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

IIT Roorkee, Cognizance 2014
March 21, 2014

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”
Perennial State of Cyber Security

"The Red Queen has to run faster and faster in order to keep still where she is. That is exactly what you all are doing!"

Micro-security

Macro-security
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 cloud

- Entanglement of cyber-physical-social space
  - Just starting
Enable system designers and operators to say:

This system is secure

There is an infinite supply of low-hanging attacks

Not attainable
Enable system designers and operators to say:

This system is secure

There is an infinite supply of low-hanging attacks

Alternate goal:

This system is as secure as possible

More secure is always better
Enable system designers and operators to say:

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

Many successful examples
Enable system designers and operators to say:

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

Many successful examples
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
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

Hypothesis

Prediction

Experimentation

Prediction Confirmed

Hypothesis → Law

Prediction Falsified

Reject Hypothesis
Scientific Method: Natural Sciences

Paradigms

Hypothesis

Prediction

Experimentation

Prediction Confirmed

Prediction Falsified

Hypothesis → Law

Reject Hypothesis
Heliocentric versus Geocentric

Geocentric Theory

Heliocentric Theory

World-Leading Research with Real-World Impact!
Epicycles
Circles versus Ellipses

**Kepler’s Laws**

1st Law

![Ellipse](image)

Equal area in the same time

2nd Law

![Equal area](image)

P: period (the time for one cycle)
M: length of the major axis

3rd Law

![P²/M³](image)

P²/M³ is the same for all planets

\[ F_1 = F_2 = G \frac{m_1 m_2}{r^2} \]

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Science explains the cause of observed phenomenon and enables better construction of future systems.
Science Quadrants

---

Fundamental Understanding

- Edison
- Pasteur
- junk
- Bohr

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

---

World-Leading Research with Real-World Impact!
Cyber Security Quadrants

Utility

H

L

H

L

junk

??

??

Fundamental Understanding
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

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

RBAC can be configured to do MAC or DAC
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

Attribute Based Access Control (ABAC), ???

Fixed Policy

Flexible Policy

© Ravi Sandhu

World-Leading Research with Real-World Impact!
Access Control

Discretionary Access Control (DAC), 1970

Mandatory Access Control (MAC), 1970

Role Based Access Control (RBAC), 1995

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

Human Driven

Automated Adaptive

© Ravi Sandhu

World-Leading Research with Real-World Impact!
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?
Perennial State of Cyber Security

"The Red Queen has to run faster and faster in order to keep still where she is. That is exactly what you all are doing!"

Micro-security  Macro-security

World-Leading Research with Real-World Impact!