The Data and Application Security and Privacy (DASPY) Challenge

Prof. Ravi Sandhu
Executive Director and Endowed Chair

October 31, 2011

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

The ATM "Paradox"

- The ATM (Automatic Teller Machine) network is
  - secure enough (but insecure)
  - global in scope and rapidly growing
- But
  - not securable by academically taught cyber security
  - not studied as a success story
  - missing technologies highly regarded by academia
- Similar "paradoxes" apply to
  - on-line banking
  - e-commerce
  - etc

Cyber Security Status

- Cyber technologies and systems have evolved
- Cyber attacks and attackers have evolved
  - Side note: all attackers are not evil
- Cyber security (defensive) goals have evolved
  - Computer security
  - Information security = Computer security + Communications security
  - Information assurance
  - Mission assurance

Cyber Security Research Status

- Cyber security research (and practice) are rapidly loosing ground
  - evolving glacially
  - in spite of increase in funding and many innovative research advances
  - in spite of numerous calls for "game changing" research

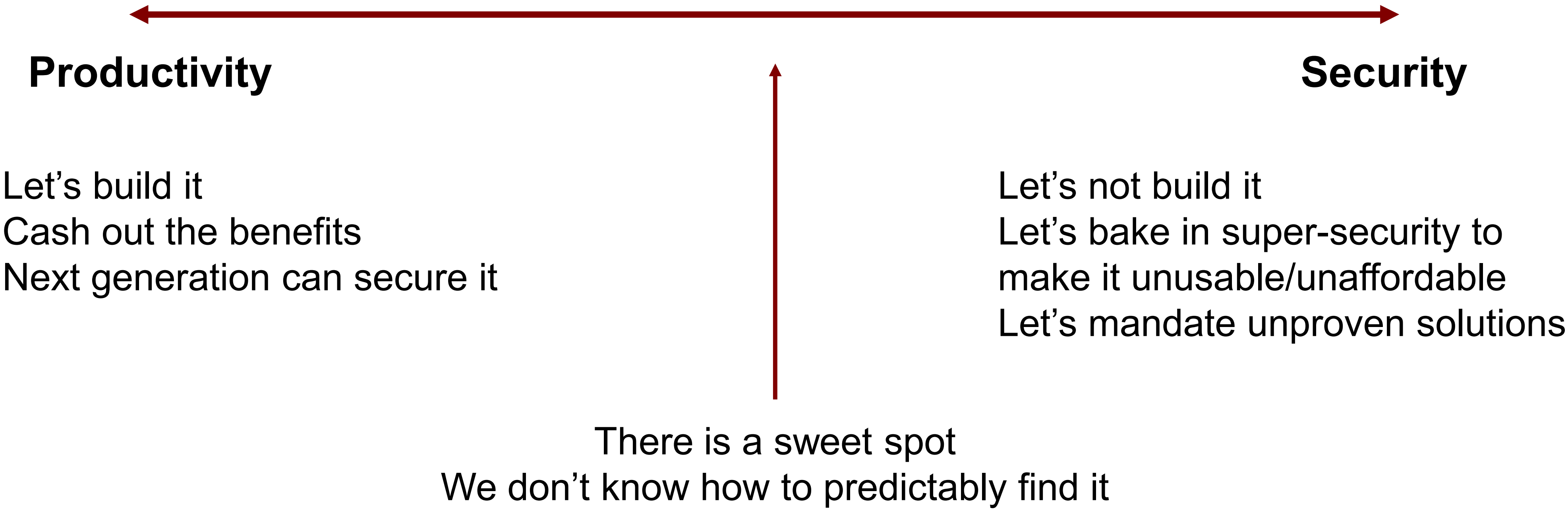
- Grand challenge: how to become relevant to the real world

Cyber Security Research Status

- We need to do something different
- Rough analogies
  - software engineering vis a vis programming
  - data models (e.g., entity-relationship) vis a vis data structures (e,g., B trees)

