

Future of Access Control: Attributes, Automation, Adaptation

Prof. Ravi Sandhu

Executive Director, Institute for Cyber Security
Lutcher Brown Endowed Chair in Cyber Security
University of Texas at San Antonio

PSG College of Technology, ICC3 Conference, Keynote
December 19, 2013

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

The Science, Engineering, and Business of Cyber Security

Prof. Ravi Sandhu

Executive Director, Institute for Cyber Security
Lutcher Brown Endowed Chair in Cyber Security
University of Texas at San Antonio

PSG College of Technology, ICC3 Conference, Keynote
December 19, 2013

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



MicroSecurity

- Not too bad
- **About as good as it is going to get**
- Criminals can only defraud so many
- Big government/big business are real threats

MacroSecurity

- New arena for researchers
- Highly asymmetric, includes offense, clandestine
- Dual goals: strong offense, strong defense
- **Cyber should be controllable**
Nuclear, chemical, biological have been “controlled”





MicroSecurity

- Not too bad
- **About as good as it is going to get**
- Criminals can only defraud so many
- Big government/big business are real threats

MacroSecurity

- New arena for researchers
- Highly asymmetric, includes offense, clandestine
- Dual goals: strong offense, strong defense
- **Cyber should be controllable**
Nuclear, chemical, biological have been “controlled”

Run as fast as you can to stay in place

- ≈ 2010 US Department of Defense epiphanies
 - ❖ A new domain akin to land, sea, air and space
 - ❖ Have and use offensive cyber weapons
 - ❖ Malware penetrations in highly classified networks
- Consumerization of cyberspace
 - ❖ Anytime, Anywhere, Anything
 - ❖ BYOD: Bring your own device
 - ❖ BYOC: Bring your own cyberspace?
- Entanglement of cyber-physical-social space
 - ❖ Just starting

- Enable system designers and operators to say:

This system is secure

Not attainable

- There is an infinite supply of low-hanging attacks

- Enable system designers and operators to say:

This system is secure

Not attainable

- There is an infinite supply of low-hanging attacks

- **Alternate goal:**

**This system is as secure as possible
More secure is always better**

Not appropriate

- Enable system designers and operators to say:

Many successful examples

This system is secure “enough”

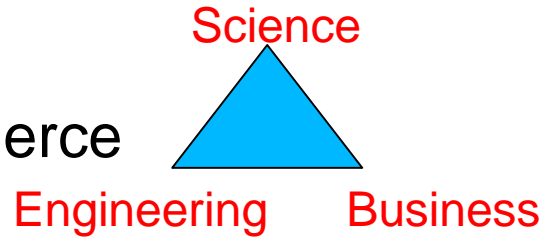
- Mass scale, rather low assurance
 - ❖ ATM network, On-line banking, E-commerce
- One of a kind, extremely high assurance
 - ❖ US President’s nuclear football

- Enable system designers and operators to say:

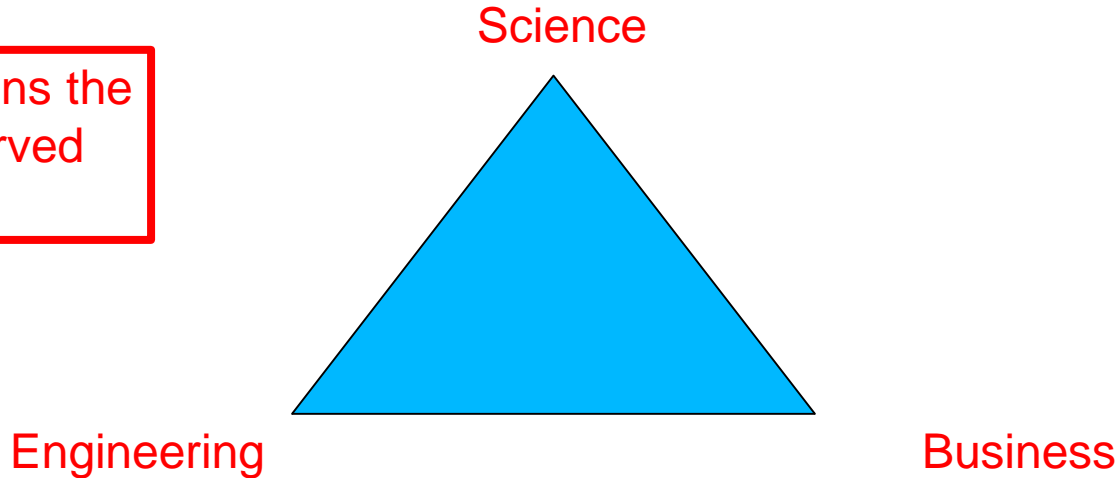
Many successful examples

This system is secure “enough”

- Mass scale, rather low assurance
 - ❖ ATM network, On-line banking, E-commerce
- One of a kind, extremely high assurance
 - ❖ US President’s nuclear football



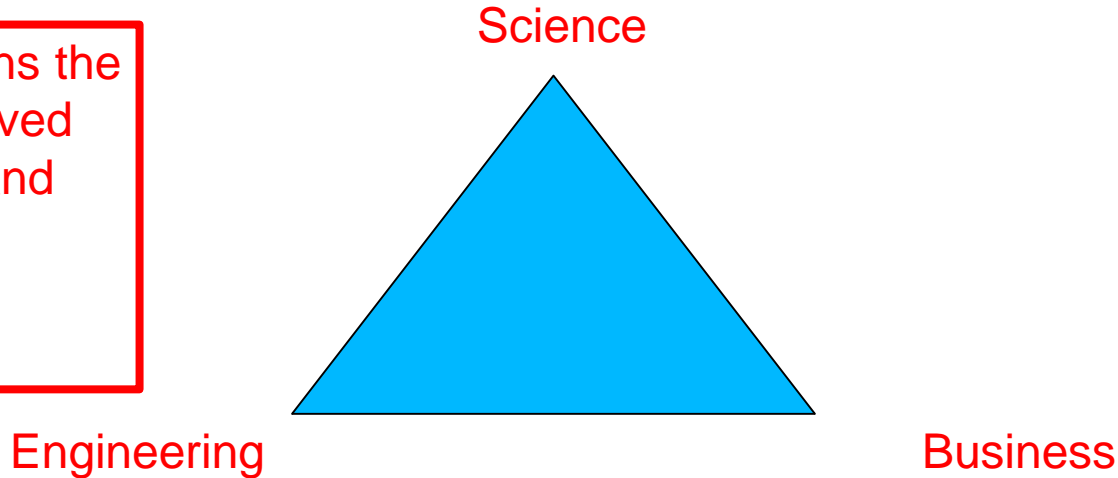
Science explains the cause of observed phenomenon



