The Science, Engineering, and Business of Cyber Security

Prof. Ravi Sandhu

Executive Director, Institute for Cyber Security
Lutcher Brown Endowed Chair in Cyber Security

COS Research Conference
October 18, 2013

ravi.sandhu@utsa.edu
www.profsandhu.com
www.ics.utsa.edu
Founded in 2007 to be a world leader in cyber security research

A unit in the College of Sciences, with strong ties to the Department of Computer Science

Cyber Security in UTSA started in 2000 and is well represented in the Colleges of Science, Engineering and Business
≈ 2010 Department of Defense epiphanies

- Cyberspace is officially recognized by Department of Defense as a new warfare domain akin to land, sea, air and space

- Department of Defense officially admits having and using offensive cyber weapons

- Department of Defense officially admits malware penetrations in its classified networks
Cyber Security Objectives

INTEGRITY
modification
misdirection

CONFIDENTIALITY
disclosure

AVAILABILITY
access
Cyber Security Objectives

CONFIDENTIALITY
  disclosure

INTEGRITY
  modification
  misdirection

AVAILABILITY
  access

USAGE
  purpose
  disposal
Security versus Privacy

Security

Privacy
Cyber Security Evolution

- Computer Security
- Communications Security

  Information Security

  Information Assurance

  Mission Assurance
Cyber Security Techniques

Prevent

Detect

Accept
Enable system designers and operators to say:

This system is secure

There is an infinite supply of attacks

Not attainable
Enable system designers and operators to say:

This system is secure enough

Mass scale, not very high assurance
- ATM network
- On-line banking
- E-commerce

One of a kind, extremely high assurance
- US President’s nuclear football

Many successful examples

Science
Engineering
Business
Why is Cyber Security so Hard?

- Halting problem
- Inference
- Weakest link
- Analog hole
- Insider
- Human element
- Usability
- Cyber innovation
- Covert channels
- Side channels
- .................
Cyber Security Prognosis

- Not too bad
- About as good as it is going to get
- The criminal enterprise can only defraud so many
- Big government and big business are a real threat

- Highly asymmetric
- Offense component
- Clandestine
- Dual goals: strong offense, strong defense
- Mankind has somehow kept nuclear, chemical and biological in control. Cyber is different but should be controllable.
ICS Research Thrusts

- Secure Information Sharing
- Social Computing Security
- Secure Provenance-aware Systems
- Privacy Policies and Enforcement

- Trustworthy Cloud Computing
- Secure Multi-Tenants in Cloud
- Big Data Security and Privacy
- Security in Internet of Things

- Malware Detection and Analysis
- Botnet Analysis and Defense
ICS FlexCloud Lab

FlexCloud/FlexFarm
- 1000 cores
- 19TB mirrored RAID
- 35TB SAN

Research
- Attribute-based Access Control
- Secure Data Provenance
- Secure Information Sharing
- Secure Cloud Computing
- Malware Detection and Analysis

Education
- Cloud Computing Courses
- Big Data
- OpenStack Training
- High Performance Computing

Commercial Collaboration/Support
- Rackspace
- Joyent

World-Leading Research with Real-World Impact!