Cyber Security Characteristics

- Cyber Security is all about tradeoffs



Productivity

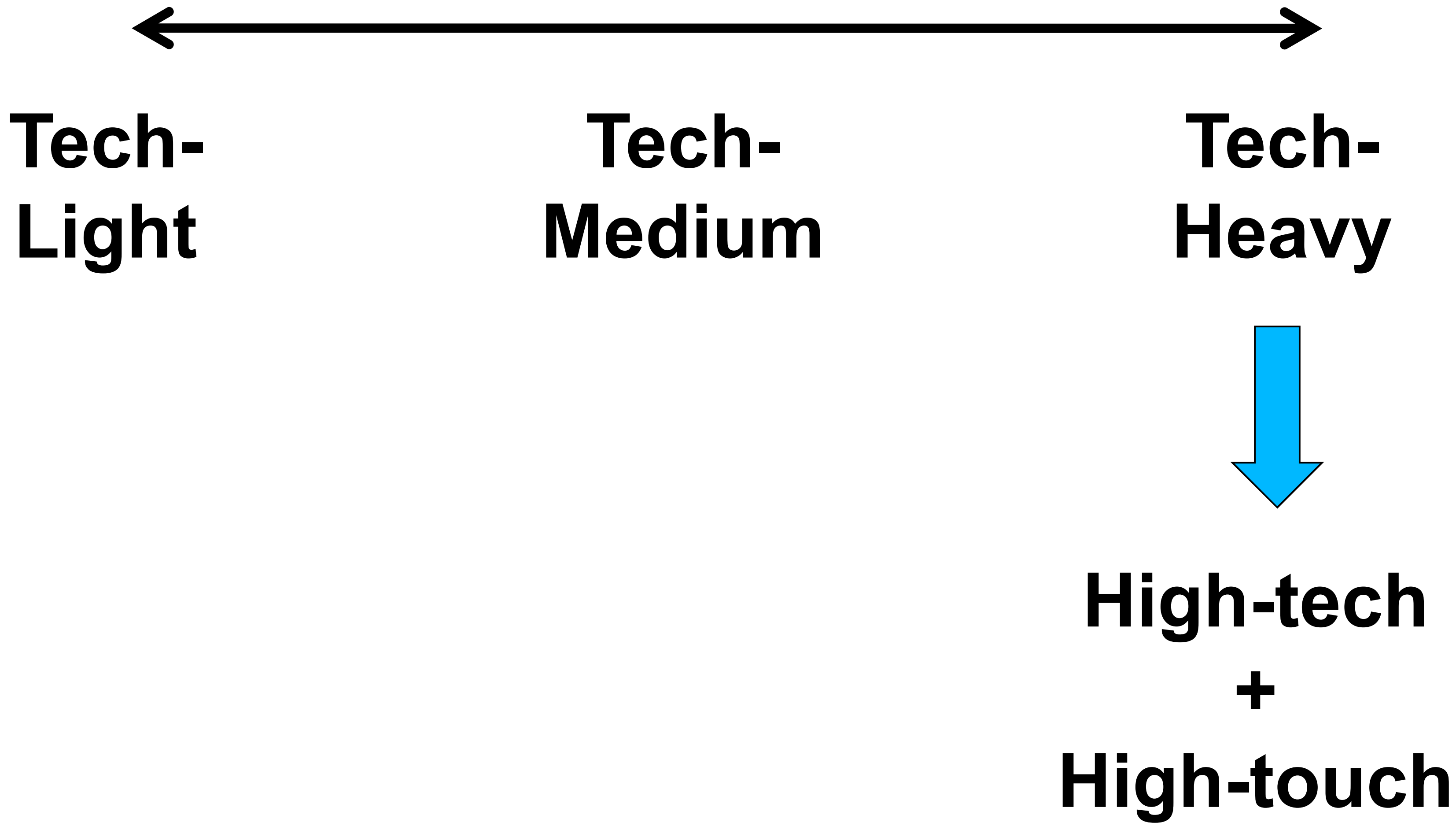
Security

Let’s build it
Cash out the benefits
Next generation can secure it

Let’s not build it
Let’s bake in super-security to make it unusable/unaffordable
Let’s mandate unproven solutions