Distinguishing Characteristics of Cyber/Cyber Security

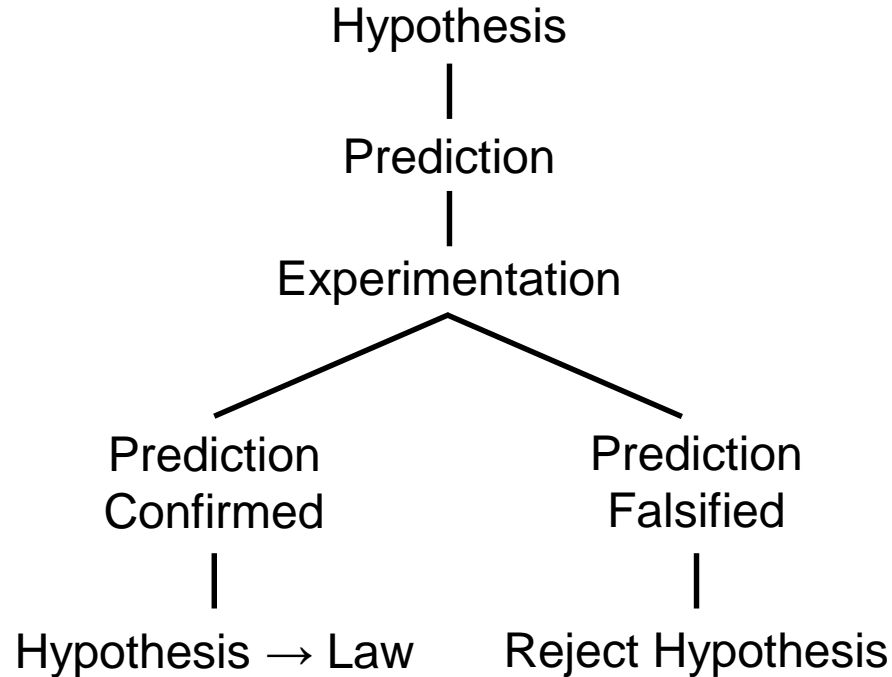
- Cyberspace is an entirely man-made domain
- Evolves rapidly and unpredictably
- Validation primarily with respect to future systems

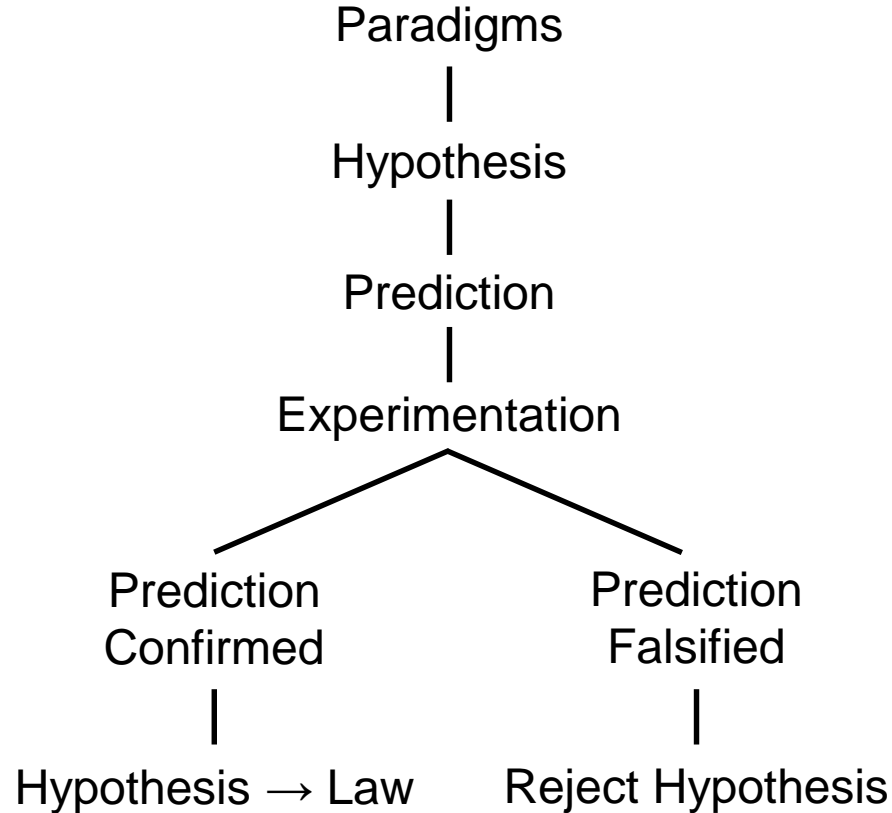
Science explains the cause of observed phenomenon and enables better construction of future systems

