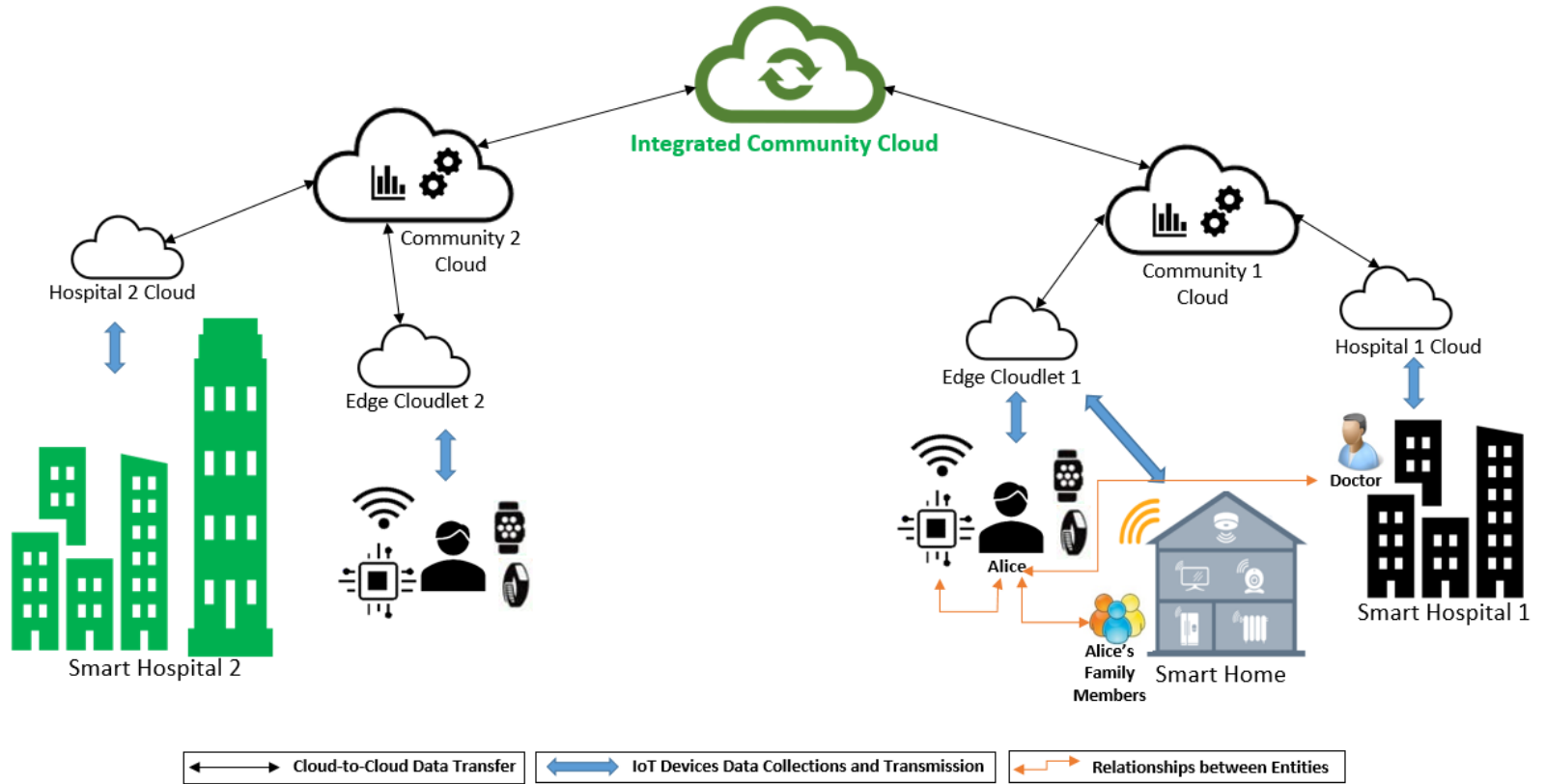
2020s (Hopefully)

- Rich set of building blocks:
DAC, MAC, RBAC, ABAC, ReBAC, UCON
- We have some understanding of the relationships amongst these

- Rich set of building blocks:
DAC, MAC, RBAC, ABAC, ReBAC, UCON
- We have some understanding of the relationships amongst these
- Do we need more building blocks?
- We have very little understanding of synergy amongst these

- Rich set of building blocks:
DAC, MAC, RBAC, ABAC, ReBAC, UCON
 - We have some understanding of the relationships amongst these
 - Do we need more building blocks?
 - We have very little understanding of synergy amongst these
- Deep scientific question
for convergent research**

- Rich set of building blocks:
DAC, MAC, RBAC, ABAC, ReBAC, UCON
 - We have some understanding of the relationships amongst these
 - Do we need more building blocks?
 - We have very little understanding of synergy amongst these
- Pressing societal need? Deep scientific question for convergent research



Entities (e.g., Users and Devices) have attributes along with other environmental attributes and may have associated roles and capabilities in Smart Communities