There is a sweet spot
We don’t know how to predictably find it

Cyber Security Characteristics



Tech-Light

Tech-Medium

Tech-Heavy

High-tech

+

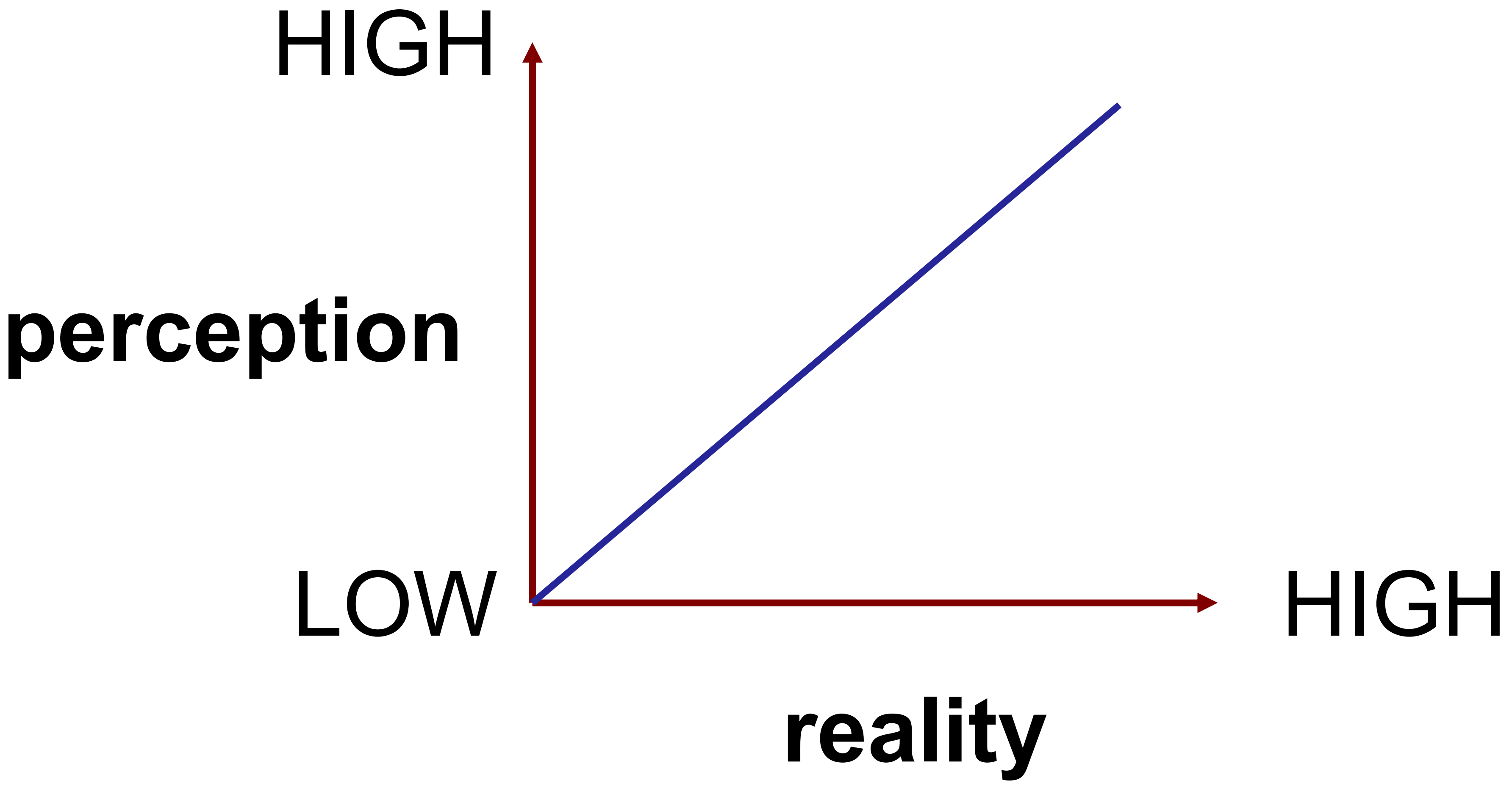
High-touch

Cyber Security Characteristics

- Microsec versus Macrosec
  - Most cyber security thinking is microsec
  - Most big (e.g., national level) cyber security threats are macrosec

- Rational microsec behavior can result in highly vulnerable macrosec

Cyber Security Characteristics



Cyber Security Characteristics

- How to justify investing in security in presence of persistent insecurity?
- And, where to invest?
  - mitigate known attacks in the wild?
  - mitigate anticipated attacks?
  - mitigate ultimate attacks?
  - some combination?

Academic Challenge

- Develop a scientific discipline
  - to cover (at least) the previous characteristics
  - that can be meaningfully taught in Universities at all levels: BS, MS, PhD

- Prognosis
  - we shall succeed (we have no choice)

Driving Principles

- Insecurity is inevitable
  - Death is inevitable

- Security investment is nevertheless justified
  - Mortals nevertheless seek medical care

- Too much security can be counter productive
  - So can too much medical care

Central Question

- How can we be “secure” while being “insecure”?

versus

- How can we be “secure”?

How Secure? How Insecure?

