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

ACM CCS Keynote
November 6, 2013

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

Cyber Security Status

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”

21st Century Cyberspace

- ≈ 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

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure

  Not attainable

- There is an infinite supply of low-hanging attacks

Cyber Security Goal

- 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

Cyber Security Goal

- 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

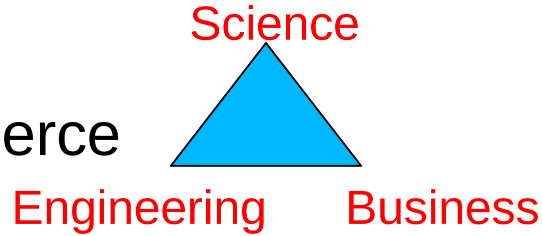
Cyber Security Goal

- Enable system designers and operators to say:

Many successful examples

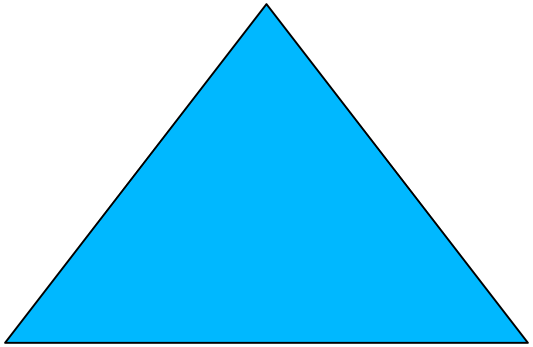
This system is secure "enough"

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



Cyber Security Ecosystem

Science explains the cause of observed phenomenon

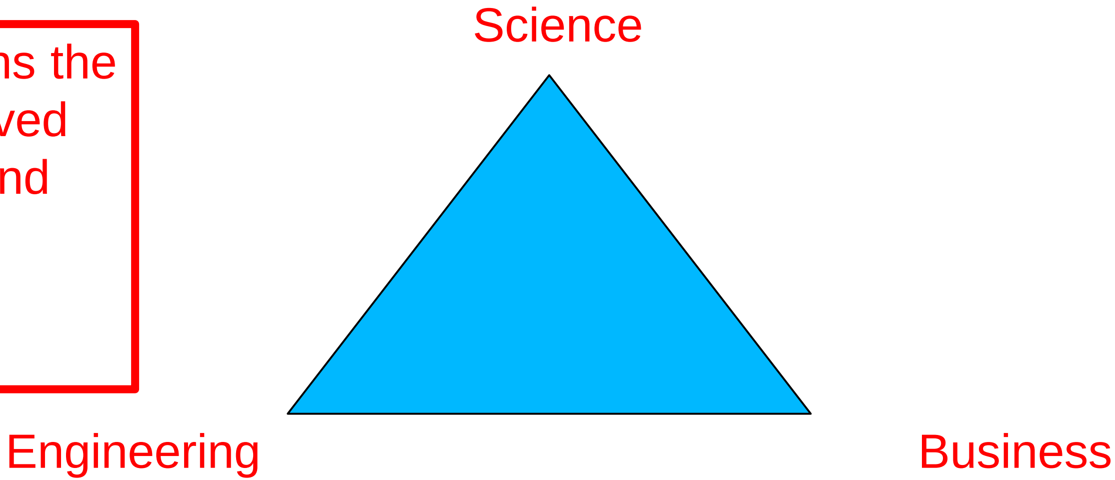


Distinguishing Characteristics of Cyber/Cyber Security

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

Cyber Security Ecosystem

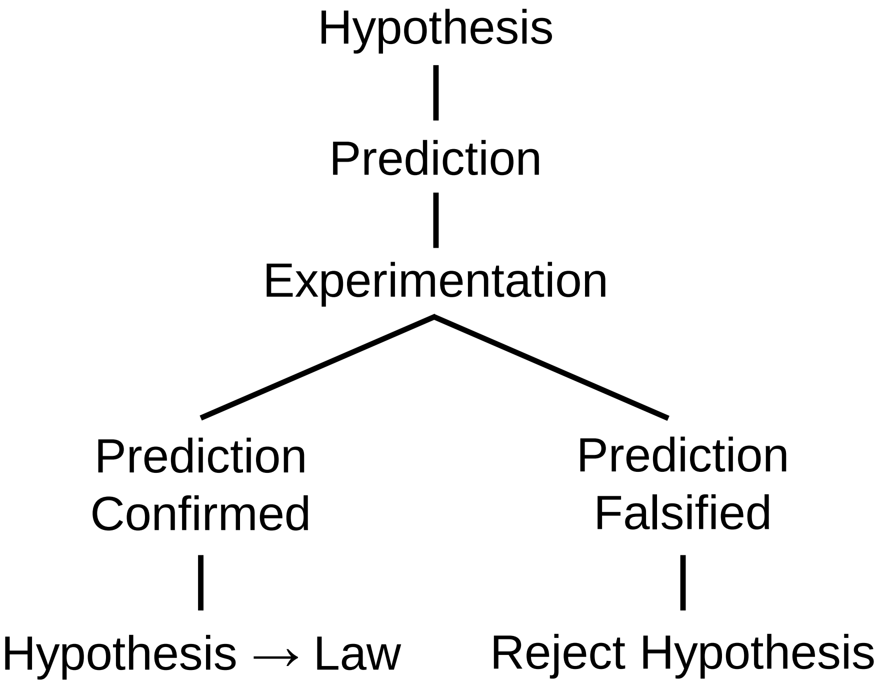
Science explains the cause of observed phenomenon and enables better construction of future systems



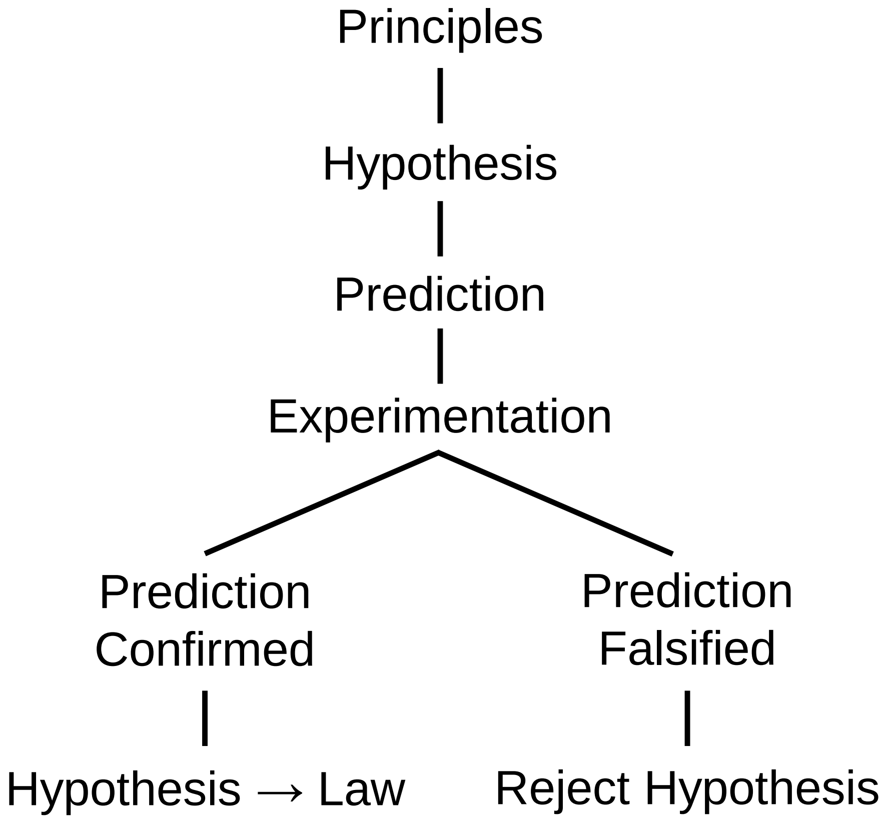
Distinguishing Characteristics of Cyber/Cyber Security