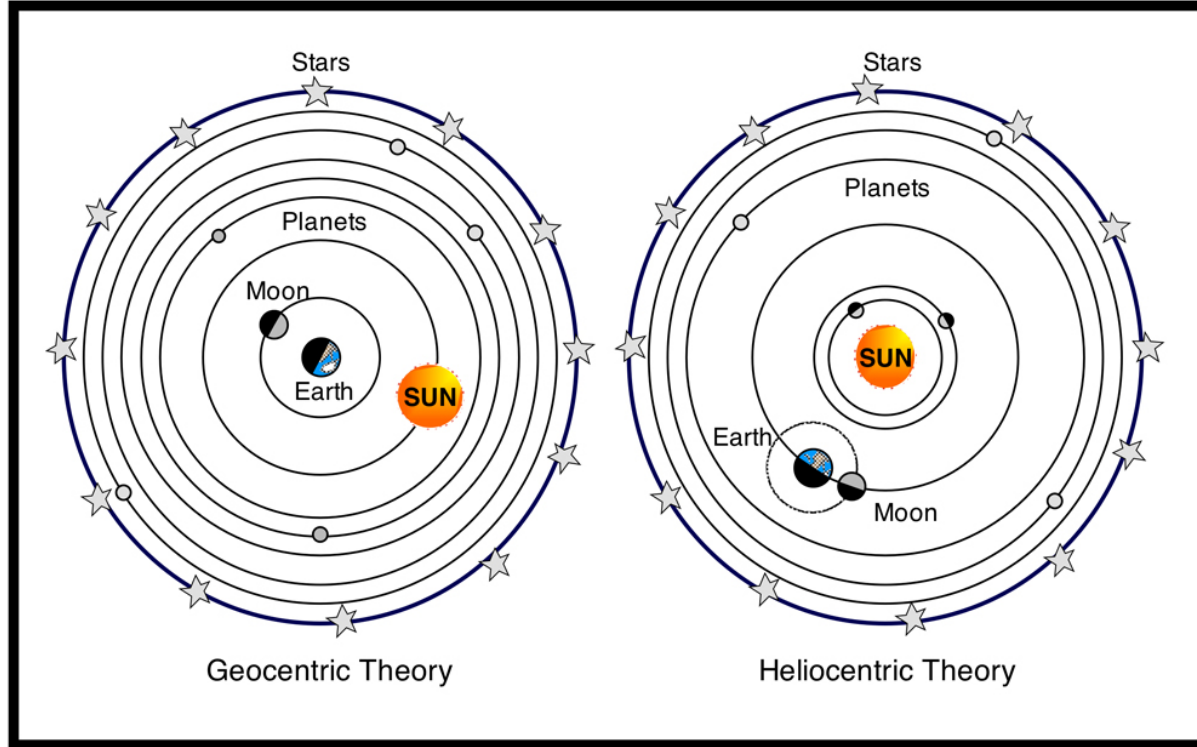


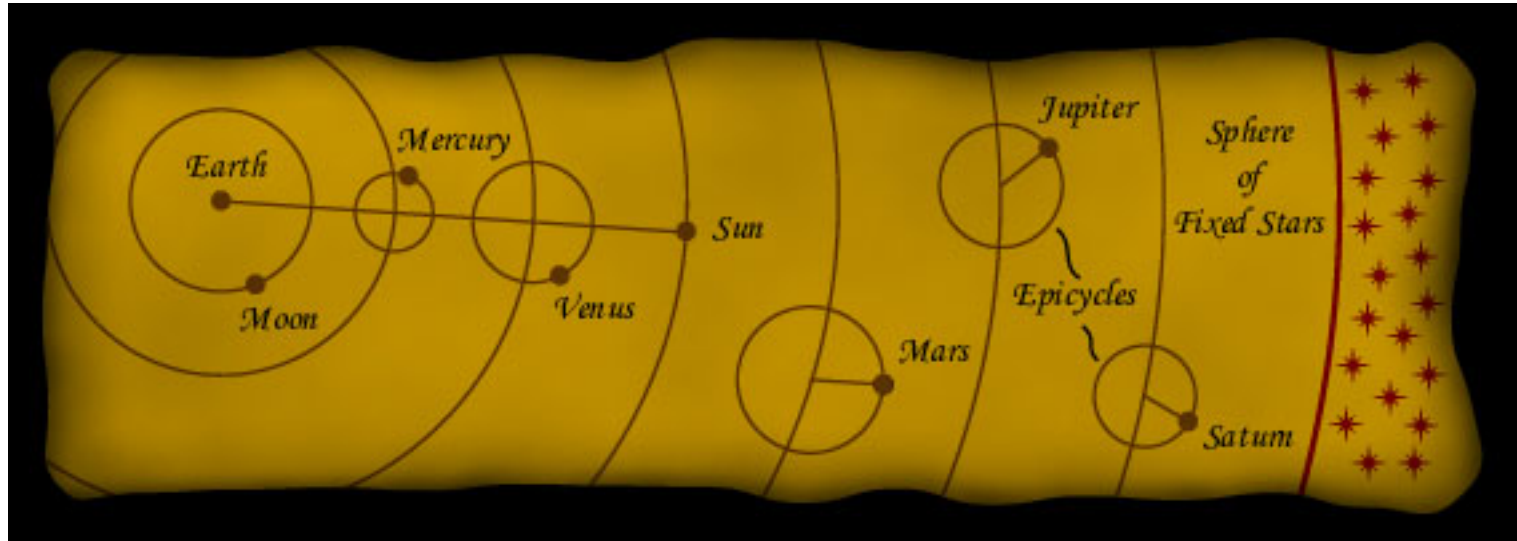
Distinguishing Characteristics of Cyber/Cyber Security

- Cyberspace is an entirely man-made domain
- Evolves rapidly and unpredictably
- Validation primarily with respect to future systems

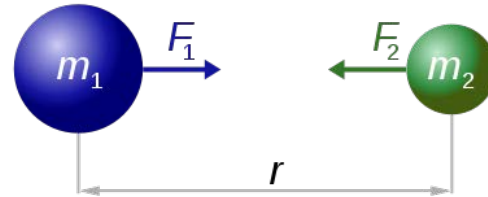
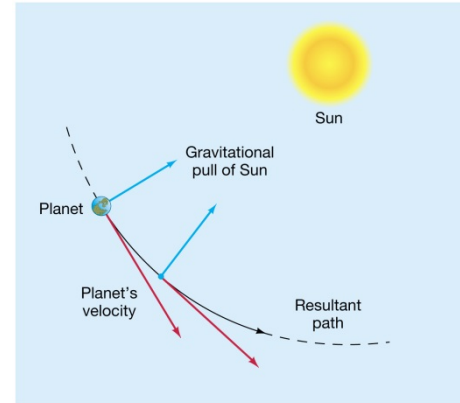
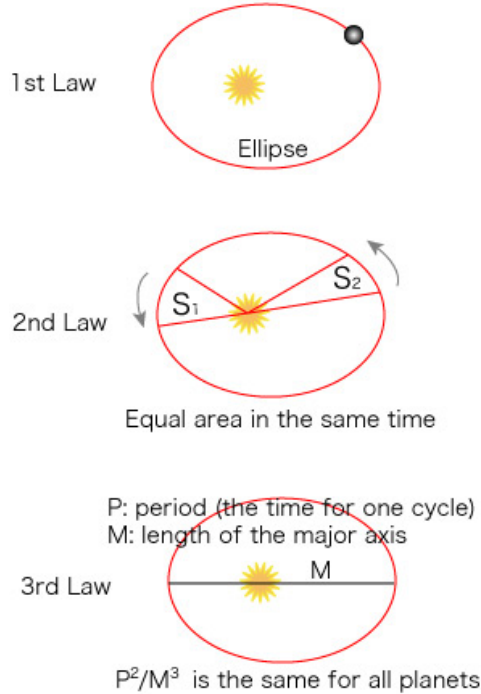






