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

Institute for Cyber Security

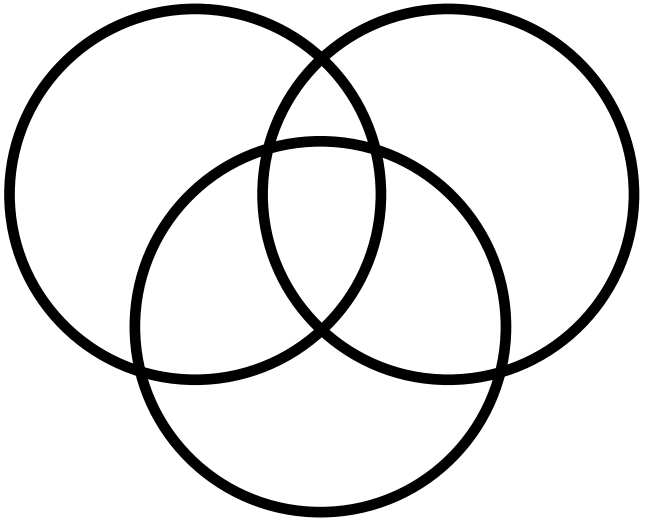
- Founded in 2007 to be a world leader in cyber security research
- A unit in the College of Sciences, with strong ties to the Department of Computer Science
- Cyber Security in UTSA started in 2000 and is well represented in the Colleges of Science, Engineering and Business

