Cyber Security
A Personal Perspective

Prof. Ravi Sandhu
Executive Director and Endowed Chair

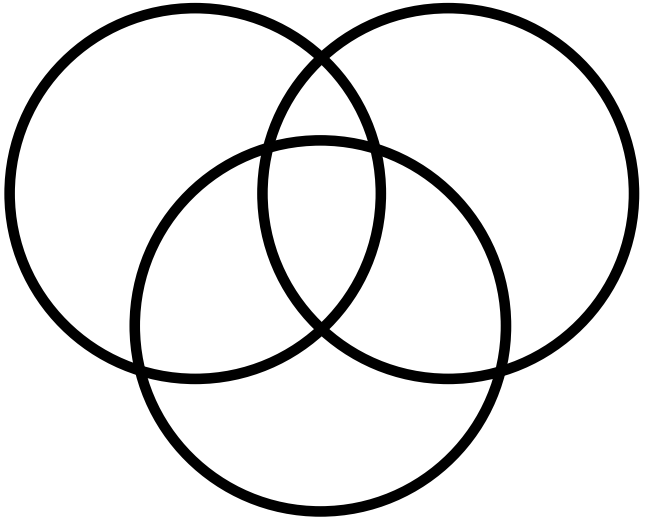
January 15, 2016

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

Prognosis

- Cyberspace will become orders of magnitude more complex and confused very quickly
  - Cyber and physical distinction will disappear
  - Threats will go beyond money to physical harm and danger to life and body
- Overall this is a very positive development and will enrich human society
- It will be messy but need not be chaotic!
- Cyber security research and practice are loosing ground

Security Objectives



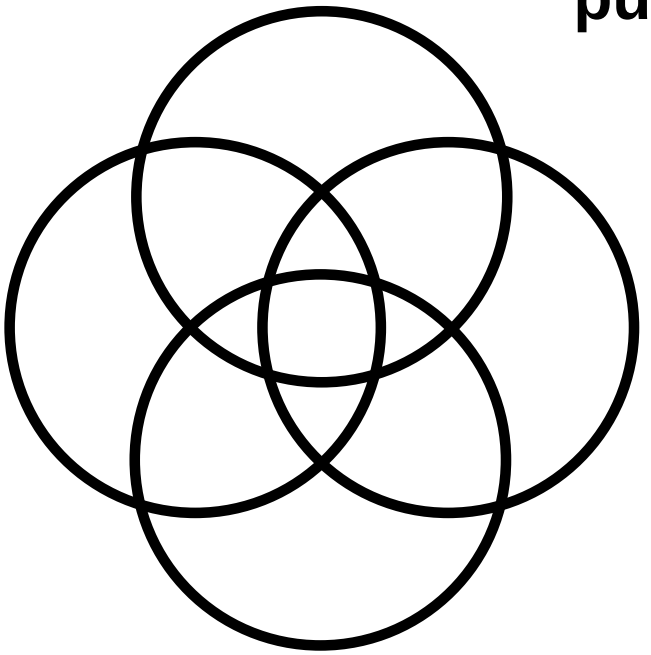
INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives

