I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

Access Control Convergence: Challenges and Opportunities

Ravi Sandhu

Executive Director and Chief Scientist

Institute for Cyber Security

Professor of Computer Science
Lutcher Brown Chair in Cyber Security

UBISEC

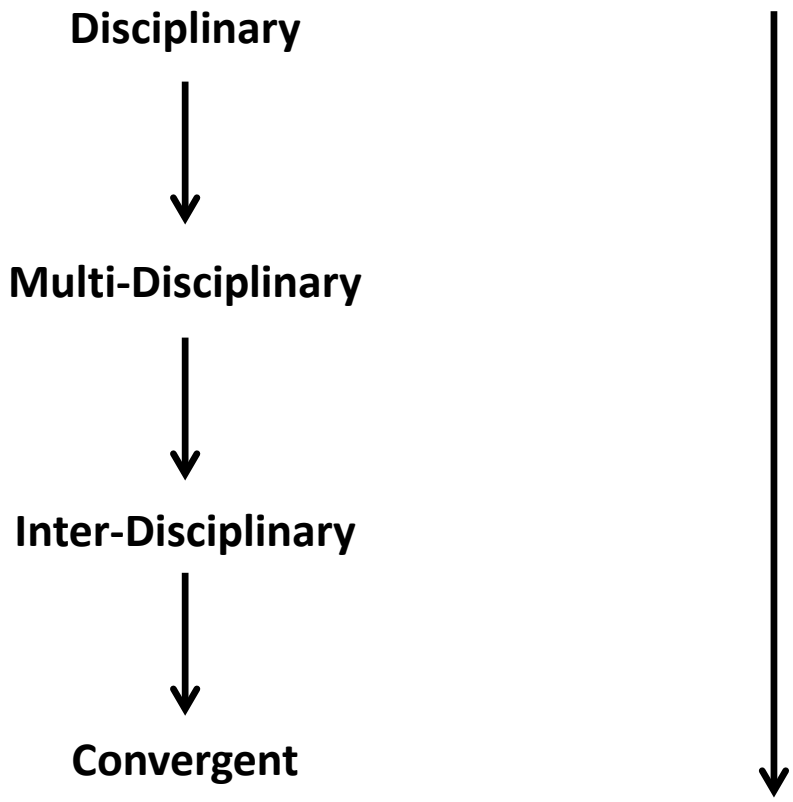
December 29, 2021

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

World-Leading Research with Real-World Impact!

UTSA Computer Science

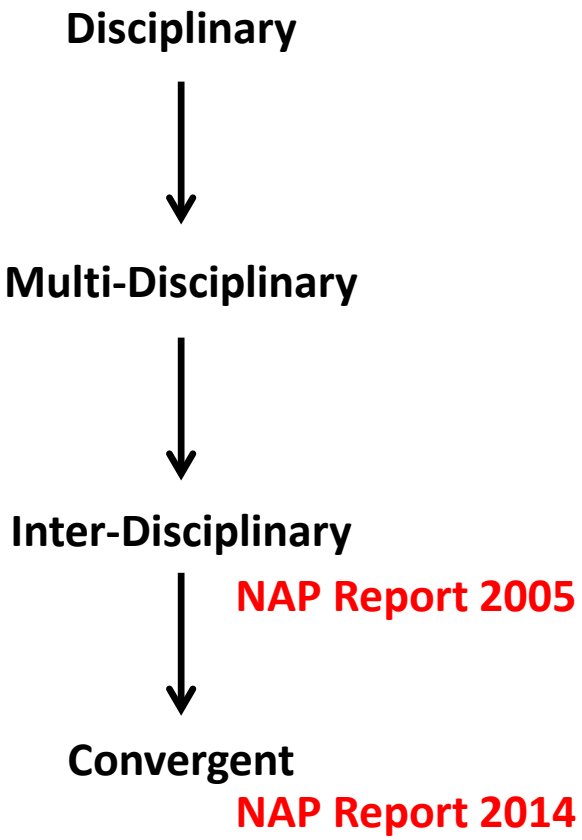
Convergent Research



INCREASED

Collaboration
Interaction
New paradigms
New concepts
New language
New disciplines