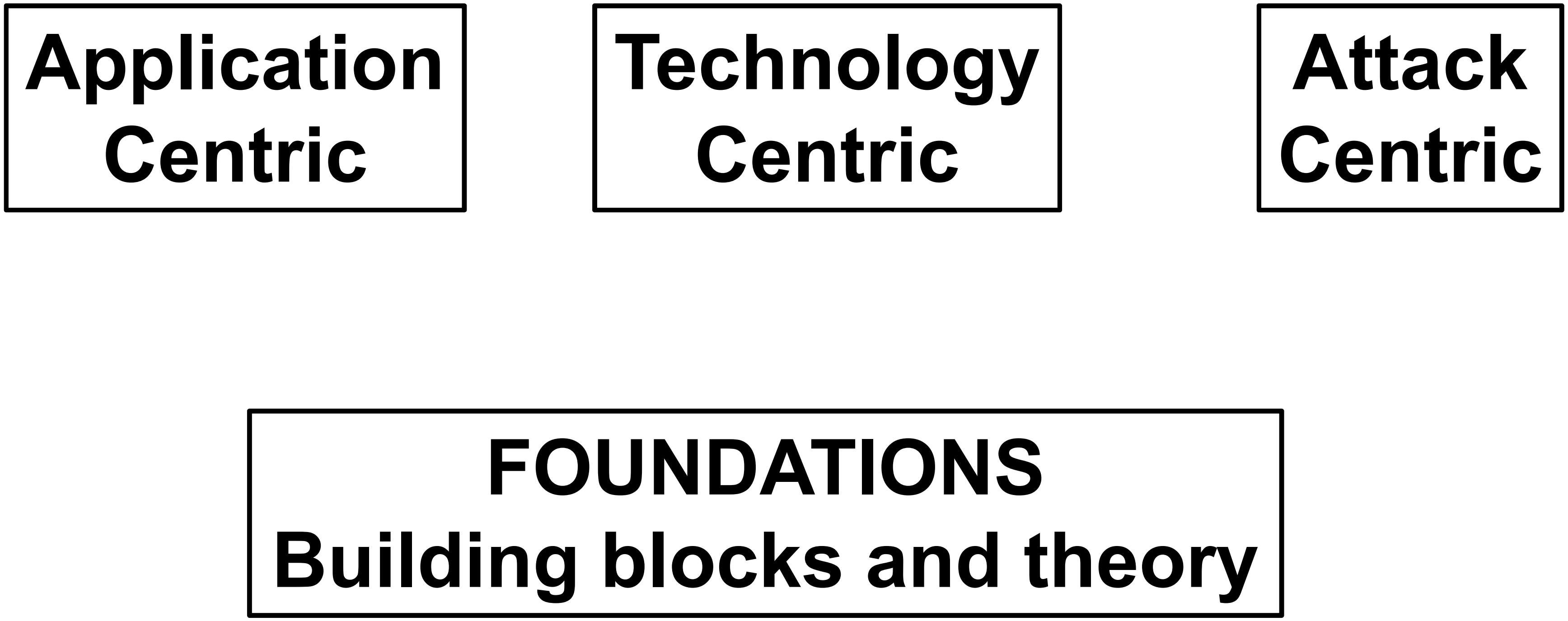
- Sometimes aiming high is very appropriate
  - The President’s nuclear football
  - Secret formula for Coca Cola

- Sometimes not
  - ATM network
  - On-line banking
  - E-commerce (B2C)

Why is the ATM System Secure?

- Monetary loss is easy to quantify and compensate
- Security principles **Application Centric**
  - stop loss mechanisms
  - audit trail (including physical video)
  - retail loss tolerance with recourse
  - wholesale loss avoidance
- Technical surprises
  - no asymmetric cryptography
  - no annonymity

Cyber Security Research



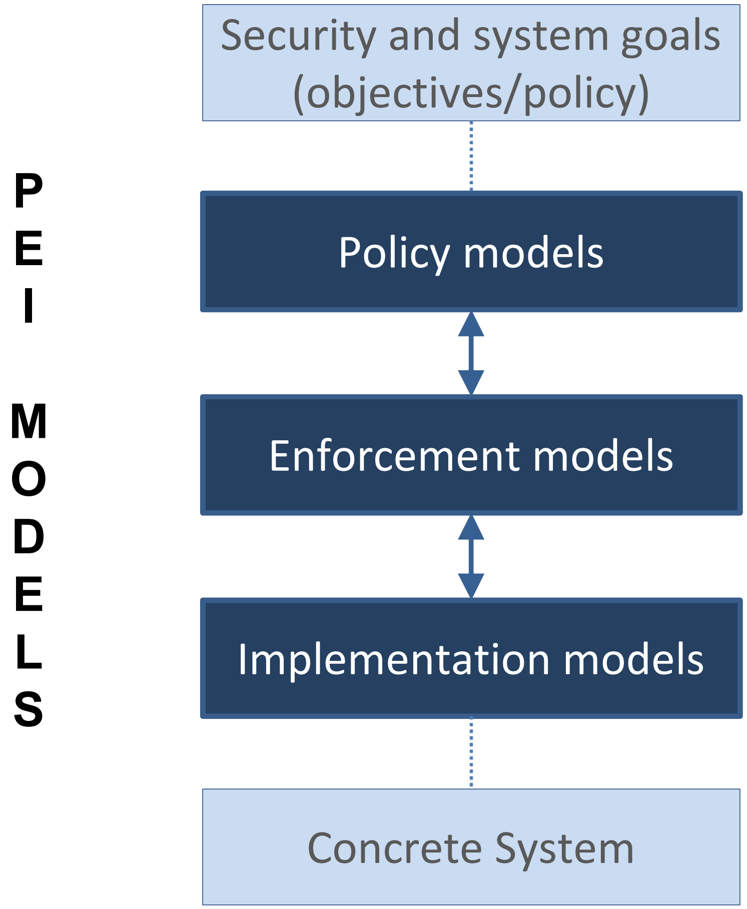
Application Centric

Technology Centric

Attack Centric

FOUNDATIONS
Building blocks and theory

The DASPY System Challenge



PEI MODELS

Security and system goals (objectives/policy)

Policy models

Enforcement models

Implementation models

Concrete System

Necessarily informal

Specified using users, subjects, objects, admins, labels, roles, groups, etc. in an ideal setting.