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

Scientific Method: Natural Sciences



Scientific Method: Natural Sciences



Principles

Hypothesis

Prediction

Experimentation

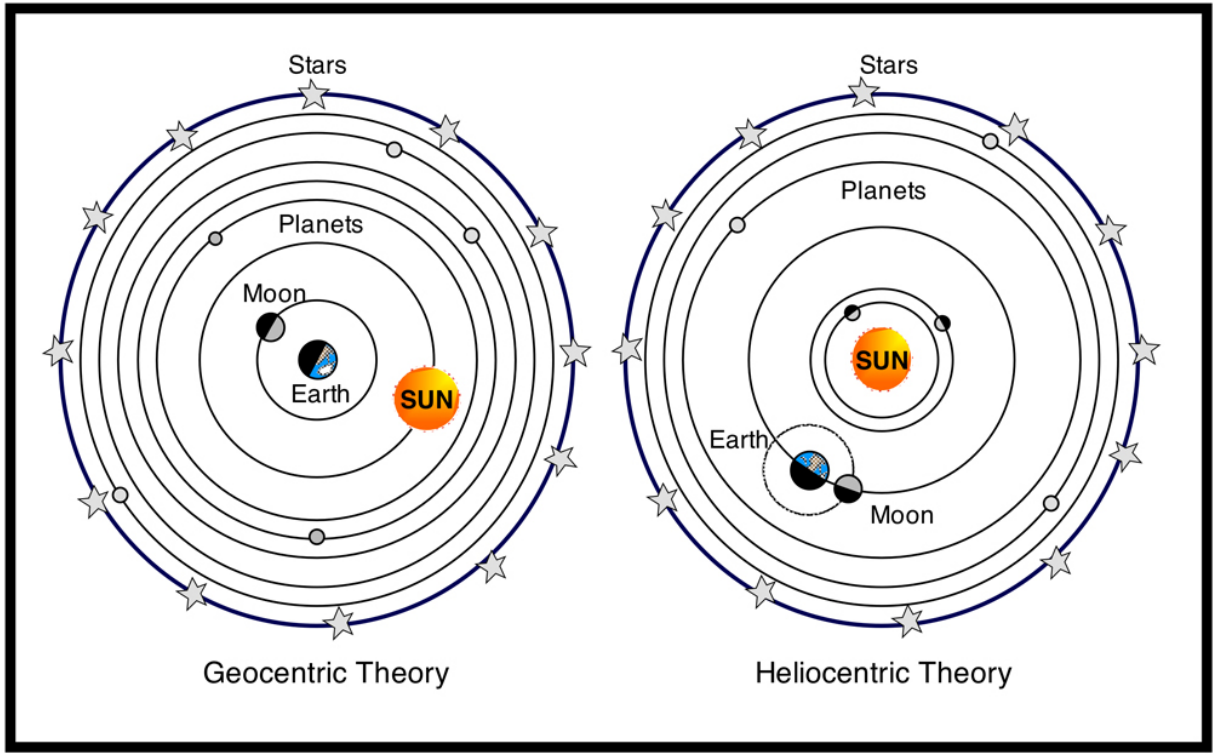
Prediction Confirmed

Prediction Falsified

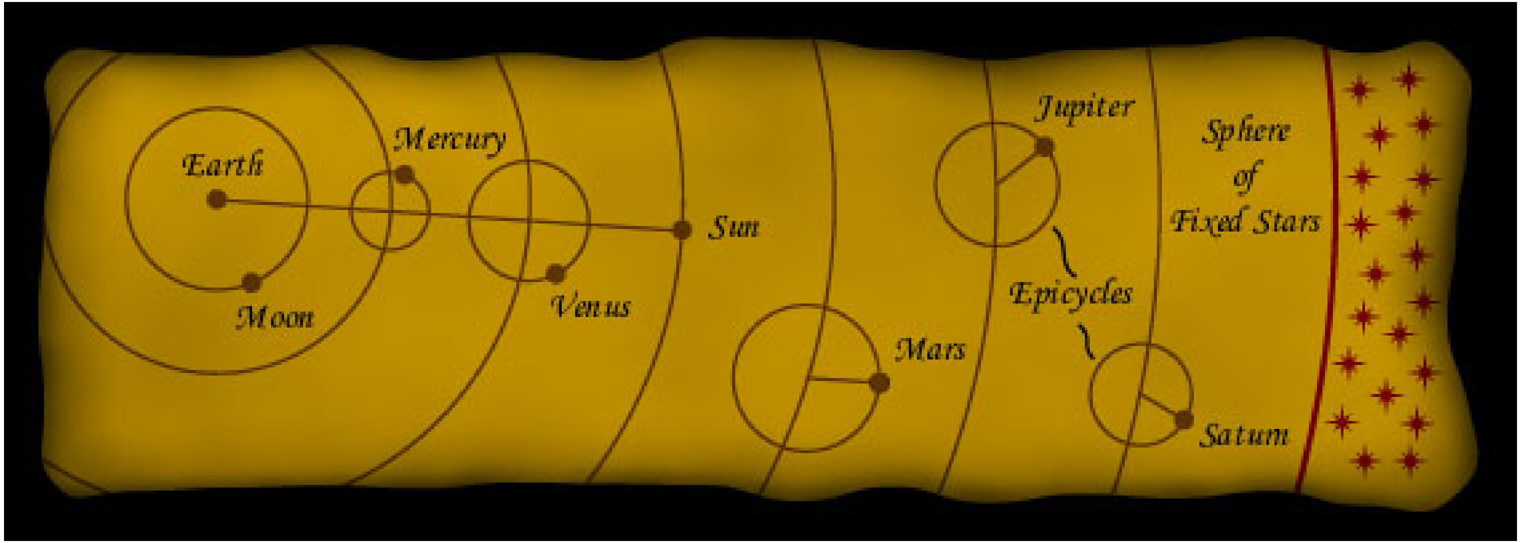
Hypothesis → Law

Reject Hypothesis

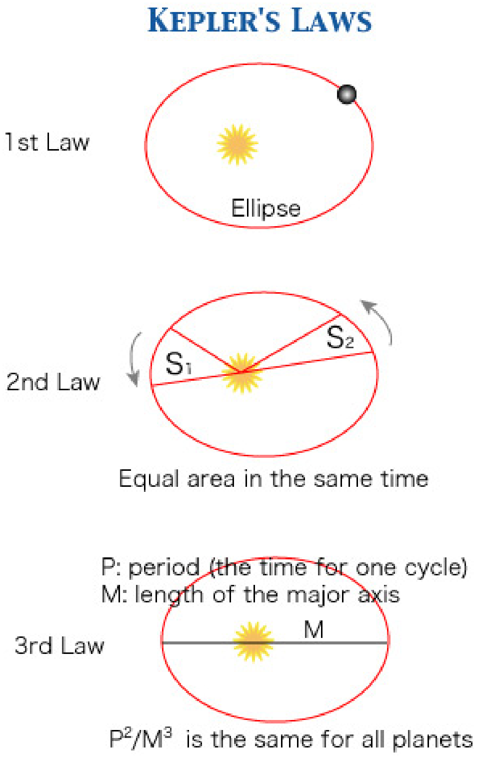
Heliocentric versus Geocentric

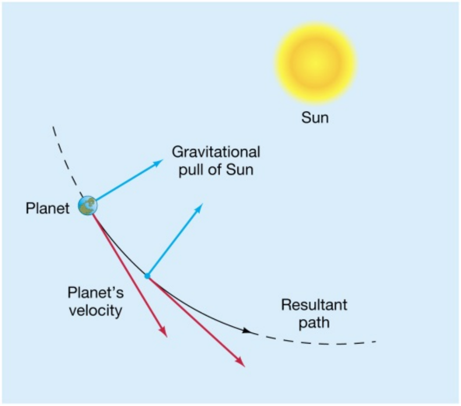


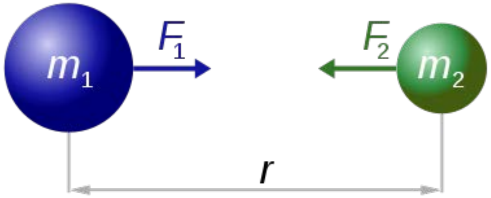
Epicycles


Earth
Moon
Mercury
Venus
Sun
Mars
Jupiter
Epicycles
Saturn
Sphere
of
Fixed Stars

Circles versus Ellipses


Kepler's Laws
1st Law
Ellipse
2nd Law
S1
S2
Equal area in the same time
P: period (the time for one cycle)
M: length of the major axis
3rd Law
M
P²/M³ is the same for all planets