Convergent Research

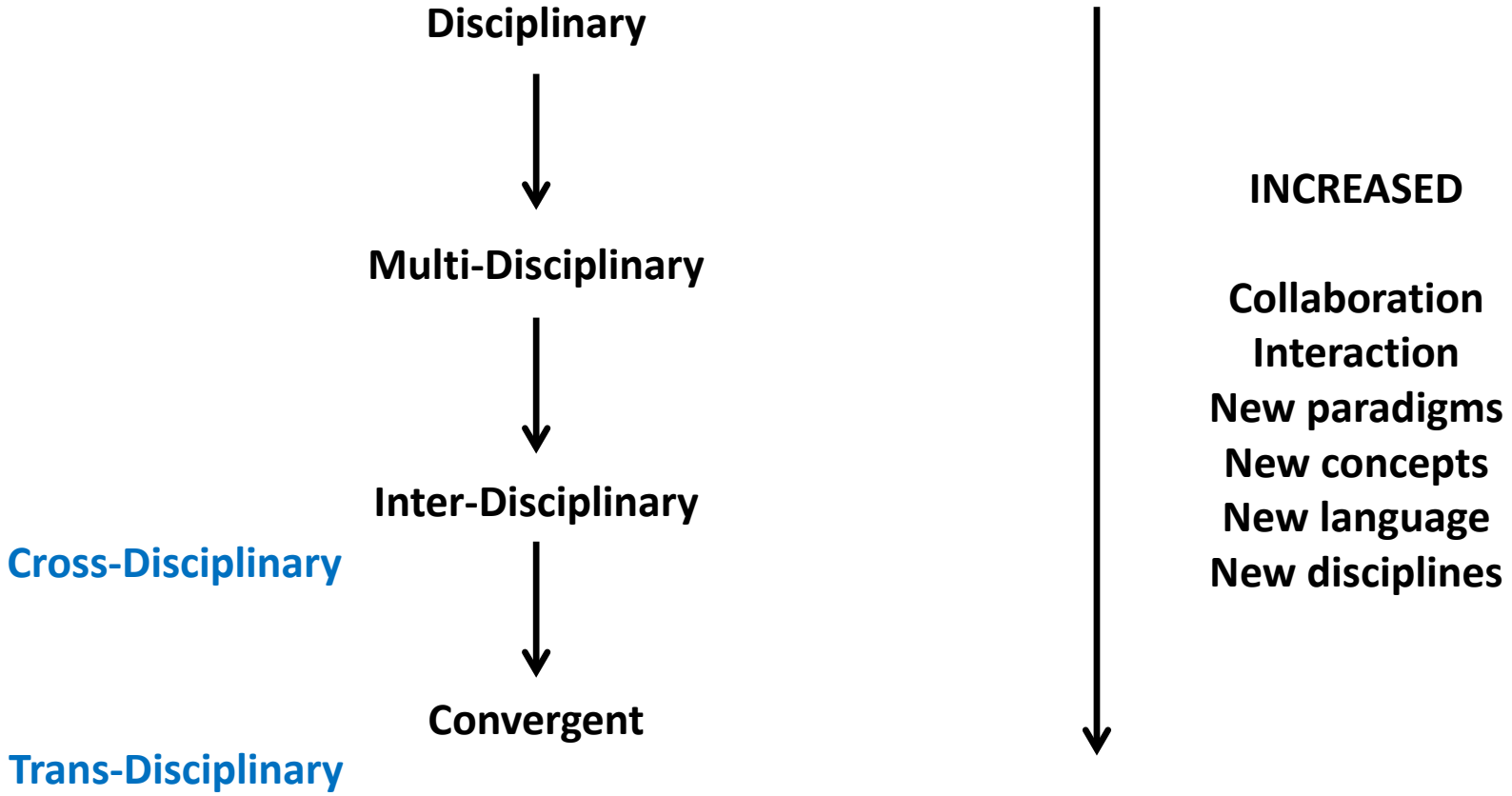


INCREASED

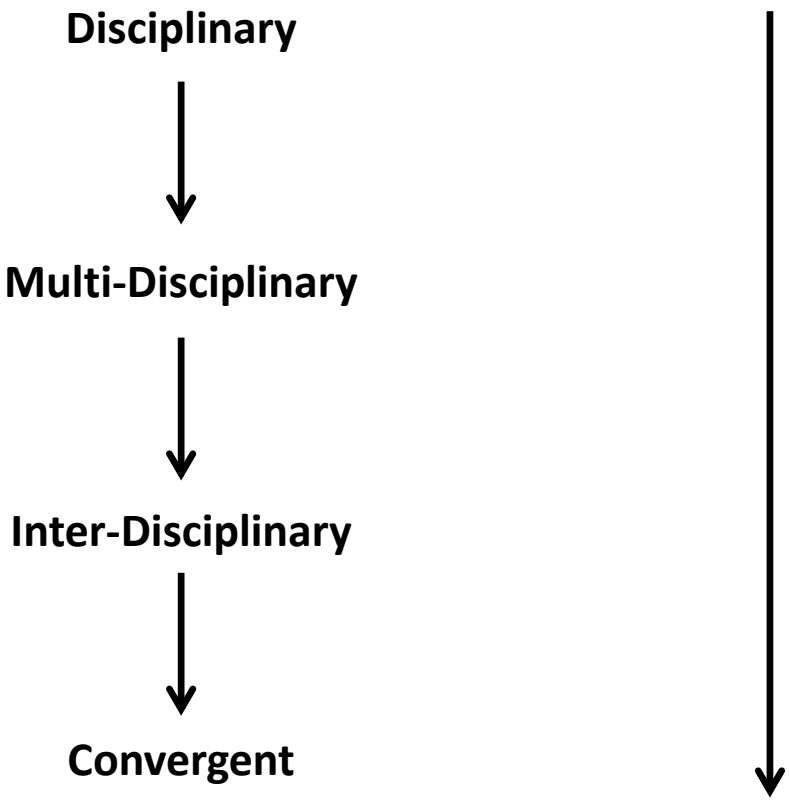
Collaboration
Interaction
New paradigms
New concepts
New language
New disciplines