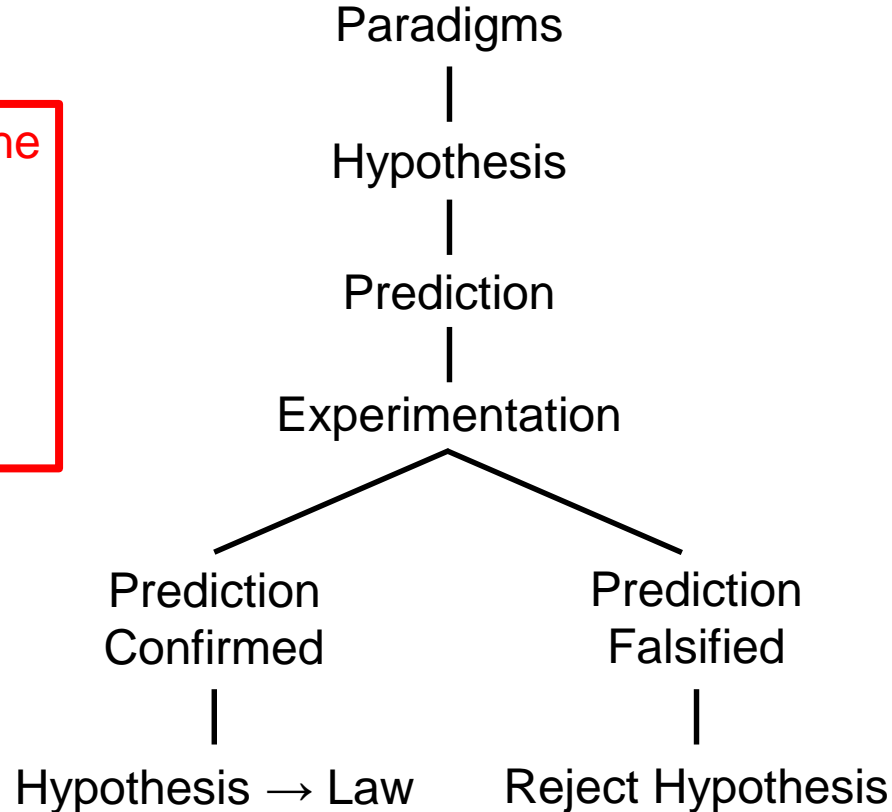


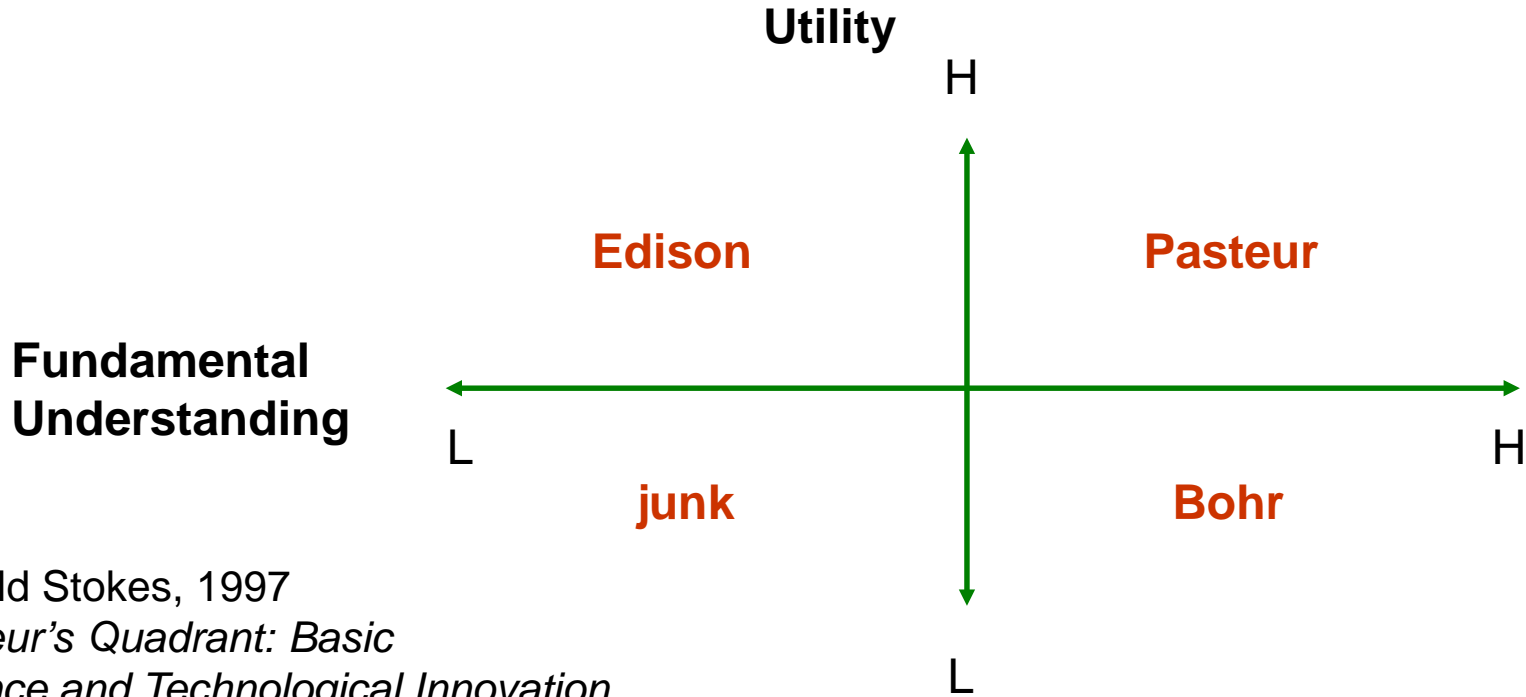
KEPLER'S LAWS



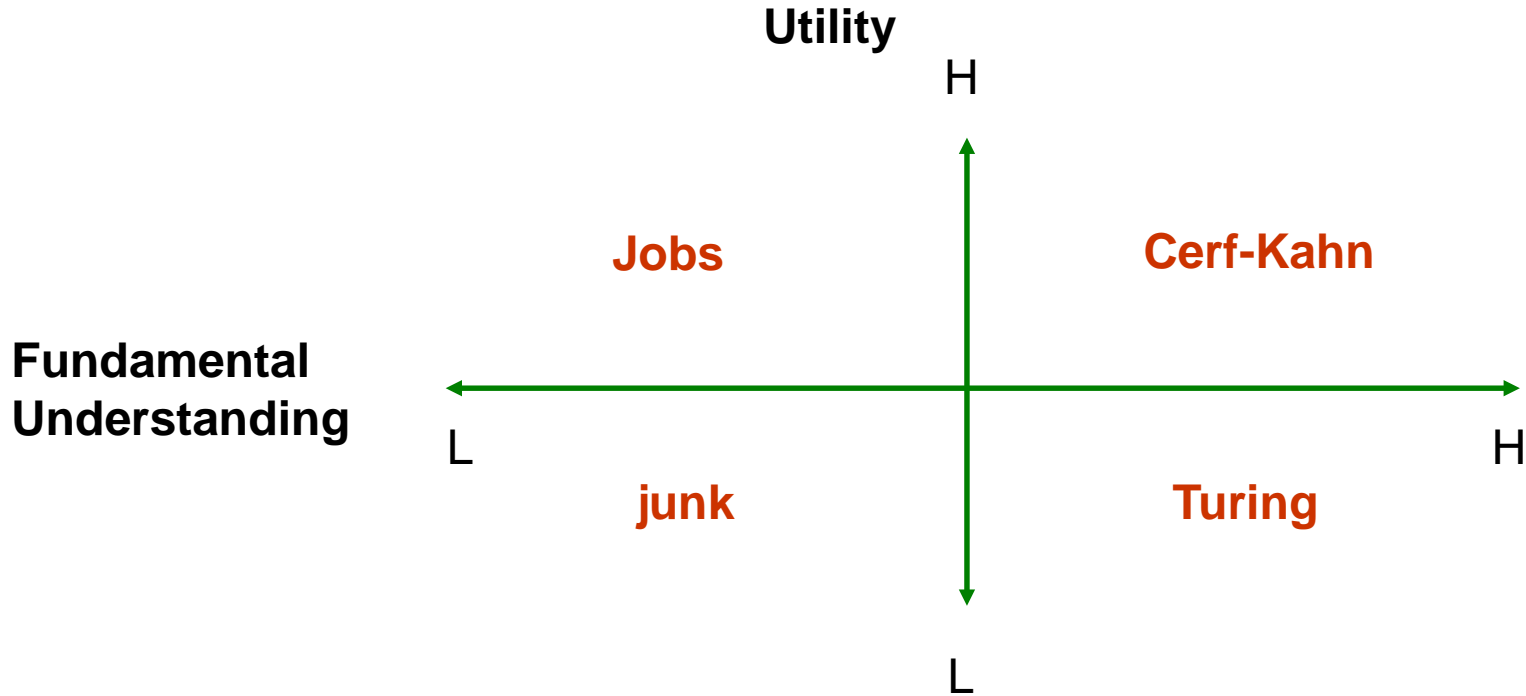