USAGE
purpose

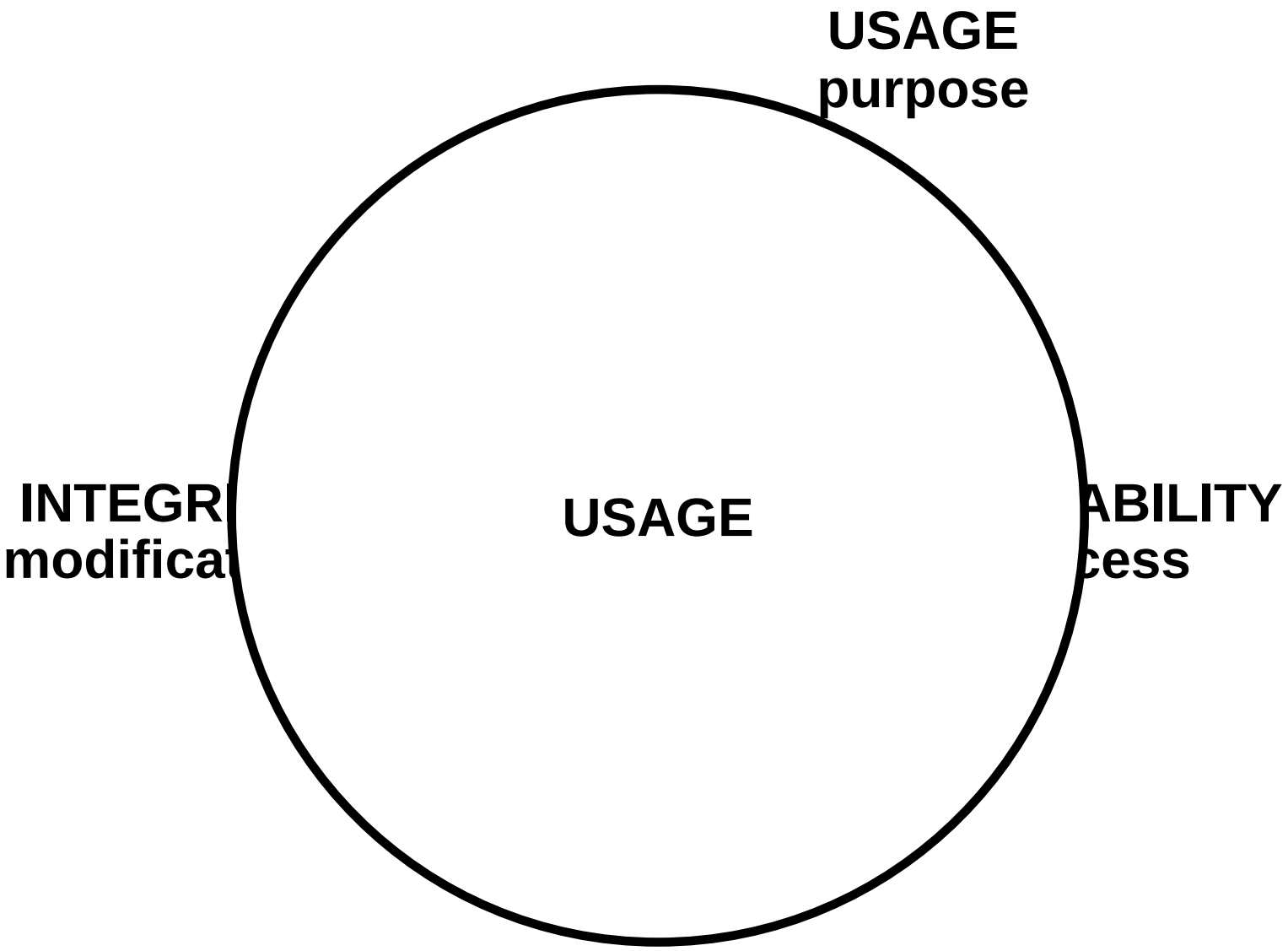


INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives



Security Objectives

Single Enterprise
- **owns all the information**
- **employs all the users**

Multiple Interacting Parties
- **no one owns all the information**
- **no one can unilaterally impose policy on all the users**

More than 2 decades of encryption versus privacy debate

Cyber Security Scope

- Computer security
- Information security =
  - Computer security + Communications security
- Information assurance
- Mission assurance
  - Includes cyber physical

Fundamental Challenge

- What is fundamental to cyber security?
- Where are the boundaries of a cyber system?
- What are the goals of cyber security?