NAP = National Academies Press

Convergent Research



Convergent Research



INCREASED

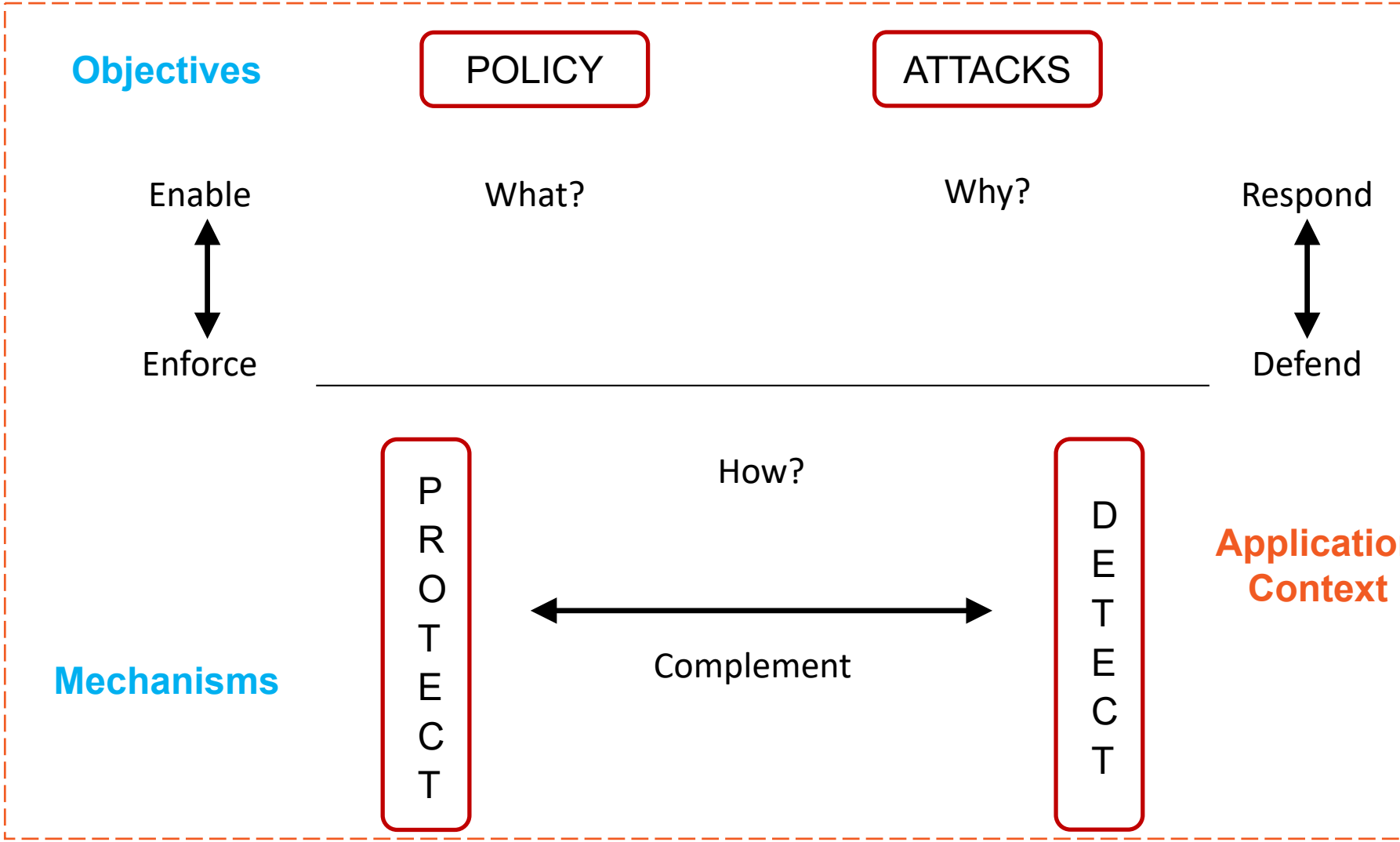
Collaboration
Interaction
New paradigms
New concepts
New language
New disciplines