$$F_1 = F_2 = G \frac{m_1 \times m_2}{r^2}$$

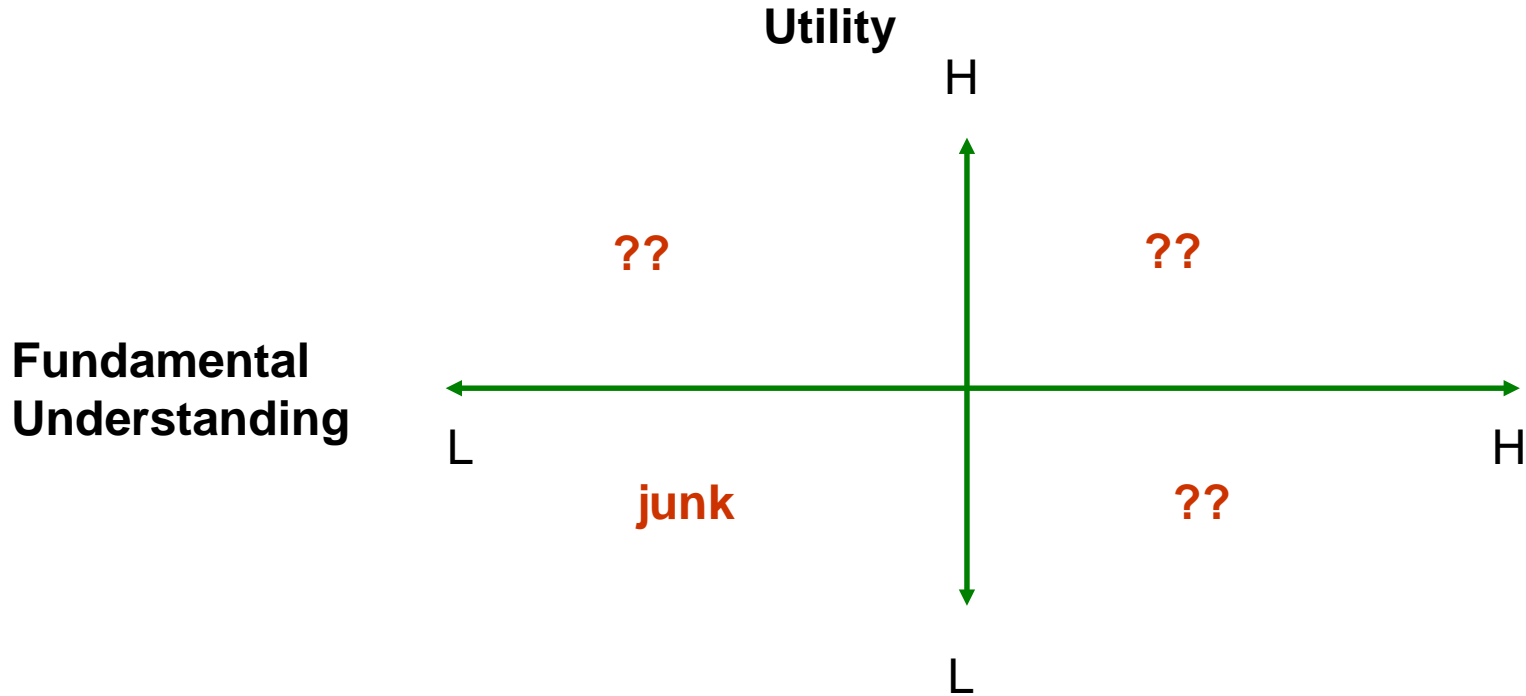
Science explains the cause of observed phenomenon and enables better construction of future systems