Security analysis (objectives, properties, etc.).

Approximated policy realized using system architecture with trusted servers, protocols, etc.

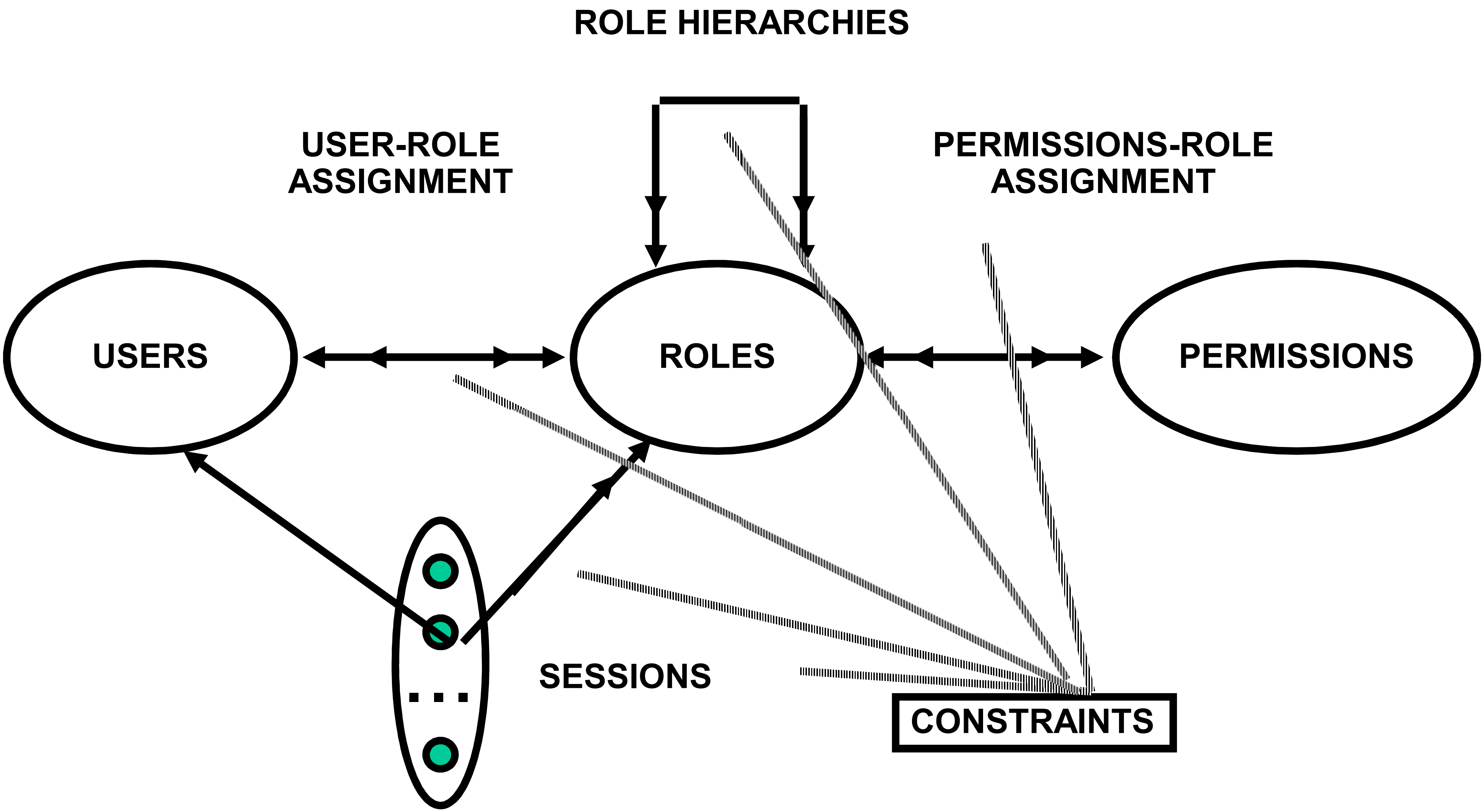
Enforcement level security analysis (e.g. stale information due to network latency, protocol proofs, etc.).

Technologies such as Cloud Computing, Trusted Computing, etc.