DRIVERS
-- Deep scientific questions
-- Pressing societal needs

I·C·S
The Institute for Cyber Security

Cyber Security Research Convergence

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing



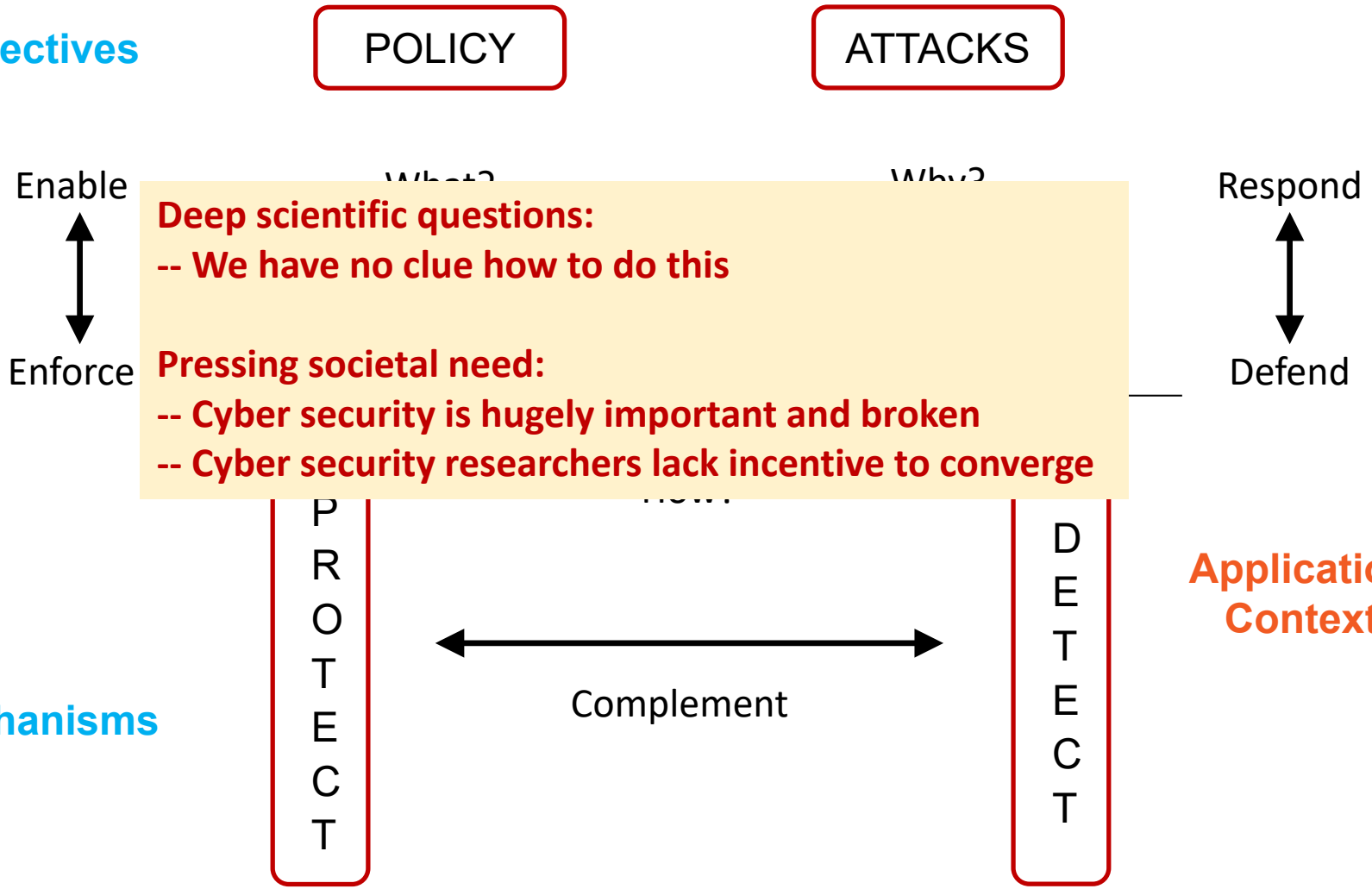
World-Leading Research with Real-World Impact!

UTSA Computer Science

I·C·S
The Institute for Cyber Security

Cyber Security Research Convergence

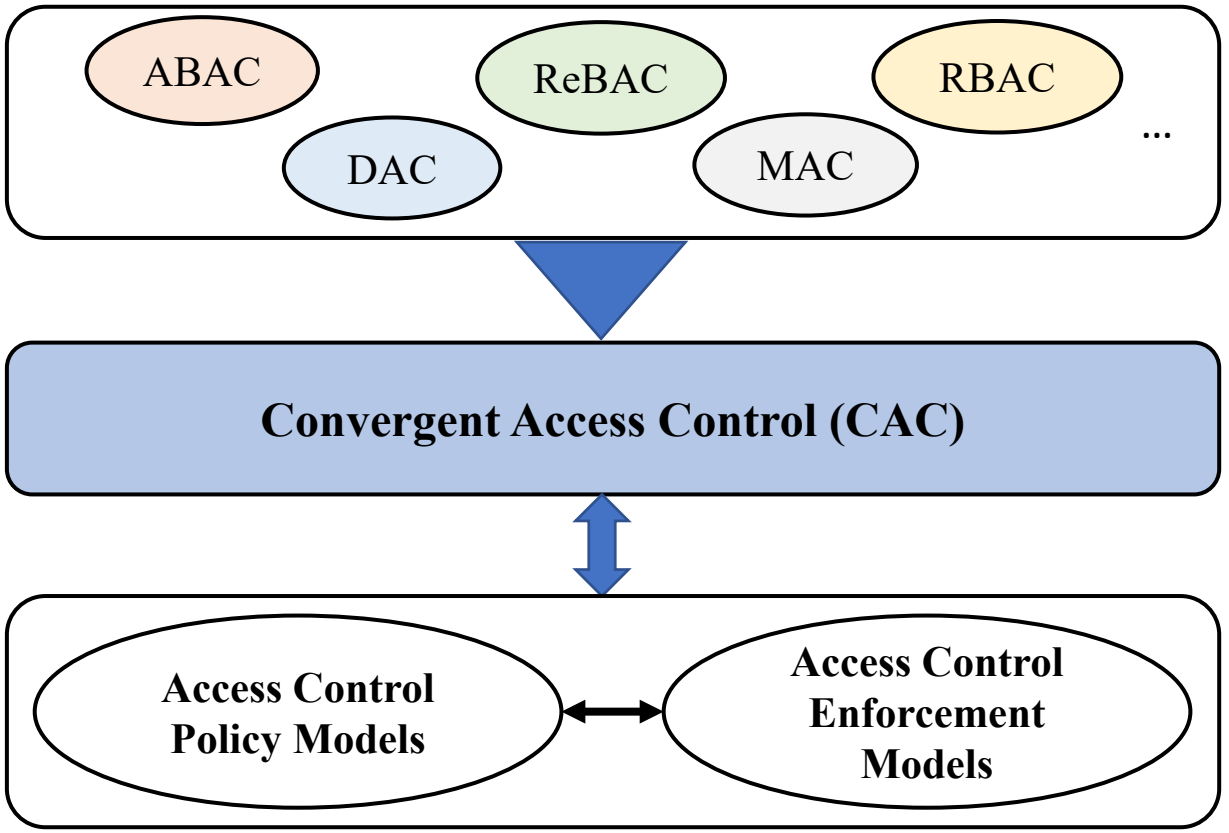
C·SPECC
Center for Security and Privacy Enhanced Cloud Computing