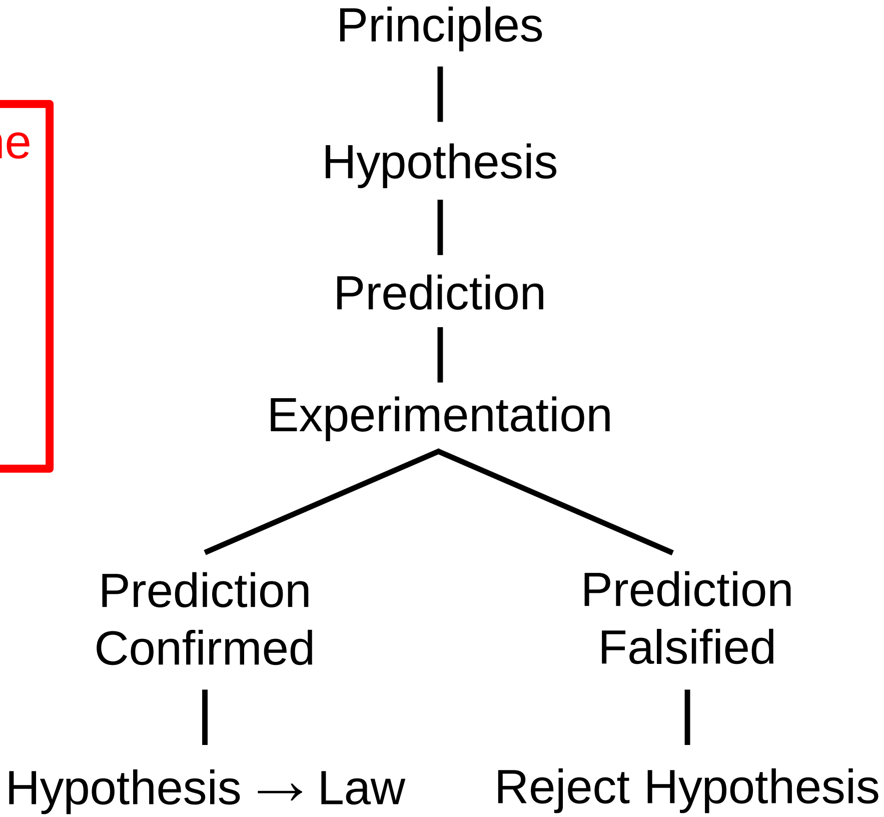




$$F_1 = F_2 = G\frac{m_1 \times m_2}{r^2}$$

Scientific Method: Cyber Sciences

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



Principles

Hypothesis

Prediction

Experimentation

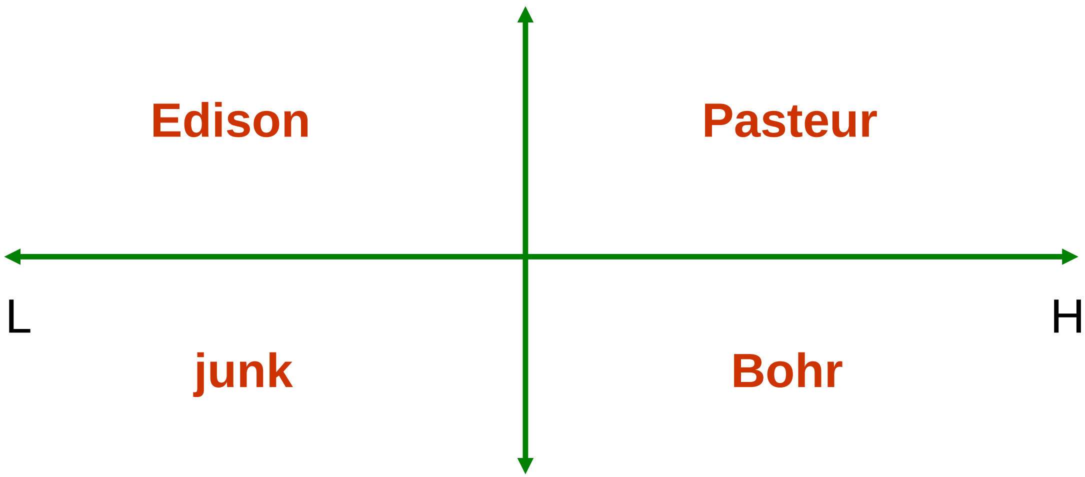
Prediction Confirmed

Hypothesis → Law

Prediction Falsified

Reject Hypothesis

Science Quadrants



Utility

H

Edison