Cyberspace

≈ 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



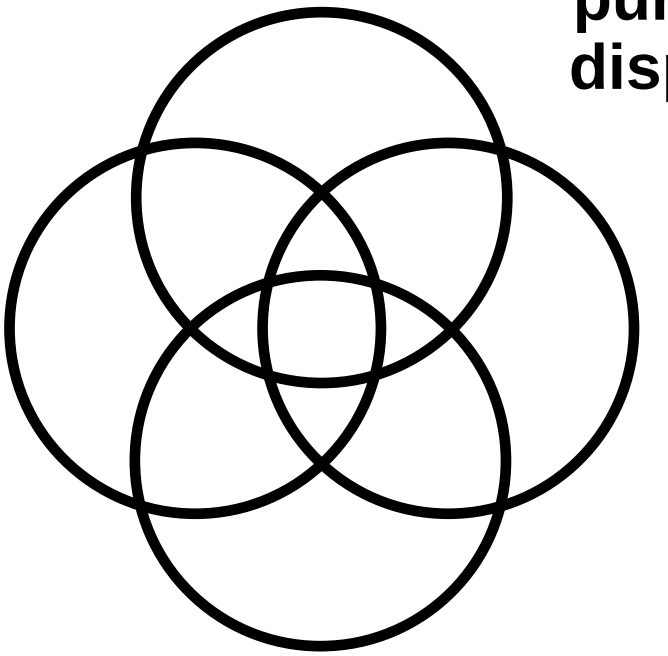
INTEGRITY
modification
misdirection

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Cyber Security Objectives

USAGE
purpose
disposal

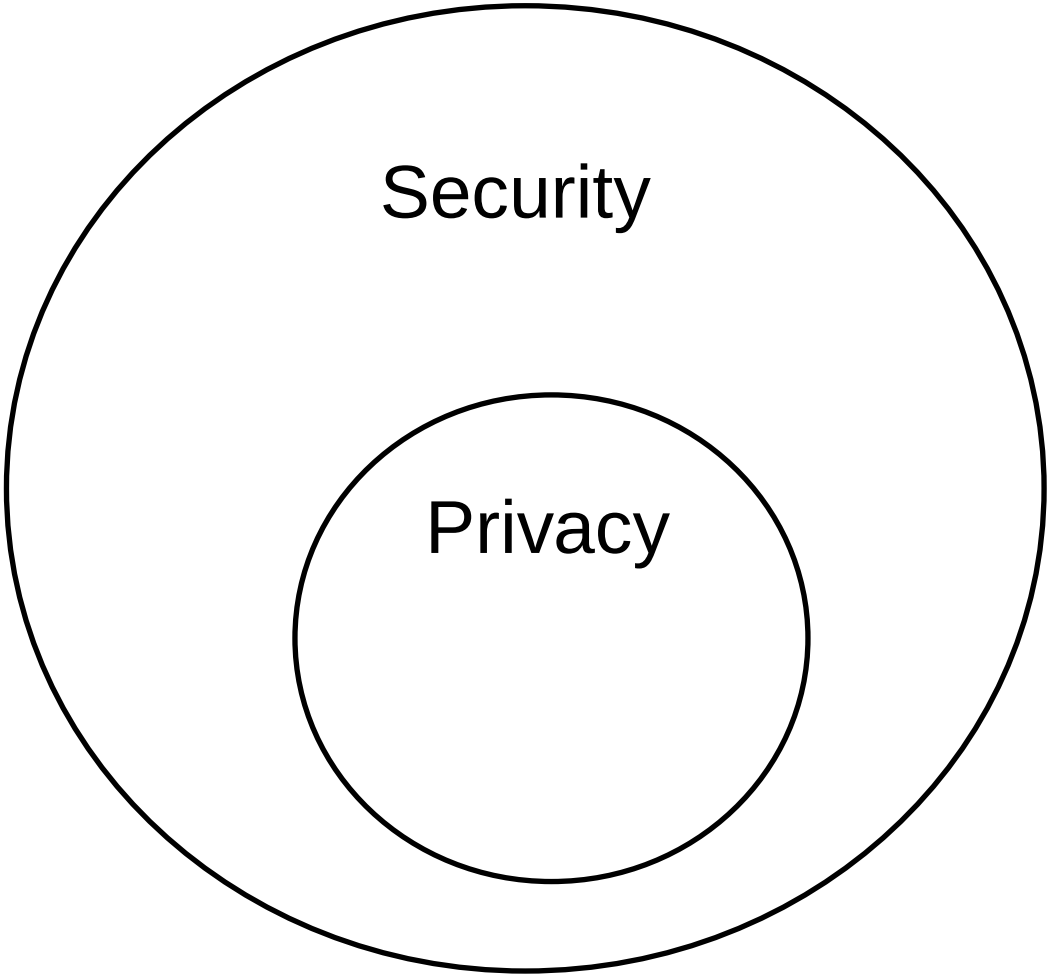


INTEGRITY
modification
misdirection

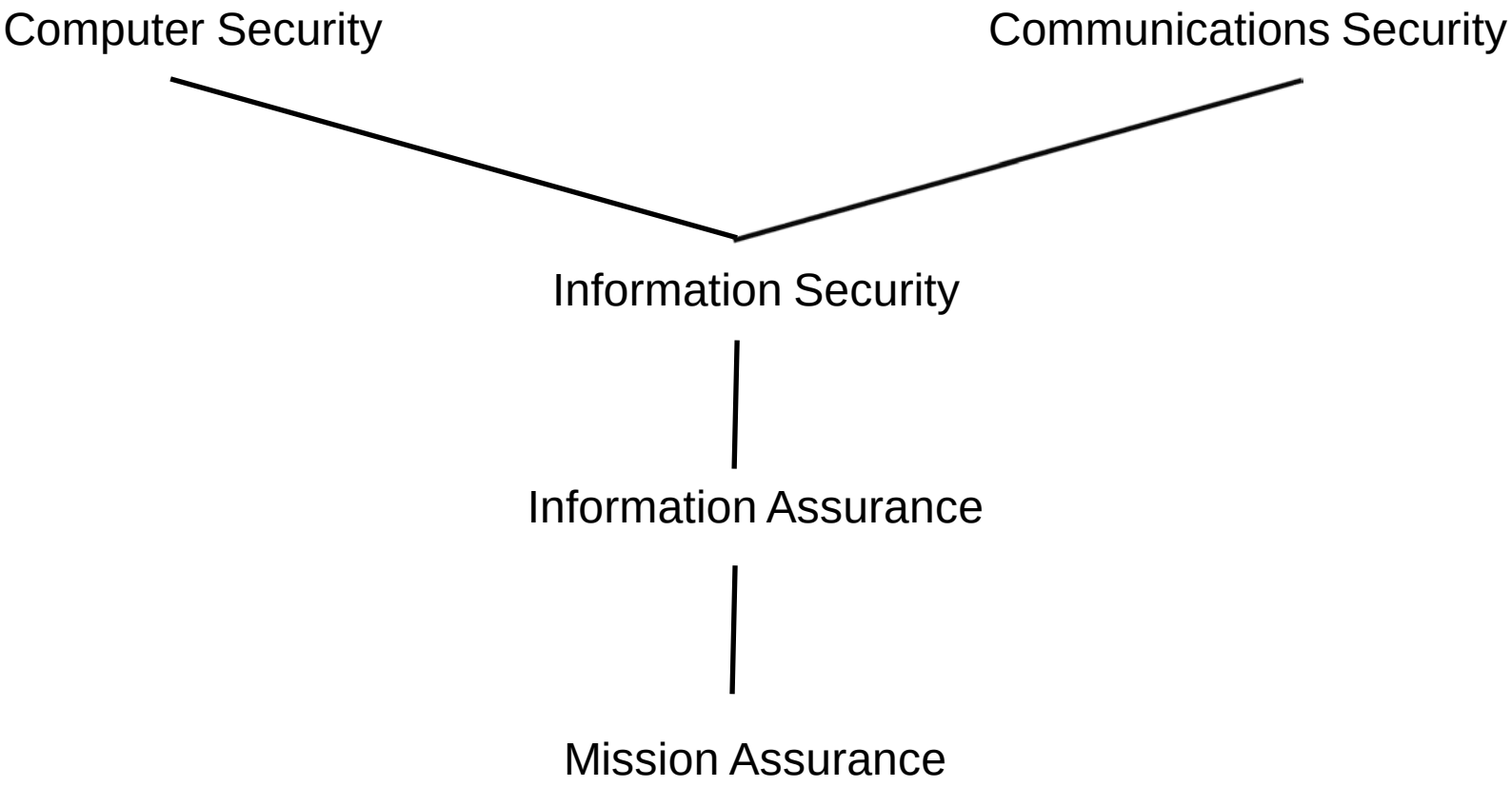
AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security versus Privacy