World-Leading Research with Real-World Impact!

UTSA Computer Science

Access Control Research Convergence



Application Context

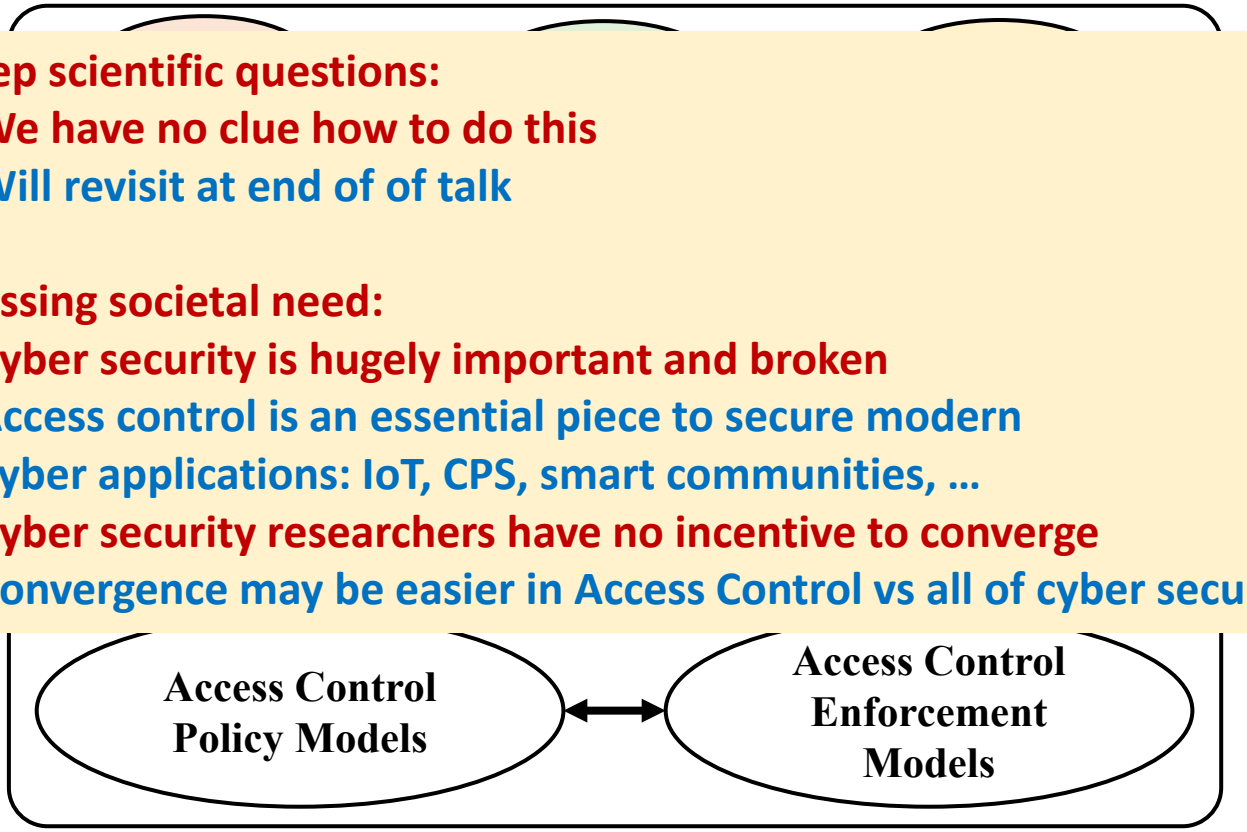
This slide prepared by Smriti Bhatt

World-Leading Research with Real-World Impact!