Pasteur

Fundamental Understanding

L

H

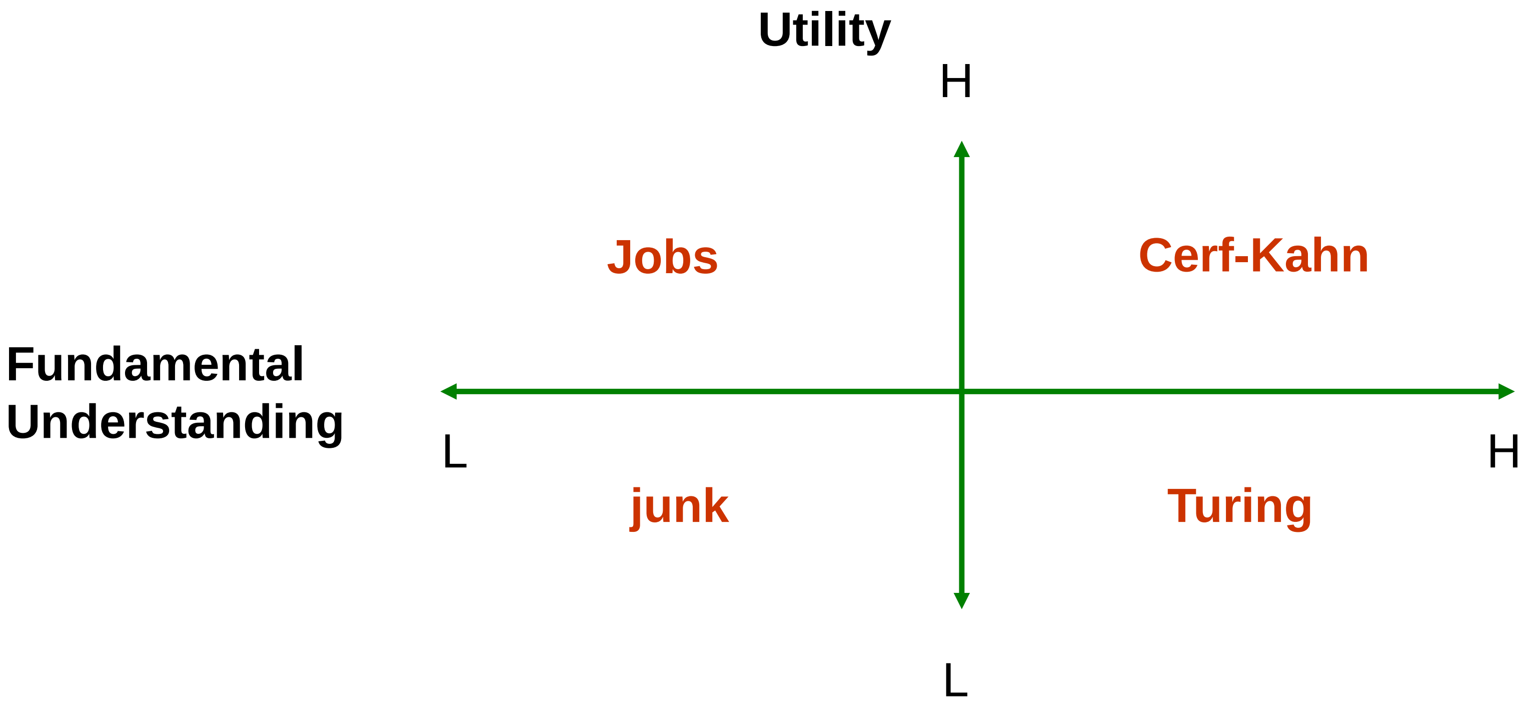
junk

Bohr

L

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

Cyber Science Quadrants



Utility

H

Jobs

Cerf-Kahn

Fundamental Understanding

L

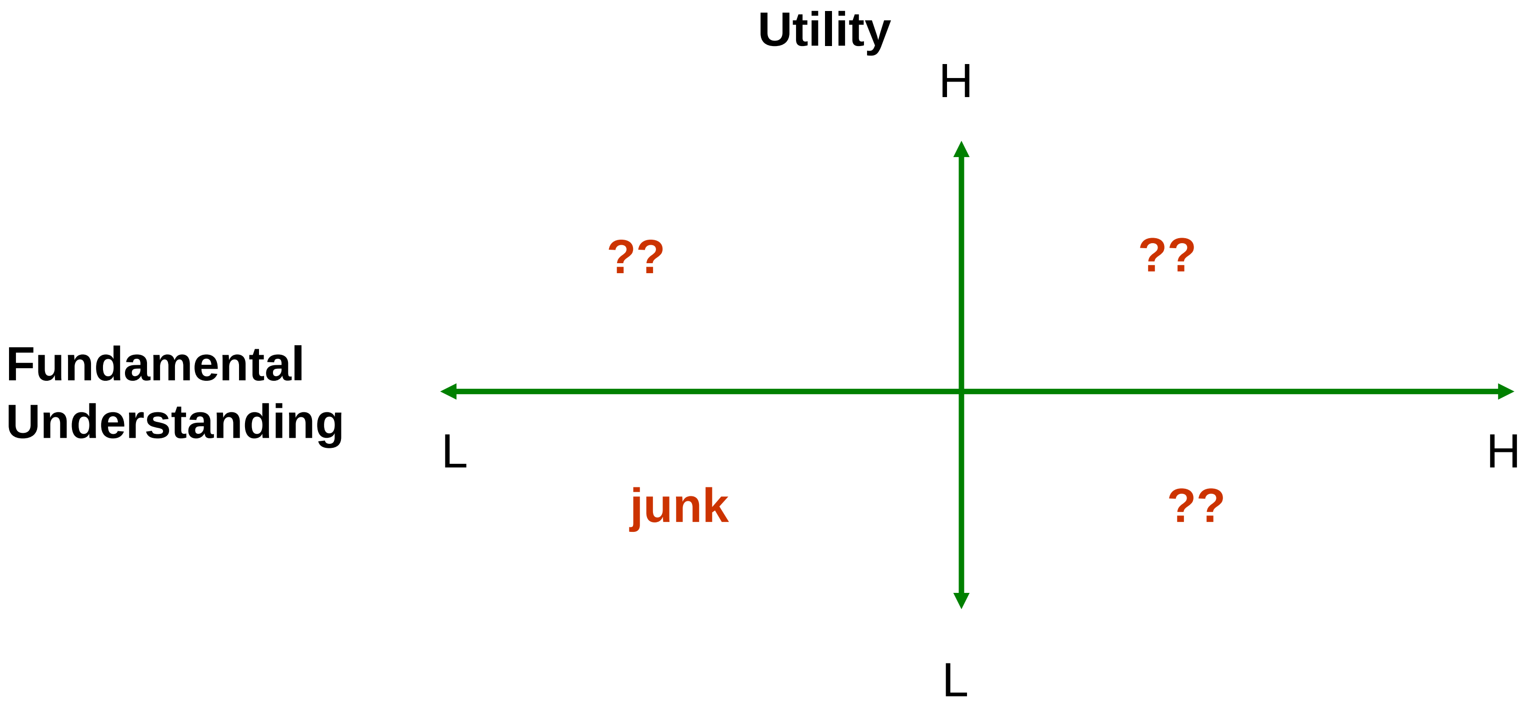
H

junk

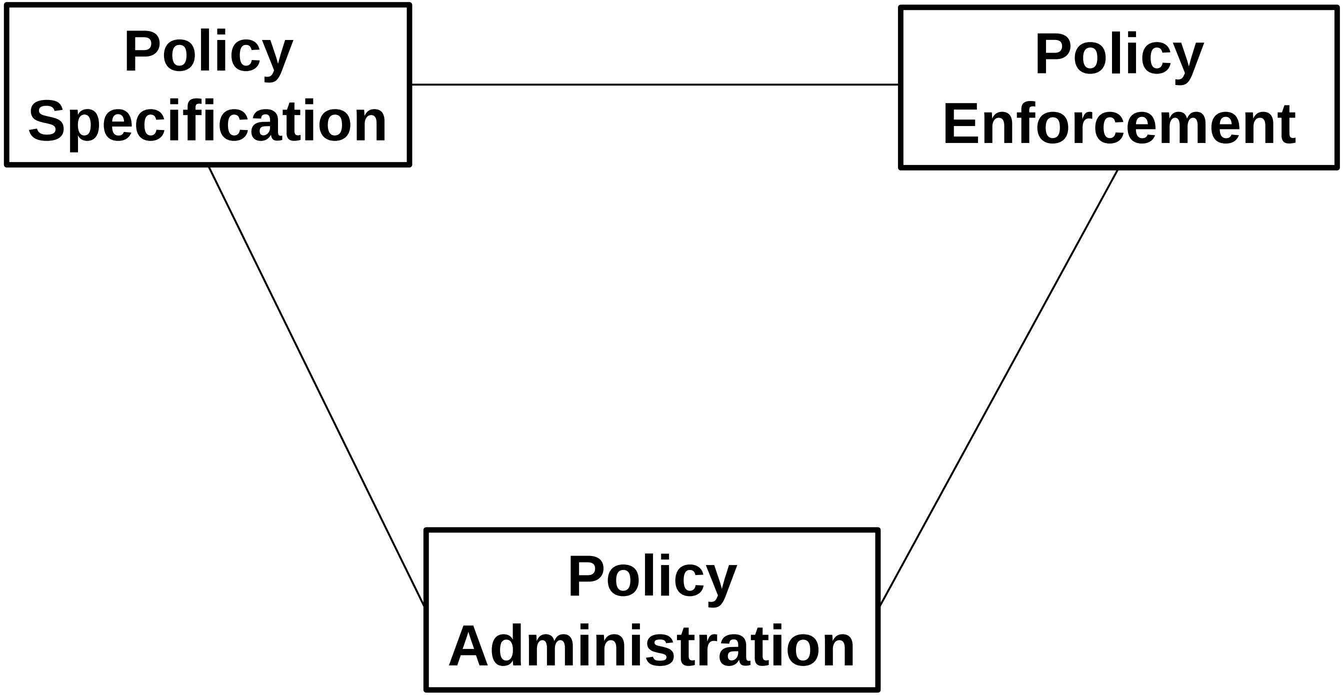
Turing

L

Cyber Security Quadrants



Access Control Decomposition