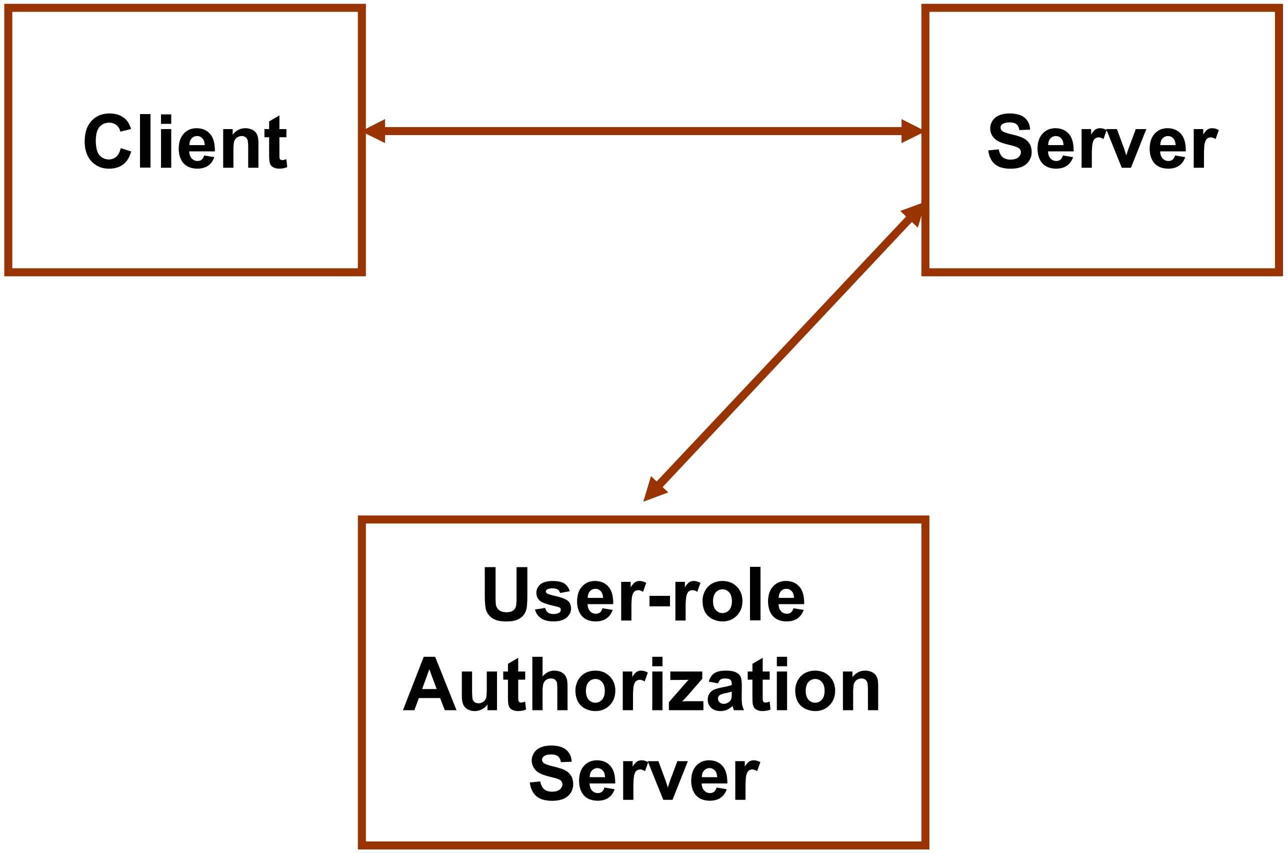
Implementation level security analysis (e.g. vulnerability analysis, penetration testing, etc.)