Access Control Research Convergence

Deep scientific questions:
-- We have no clue how to do this
-- Will revisit at end of 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

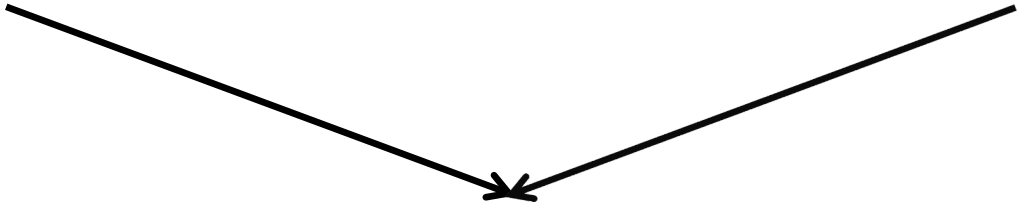


Application Context

Access Control

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)

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

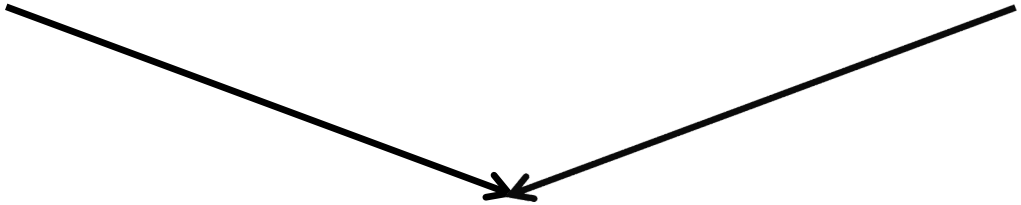
Mandatory Access Control (MAC)

- Core concept:
  - One-way information flow via security labels
  - Controls on originals and copies
- 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)
Relationship-Based Access Control (ReBAC)
Usage Control (UCON)
2020s (Hopefully)

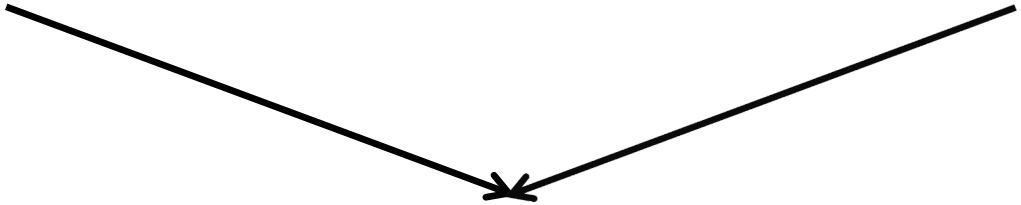
Role-Based Access Control (RBAC)