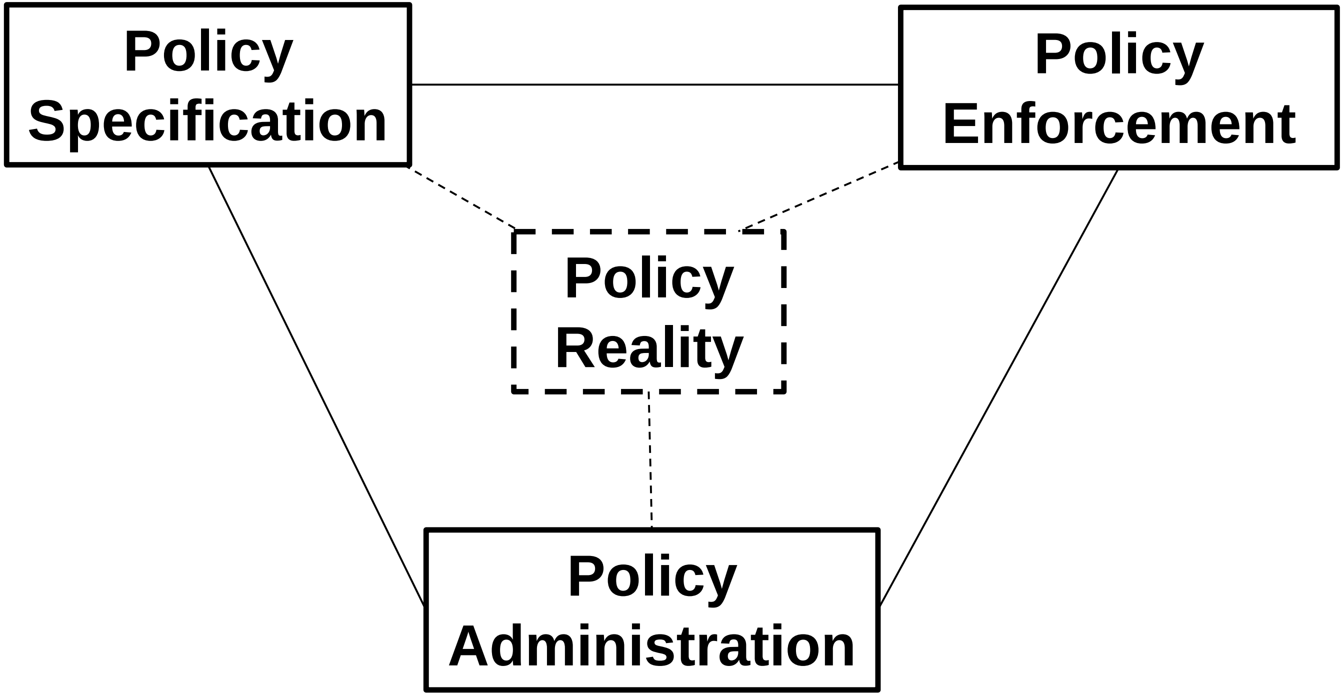


Policy Specification

Policy Enforcement

Policy Administration

Access Control Decomposition



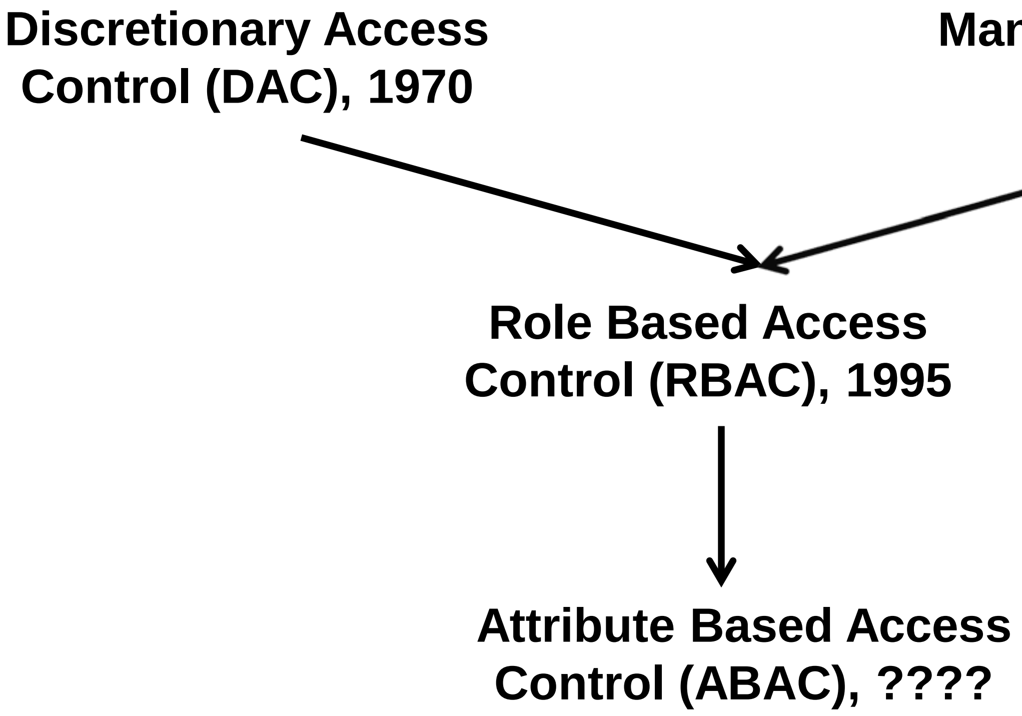
Policy Specification

Policy Enforcement

Policy Reality

Policy Administration

Access Control



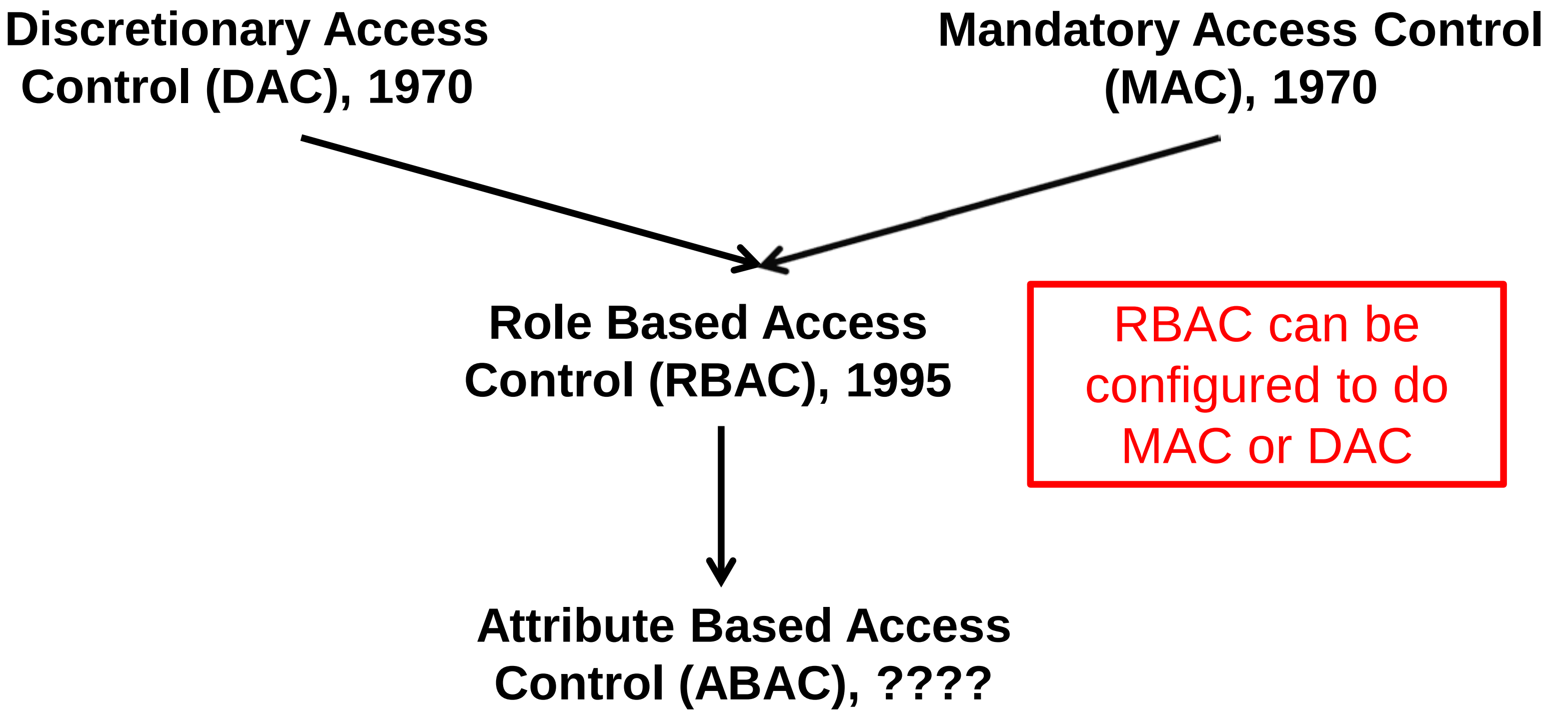
Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Access Control