Software and Hardware

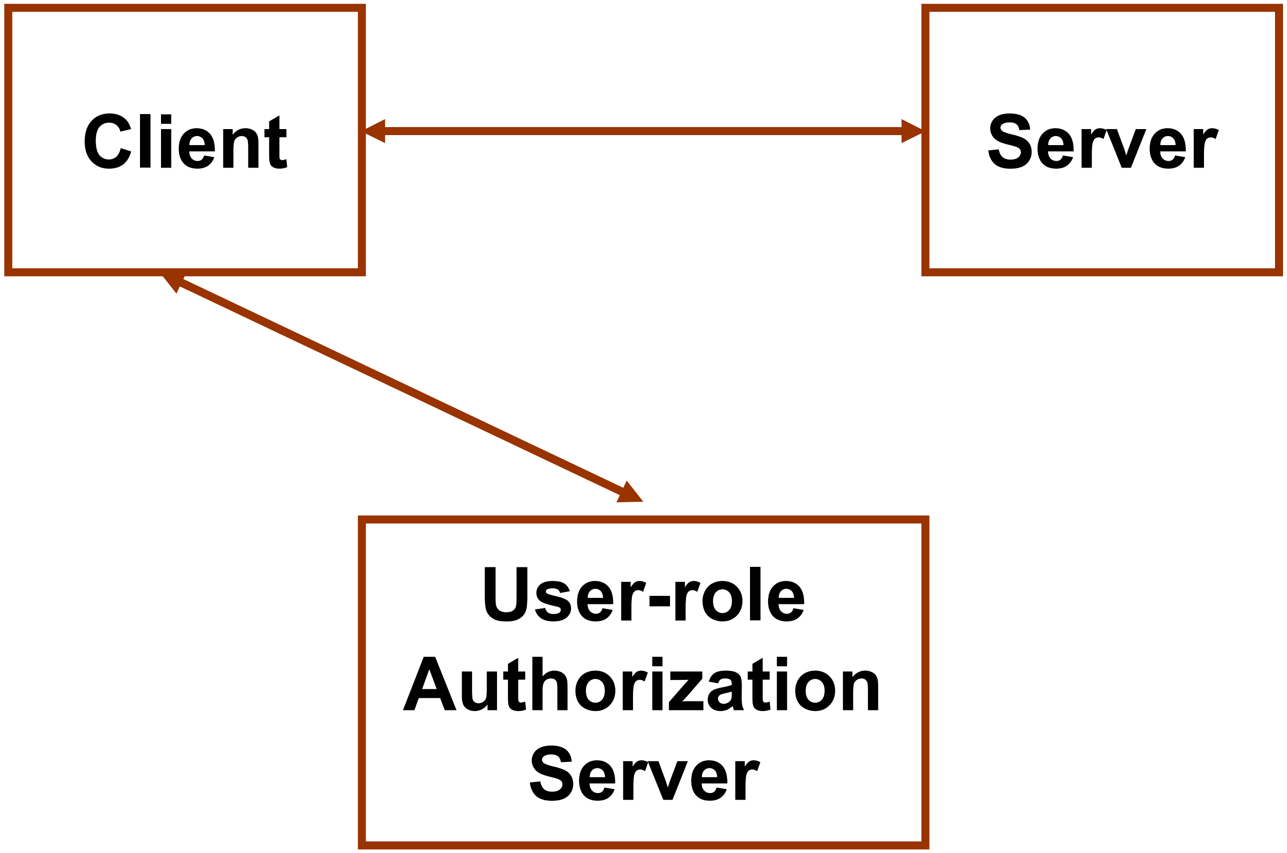
RBAC96 Model (P Layer)



Server Pull Model (E Layer)

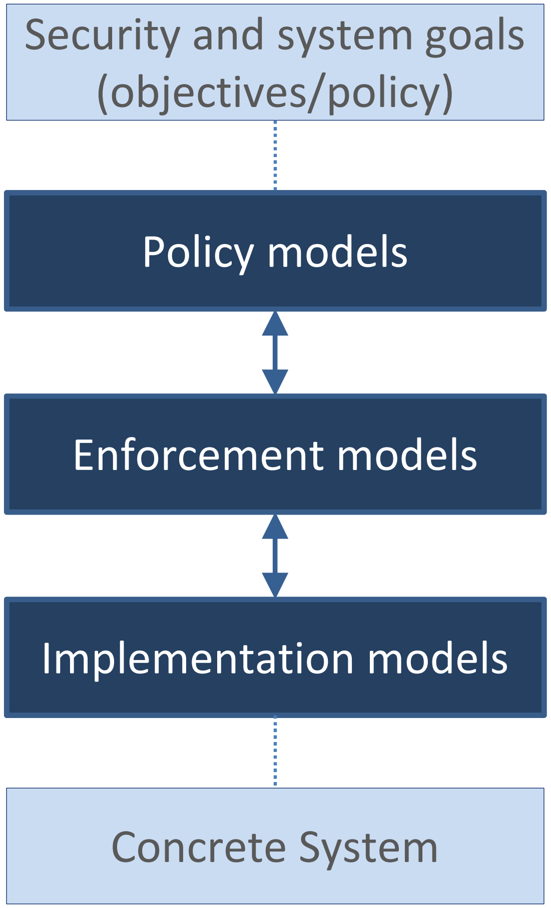


Client Pull Model (E Layer)



The DASPY System Challenge

PEI MODELS



Security and system goals (objectives/policy)

Necessarily informal

Policy models

Specified using users, subjects, objects, admins, labels, roles, groups, etc. in an ideal setting.

Security analysis (objectives, properties, etc.).

Enforcement models

Approximated policy realized using system architecture with trusted servers, protocols, etc.

Enforcement level security analysis (e.g. stale information due to network latency, protocol proofs, etc.).

Implementation models

Technologies such as Cloud Computing, Trusted Computing, etc.

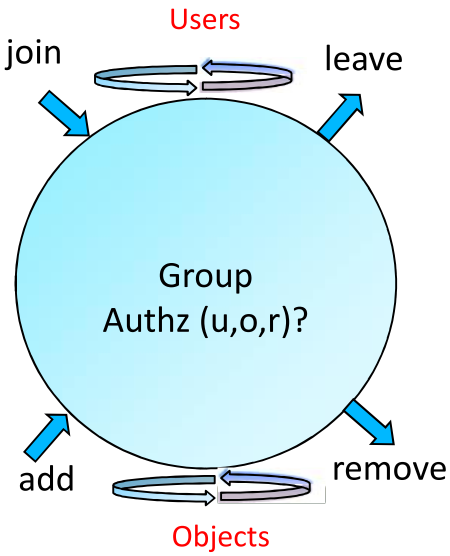
Implementation level security analysis (e.g. vulnerability analysis, penetration testing, etc.)