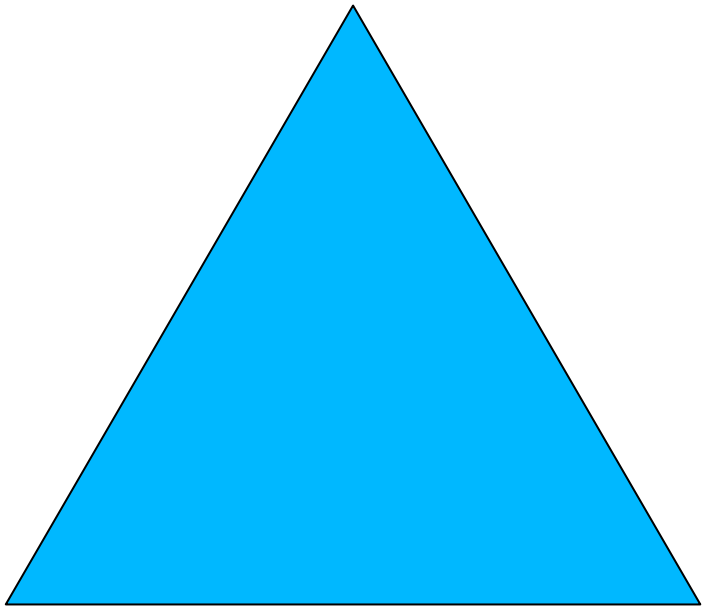


Cyber Security Evolution



Cyber Security Techniques

Prevent



Detect

Accept

Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure

  Not attainable

- There is an infinite supply of attacks

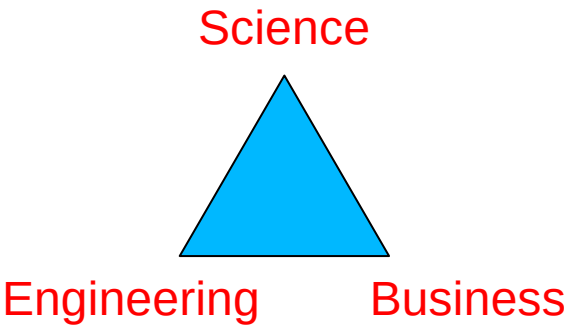
Cyber Security Goal

- Enable system designers and operators to say:

  This system is secure enough

  Many successful examples

- 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

Why is Cyber Security so Hard?