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure

  Not attainable

- There is an infinite supply of attacks

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure enough

Many successful examples

The ATM Paradox

- The ATM (Automatic Teller Machine) system is
  - secure enough
  - global in scope
- Not attainable via current cyber security science, engineering, doctrine
  - not studied as a success story
- Similar paradoxes apply to
  - on-line banking
  - e-commerce payments

- US President's nuclear football
- Secret formula for Coca-Cola

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure enough

- In an innovative ecosystem the innovation drive will ensure that the bar for enough will be fairly low

Productivity-Security

- 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 sell unproven solutions

There is a middle ground
We don't know how to predictably find it

Grand Challenges

- Develop a scientific discipline
  - to predictably find the sweet spots for different application and mission contexts
  - to predictably find, incentivize and deploy microsec that leads to desirable macrosec outcomes
  - that can be meaningfully taught in Universities at all levels: BS, MS, PhD

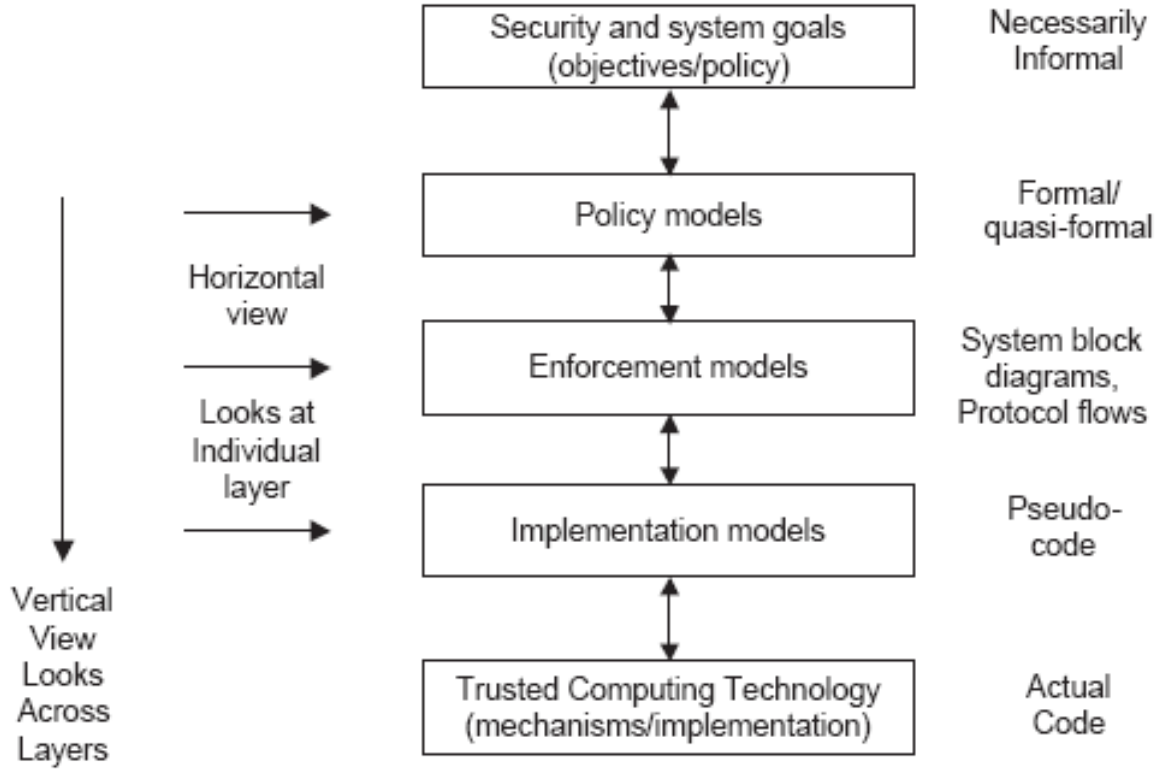
- Prognosis
  - we shall succeed (we have no choice)
  - but we need to change to succeed

Butler Lampson Paraphrased (I think)

- Computer scientists could never have designed the web because they would have tried to make it work.
  - But the Web does “work.”
  - What does it mean for the Web to “work”?
- Security geeks could never have designed the ATM network because they would have tried to make it secure.
  - But the ATM network is “secure.”
  - What does it mean for the ATM network to be “secure”?

Bellovin's Slides digression

PEI Models



Idealized

Enforceable (Approximate)

Codeable

Limits on Security

- Trojan horse/malware
- Covert channels/side channels
- Inference
- Analog hole
- Assured enforcement
- Privilege escalation
- Policy comprehension and analysis
- Predicting value and future usage of data
- …..

Reference Material digression