Discretionary Access Control (DAC), 1970

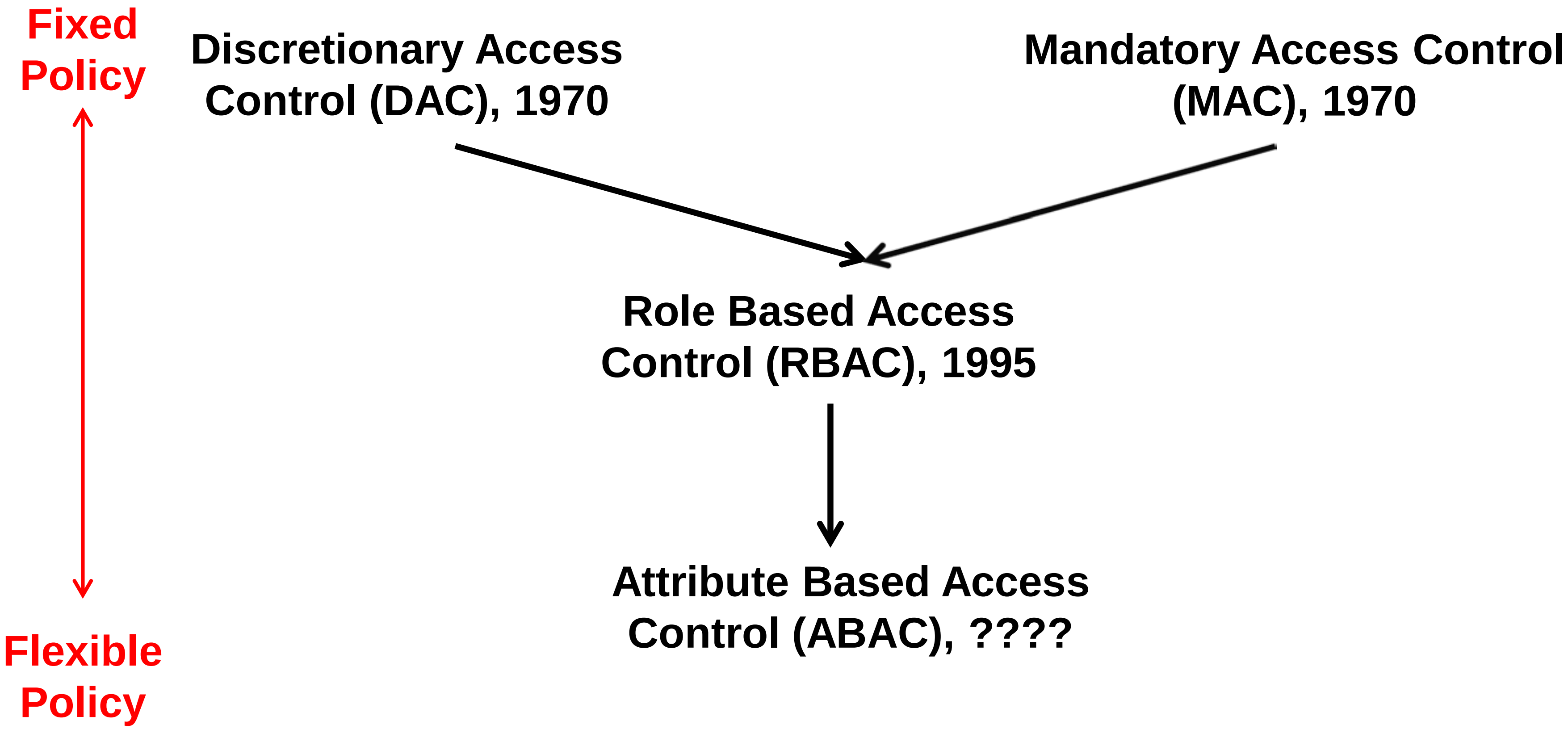
Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

RBAC can be configured to do MAC or DAC

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

Access Control



Fixed Policy

Discretionary Access Control (DAC), 1970

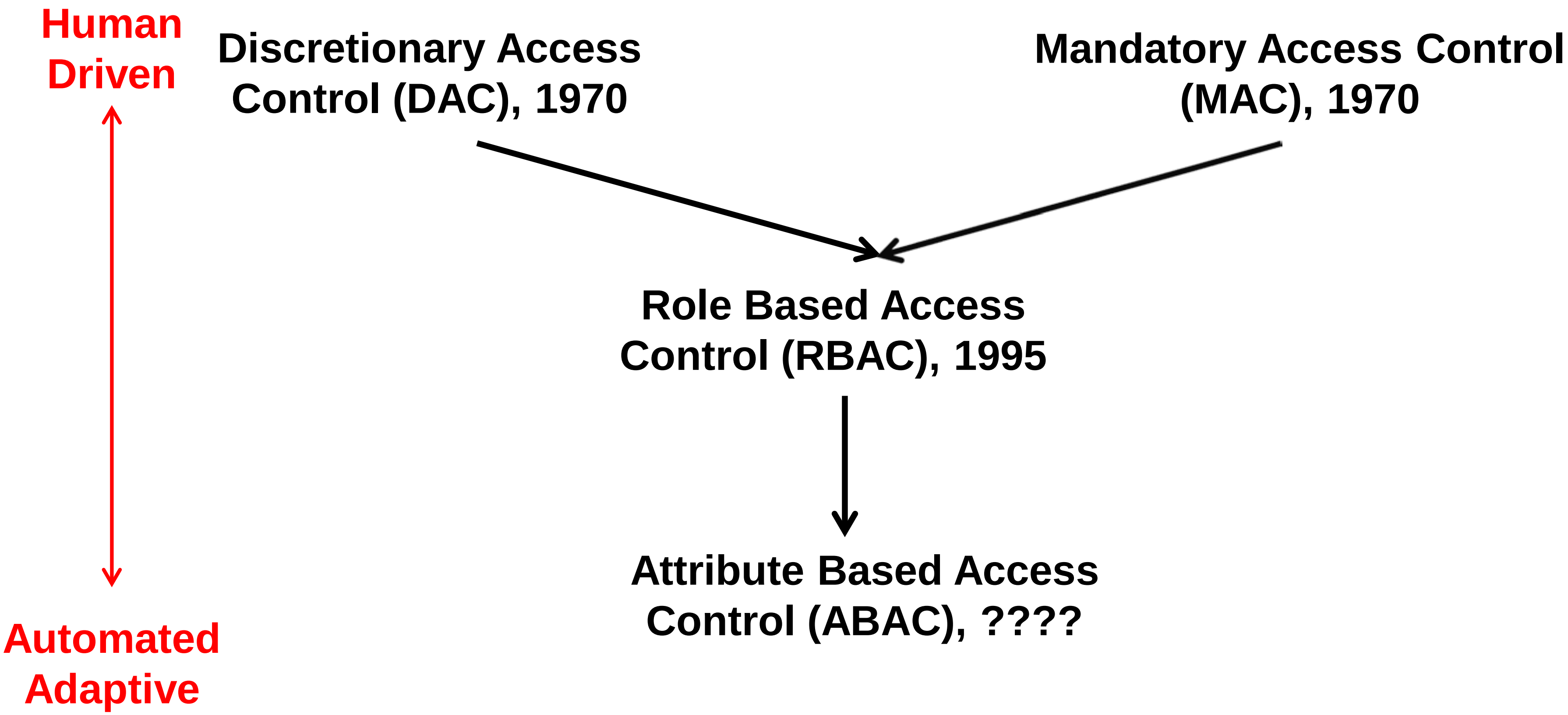
Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Flexible Policy