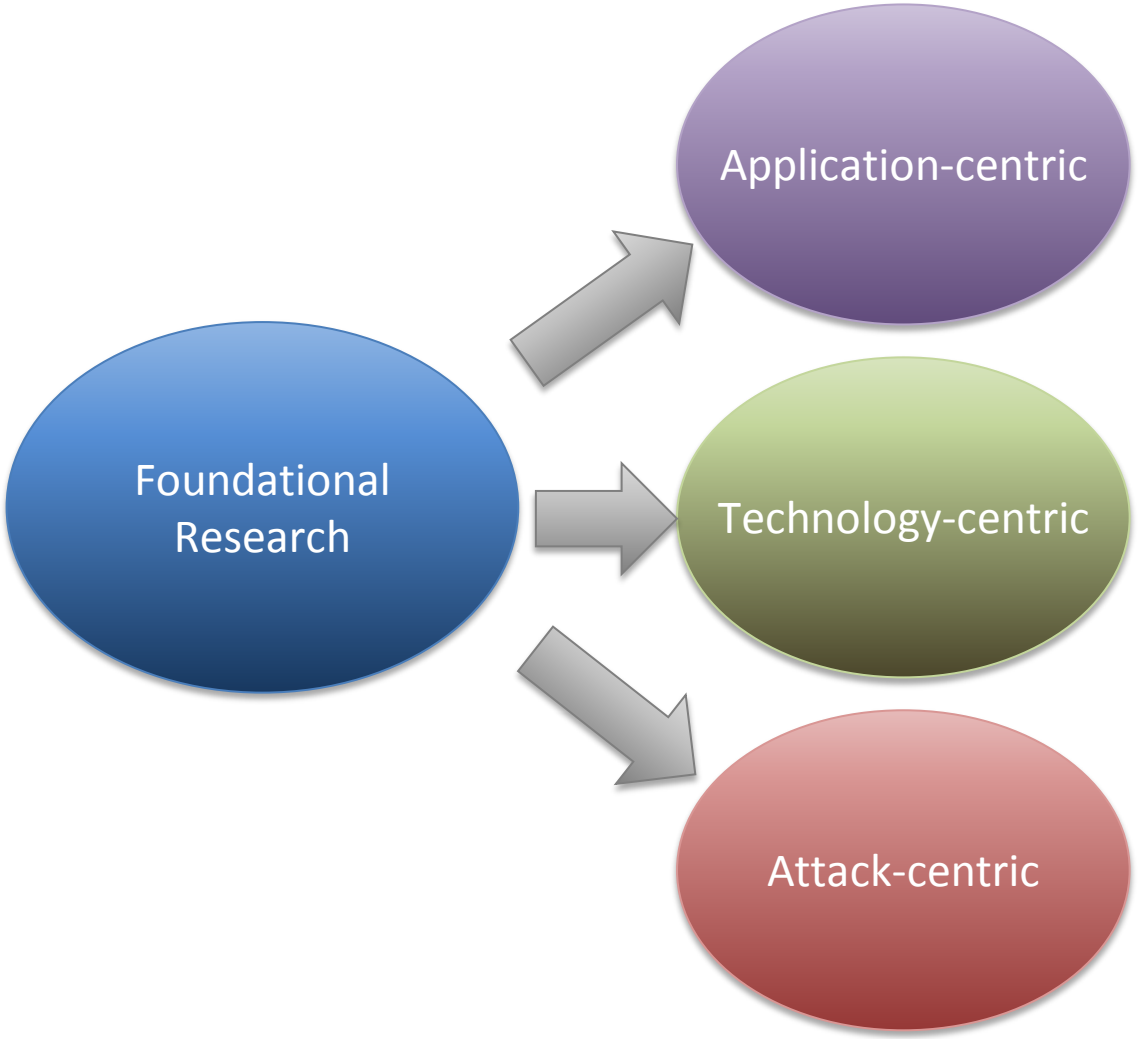
- Halting problem
- Inference
- Weakest link
- Analog hole
- Insider
- Human element
- Usability
- Cyber innovation
- Covert channels
- Side channels
- ……

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