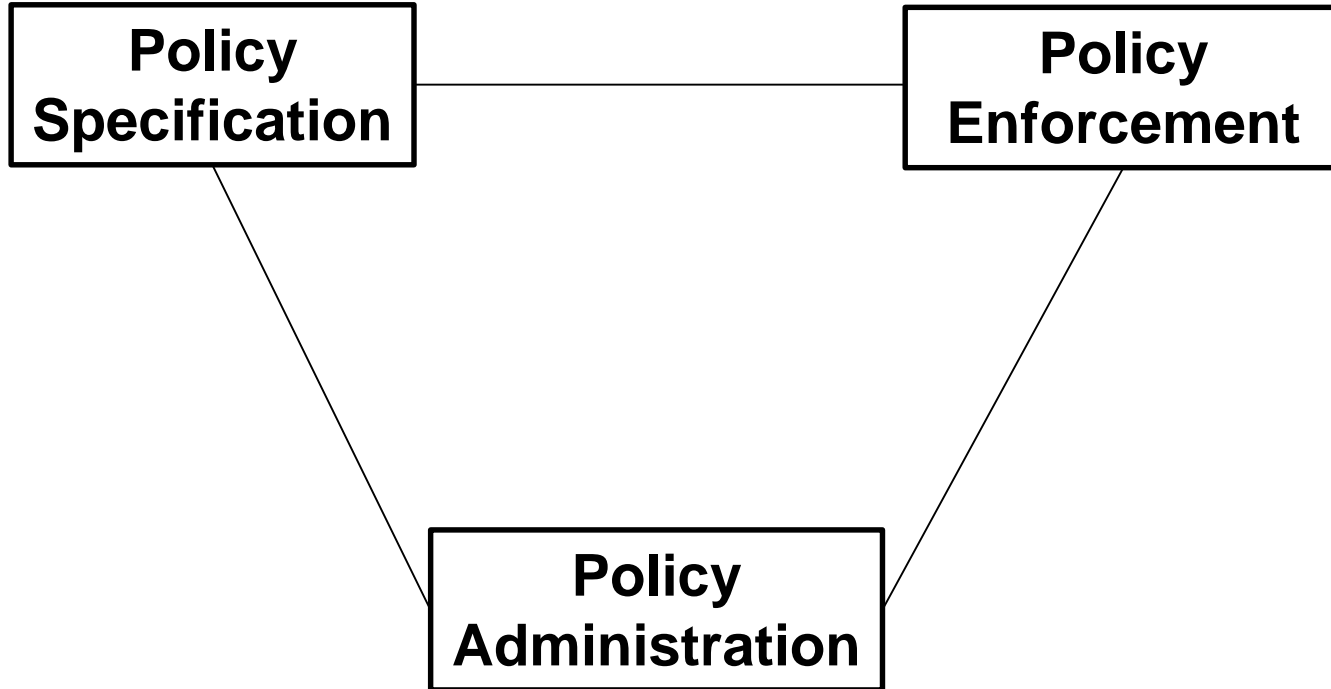


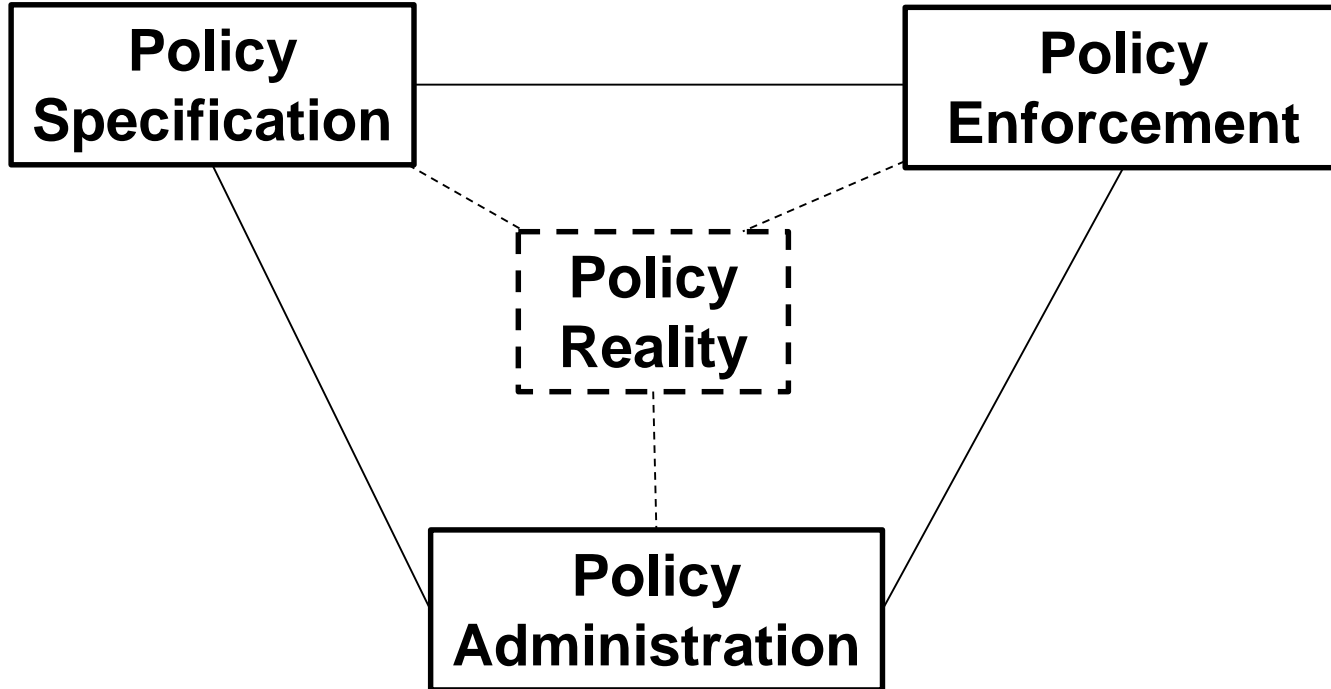


Donald Stokes, 1997
*Pasteur's Quadrant: Basic
Science and Technological Innovation*









**Discretionary Access
Control (DAC), 1970**

**Mandatory Access Control
(MAC), 1970**

```
graph TD; DAC[Discretionary Access Control (DAC), 1970] --> RBAC[Role Based Access Control (RBAC), 1995]; MAC[Mandatory Access Control (MAC), 1970] --> RBAC; RBAC --> ABAC[Attribute Based Access Control (ABAC), ????]
```