Access Control



Human Driven

Discretionary Access Control (DAC), 1970

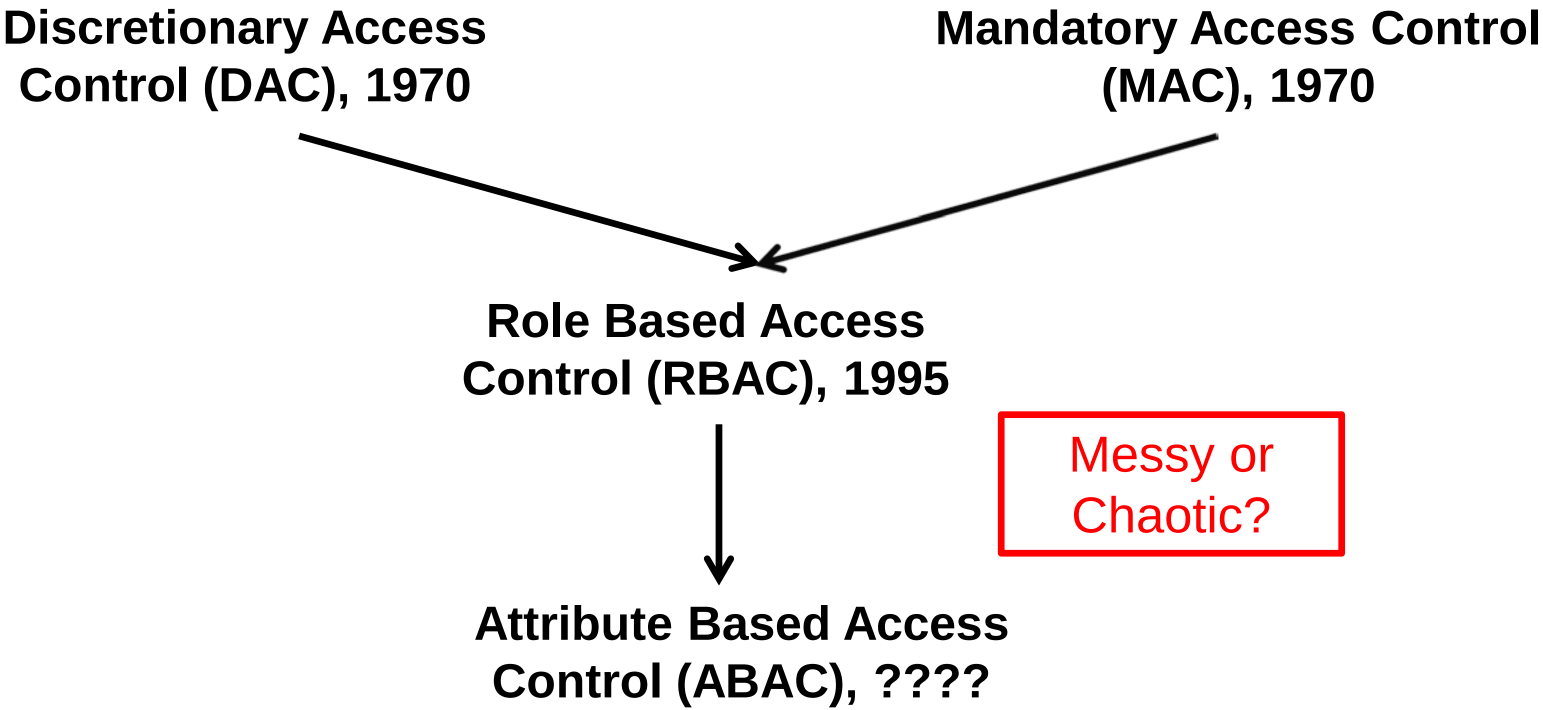
Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Automated Adaptive

Access Control



Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

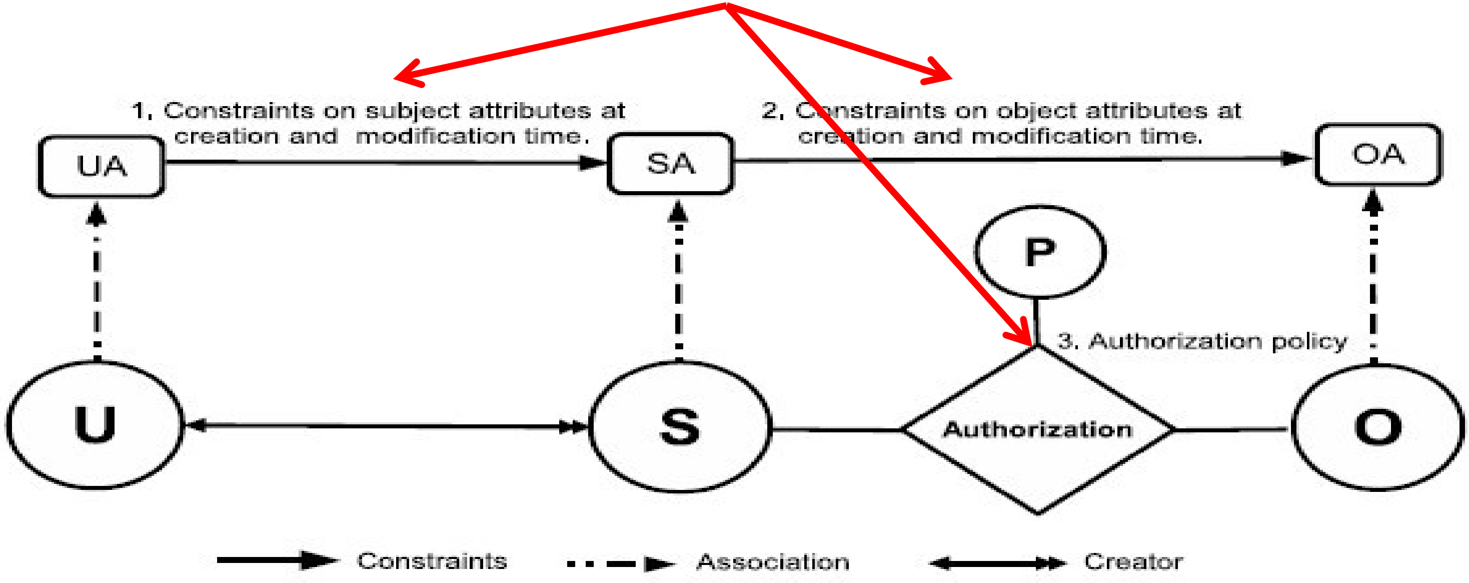
Role Based Access Control (RBAC), 1995

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

Messy or Chaotic?

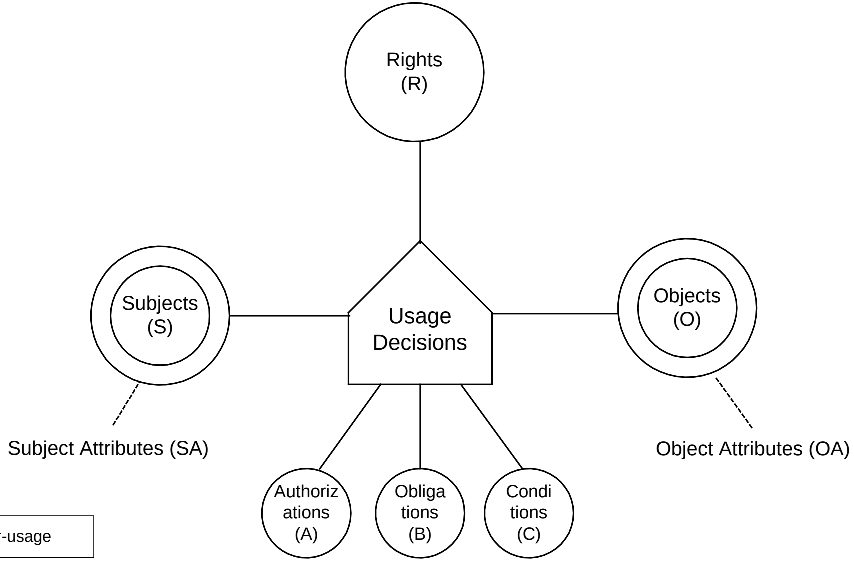
ABAC Model Structure

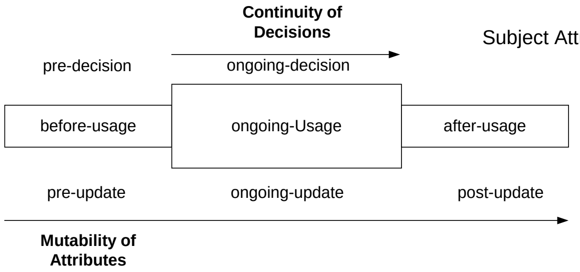
Policy Configuration Points


1, Constraints on subject attributes at creation and modification time.
2, Constraints on object attributes at creation and modification time.
UA
SA
OA
P
3. Authorization policy
U
S
Authorization
O
Constraints
Association
Creator