- 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

Access Control

Discretionary Access Control (DAC)
1970

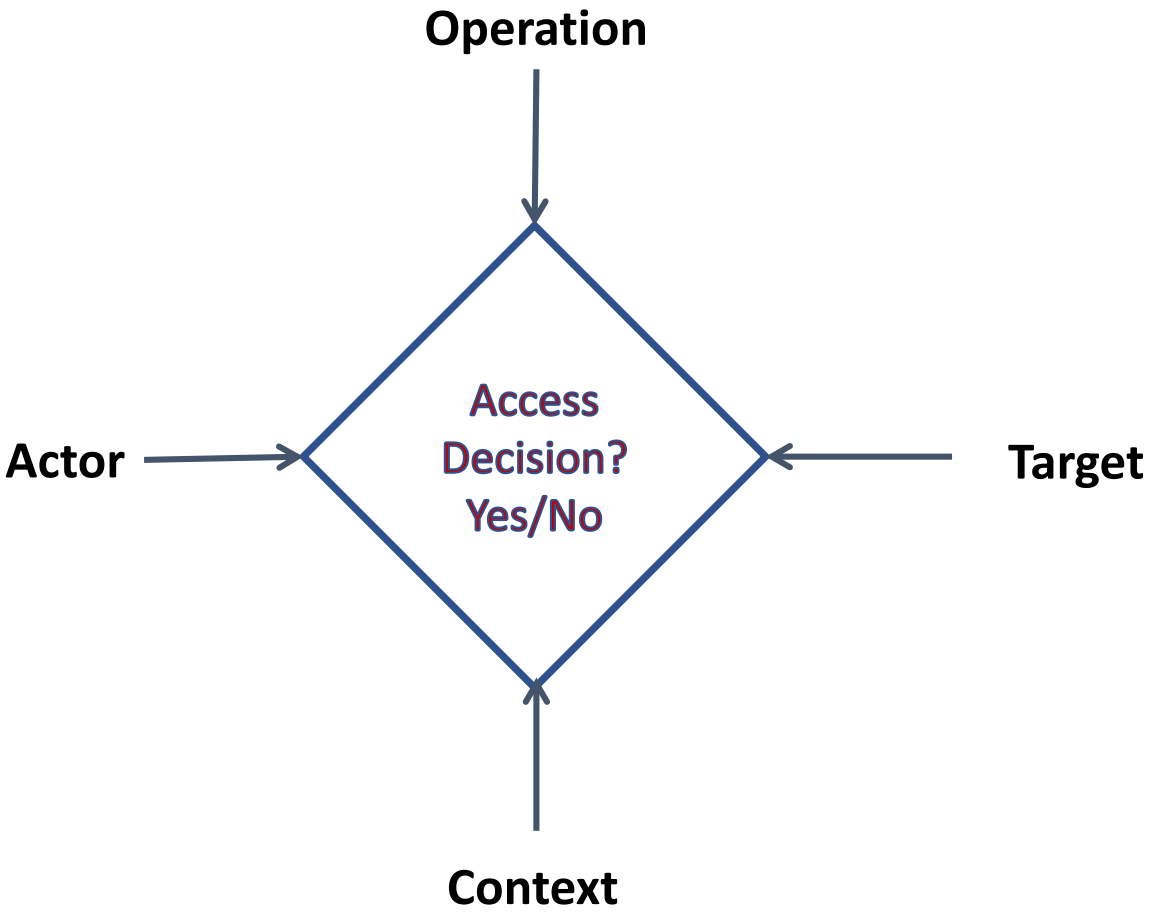
Mandatory Access Control (MAC)
1970



Role Based Access Control (RBAC)
1995

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

Attribute-Based Access Control (ABAC)



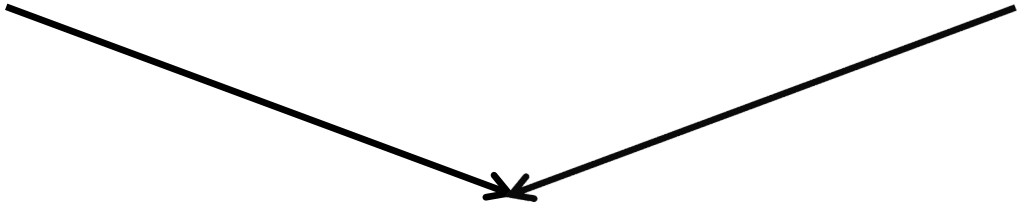
Attribute-Based Access Control (ABAC)

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

Access Control: Where Are We?

- Rich set of building blocks:

  DAC, MAC, RBAC, ABAC, ReBAC, UCON

- We have some understanding of the relationships amongst these

Access Control: What Next?

- 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

Access Control: What Next?

- 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

Access Control: What Next?

- Rich set of building blocks:

  DAC, MAC, RBAC, ABAC, ReBAC, UCON

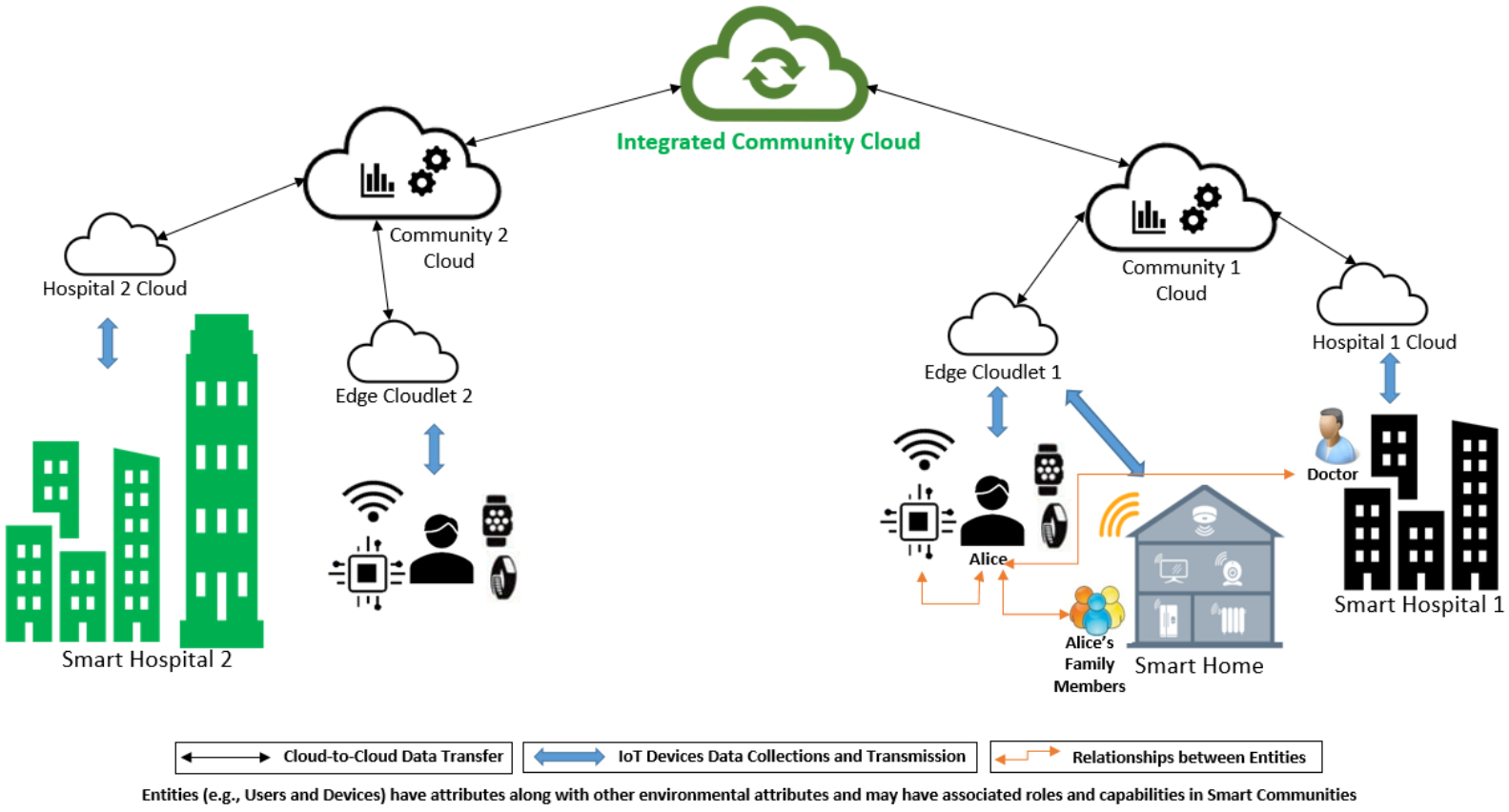
- We have some understanding of the relationships amongst these