Concrete System

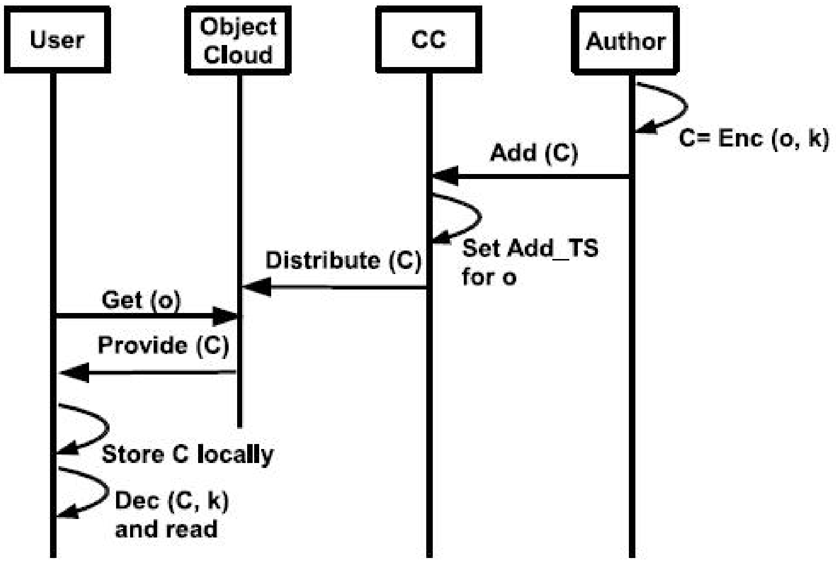
Software and Hardware

g-SIS Model (P layer)

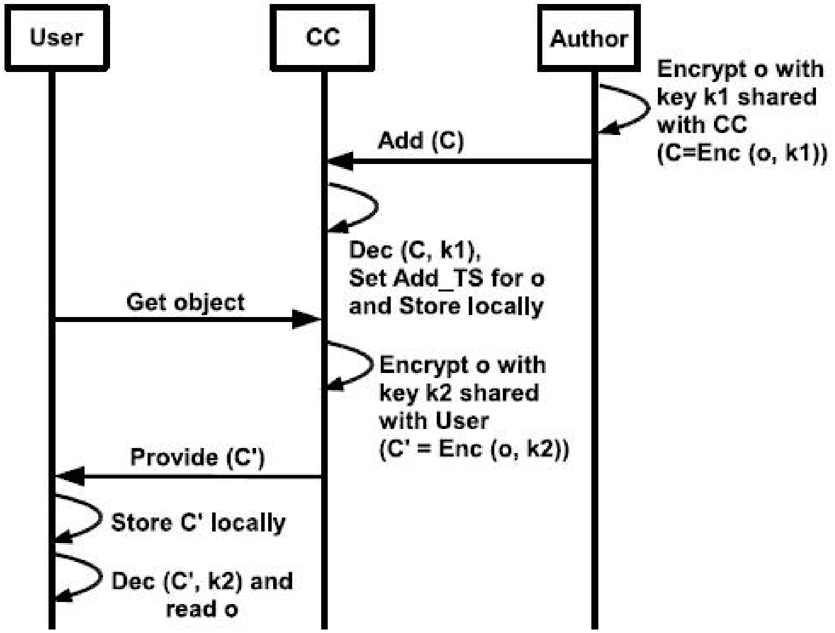
- Operational aspects
  - Group operation semantics
    - Add, Join, Leave, Remove, etc
    - Multicast group is one example
  - Object model
    - Read-only
    - Read-Write (no versioning vs versioning)
  - User-subject model
    - Read-only Vs read-write
  - Policy specification
- Administrative aspects
  - Authorization to create group, user join/leave, object add/remove, etc.



g-SIS Model (E layer)



Super-Distribution (SD)


User
CC
Author
Encrypt o with key k1 shared with CC (C=Enc (o, k1))
Add (C)
Dec (C, k1), Set Add_TS for o and Store locally
Get object
Encrypt o with key k2 shared with User (C' = Enc (o, k2))
Provide (C')
Store C' locally
Dec (C', k2) and read o

Micro-Distribution (MD)

- Scalability/Performance
  - SD: Encrypt once, access where authorized
  - MD: Custom encrypt for each user on initial access
- Assurance/Recourse
  - SD: Compromise one client, compromise group key
  - MD: Compromise of one client contained to objects on that client

Conclusion

- How can we be “secure” while being “insecure”?

  versus

- How can we be “secure”?