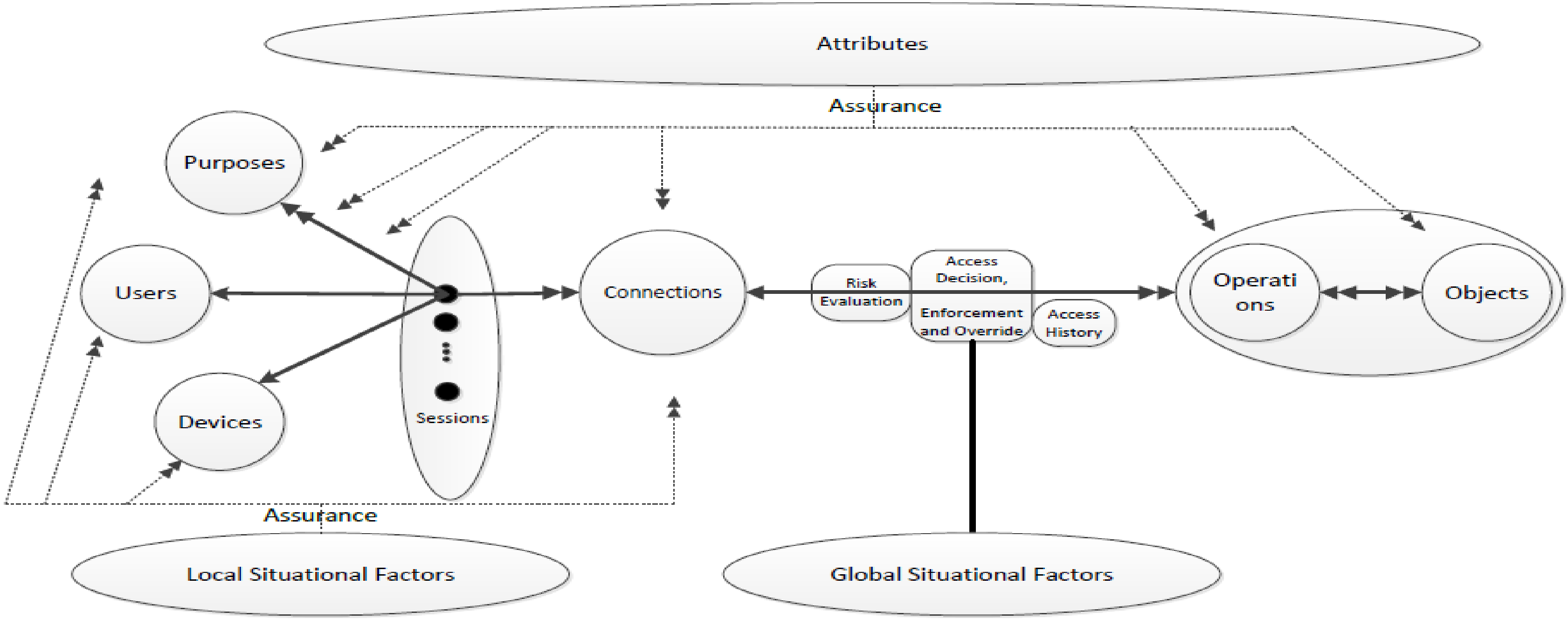
Usage Control Model (UCON)

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

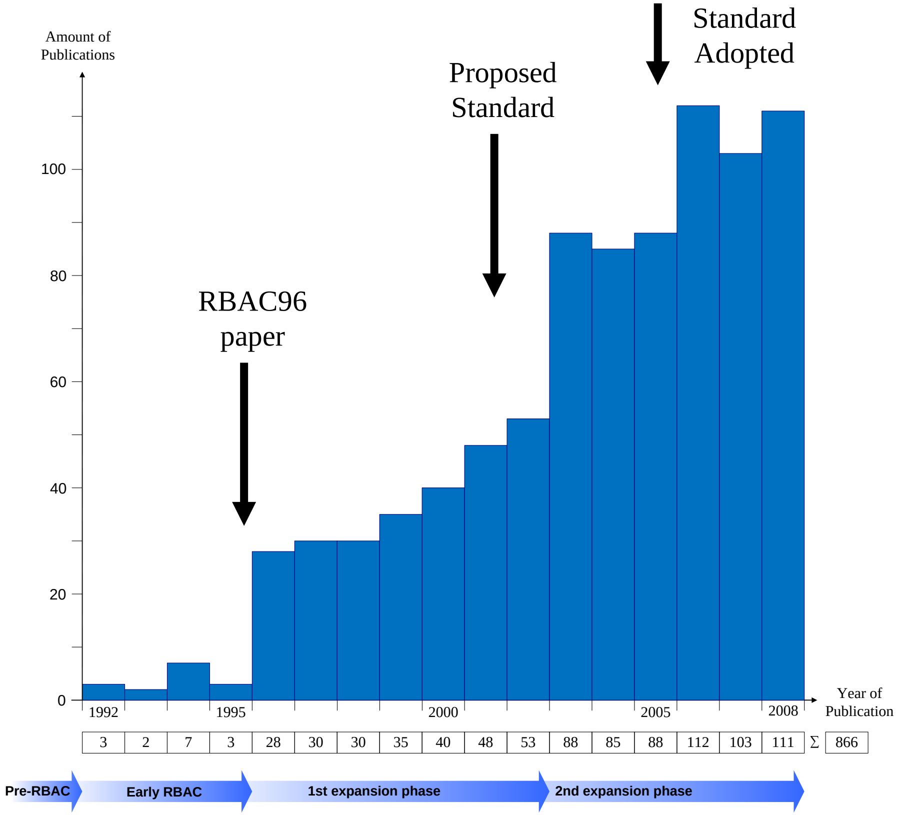




Risk Adaptive Access Control (RAdAC)



The RBAC Story

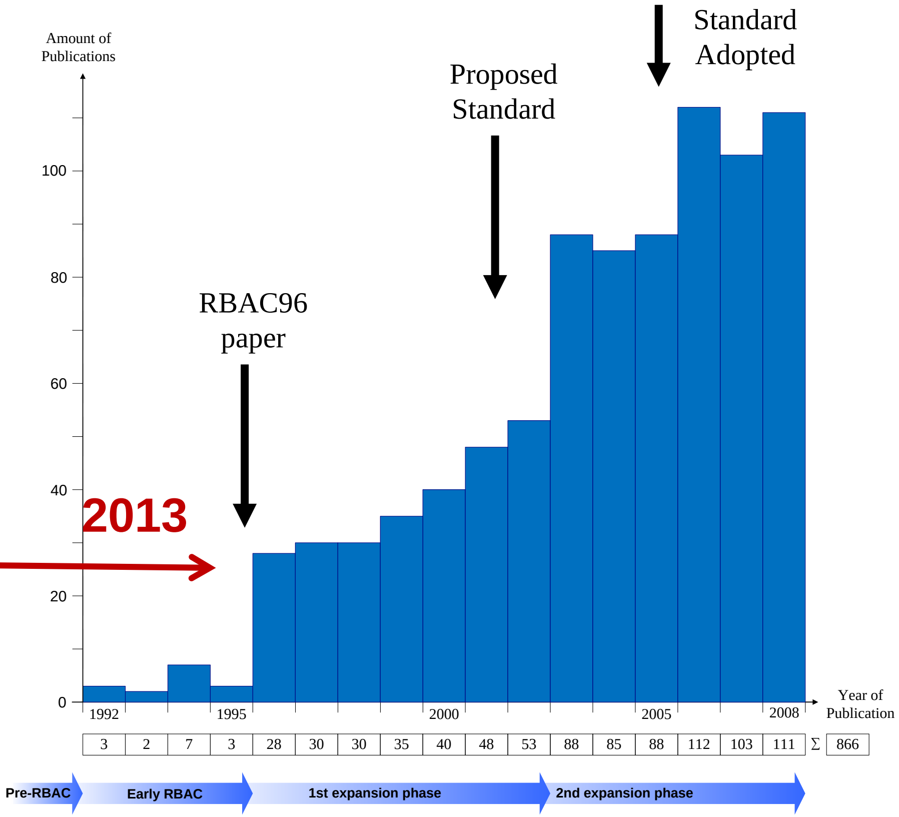


RBAC96 paper

Proposed Standard

Standard Adopted

ABAC Status



199x?

2013

ABAC still in pre/early phase

Access Control Prognosis

- 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