- Do we need more building blocks?
- We have very little understanding of synergy amongst these

Pressing societal need?

Deep scientific question for convergent research

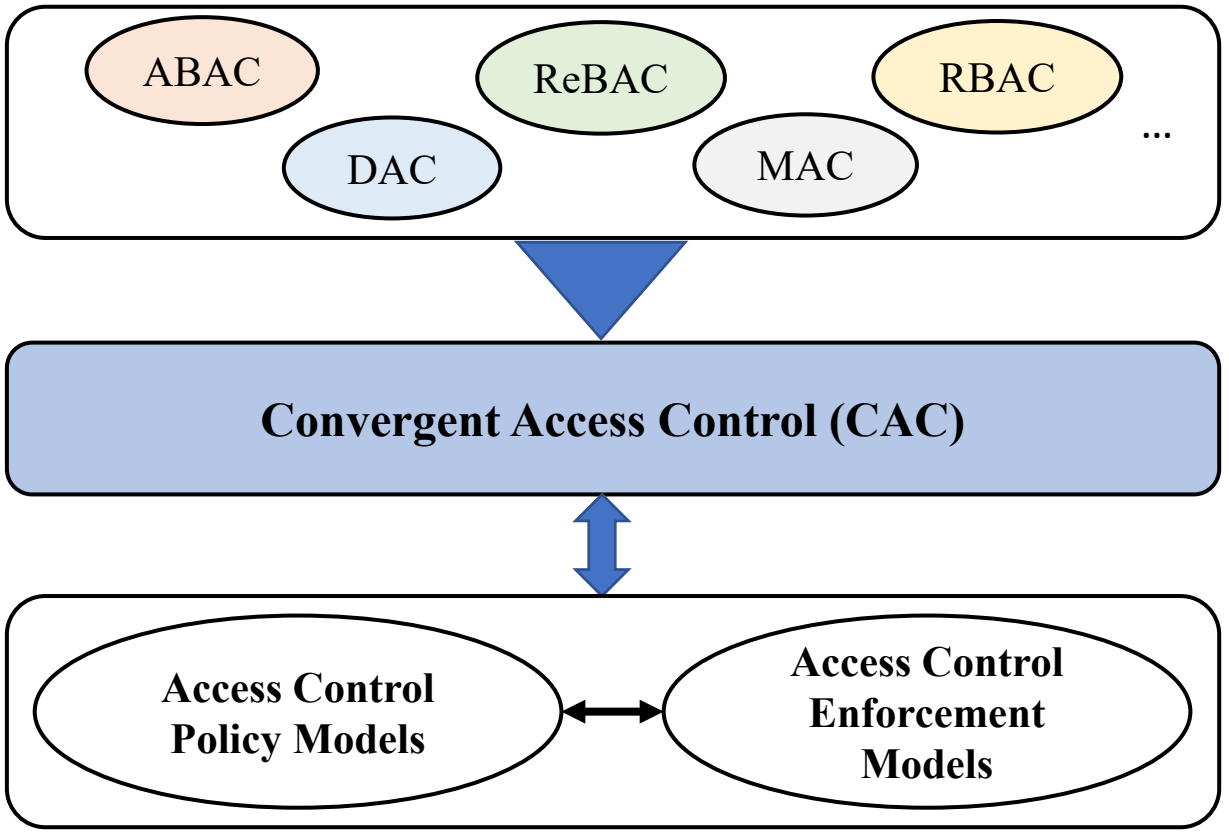
Smart Communities



This slide prepared by Smriti Bhatt

World-Leading Research with Real-World Impact!

Access Control Research Convergence



Application Context

This slide prepared by Smriti Bhatt