**Role Based Access
Control (RBAC), 1995**

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

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

RBAC can be configured to do MAC or DAC

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

**Fixed
Policy**

**Discretionary Access
Control (DAC), 1970**

**Mandatory Access Control
(MAC), 1970**

**Role Based Access
Control (RBAC), 1995**

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

**Flexible
Policy**

**Human
Driven**

**Discretionary Access
Control (DAC), 1970**

**Mandatory Access Control
(MAC), 1970**

**Role Based Access
Control (RBAC), 1995**

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

**Automated
Adaptive**

**Discretionary Access
Control (DAC), 1970**

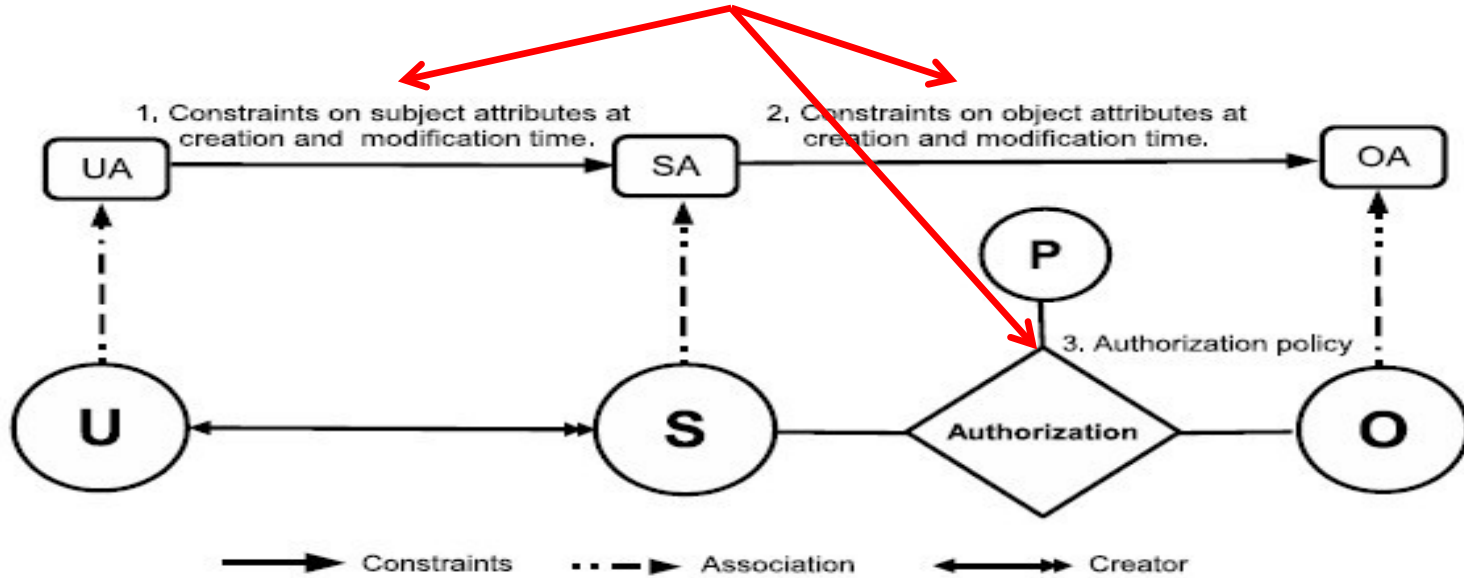
**Mandatory Access Control
(MAC), 1970**

**Role Based Access
Control (RBAC), 1995**

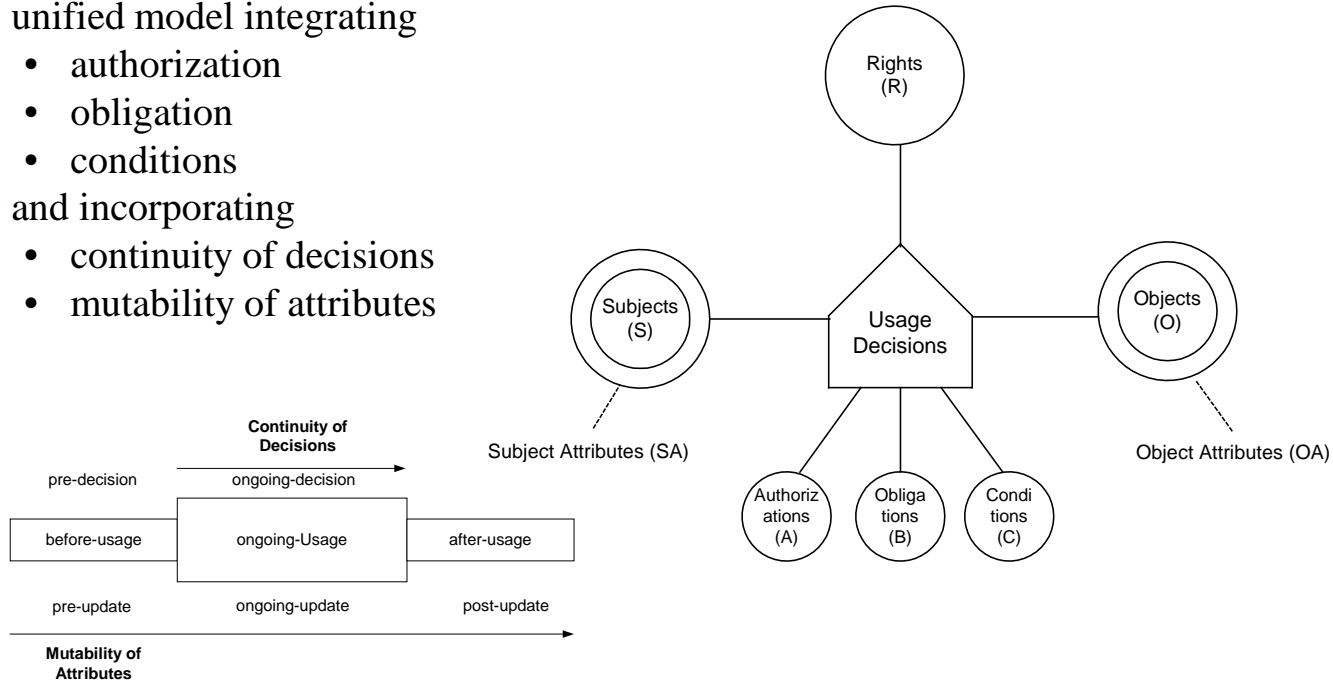
Messy or
Chaotic?

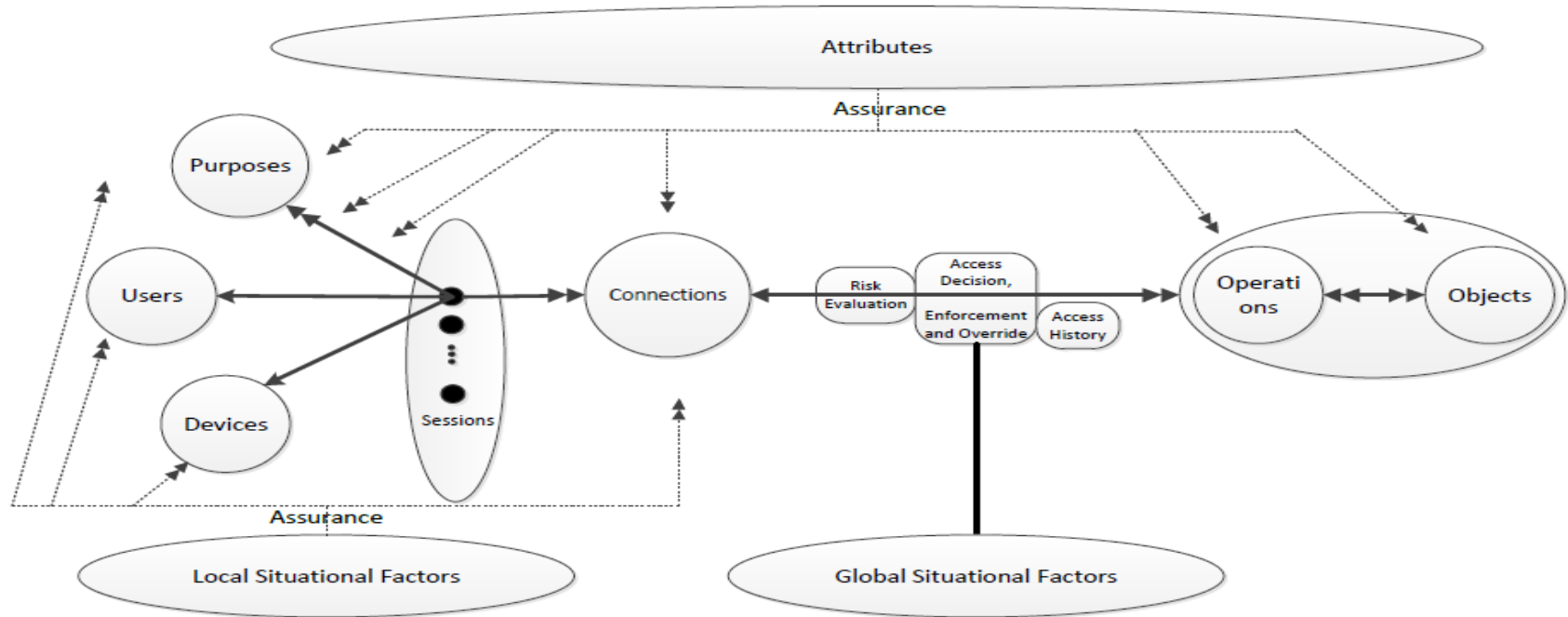
**Attribute Based Access
Control (ABAC), ????**

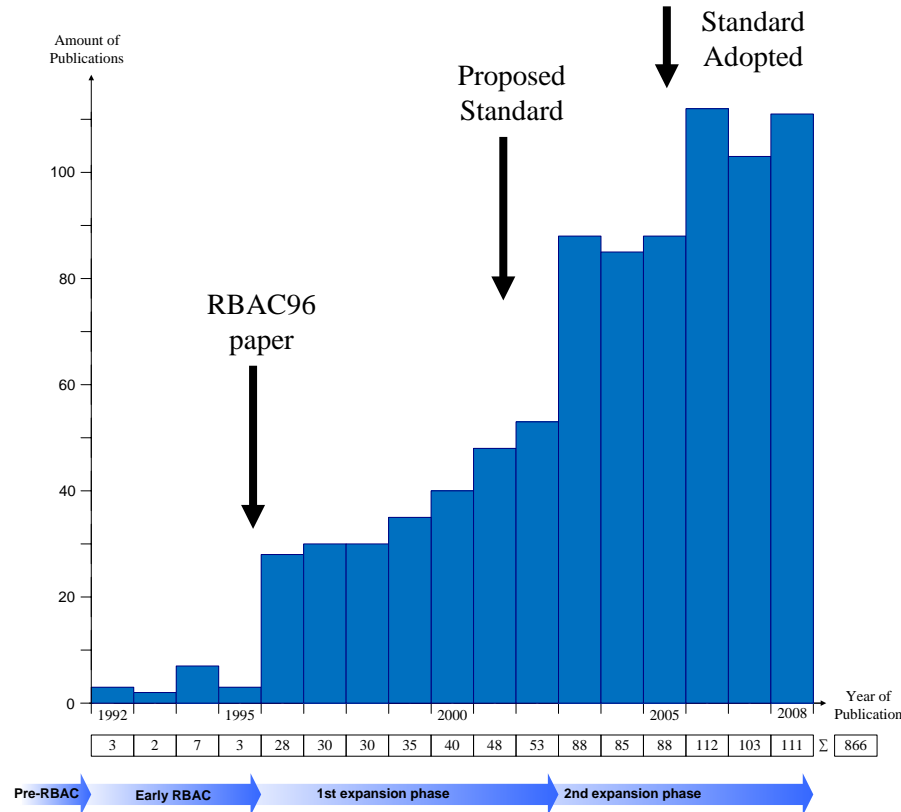
Policy Configuration Points



- unified model integrating
 - authorization
 - obligation
 - conditions
- and incorporating
 - continuity of decisions
 - mutability of attributes



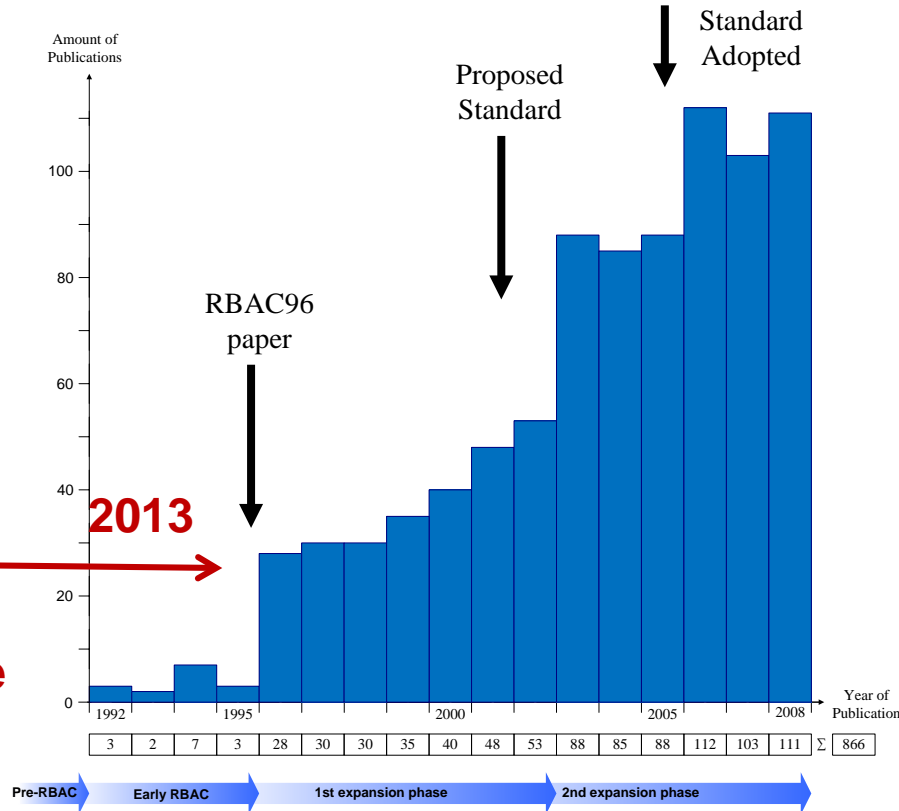




199x?

2013

ABAC still in pre/early phase



- Cyber technologies and systems trends will drive pervasive adoption of ABAC
- ABAC deployment is going to be messy but need not be chaotic
- Researchers can facilitate ABAC adoption and reduce chaos by developing
 - ❖ Models
 - ❖ Theories
 - ❖ Systems