I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

Cyber Security Trends and Challenges

Ravi Sandhu

Executive Director
Professor of Computer Science
Lutcher Brown Chair in Cyber Security

Financial Executives International
San Antonio Chapter

March 19, 2019

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

World-Leading Research with Real-World Impact!

UTSA Computer Science

ICS Mission and History

I·C·S The Institute for Cyber Security

C·SPECC Center for Security and Privacy Enhanced Cloud Computing

MISSION

Sustained excellence in leading edge research

2007-2012
Founded by start-up funding from State of Texas

→

2012-2017
Graduated to a self-sustaining operation

→

2017-2022
Major expansion by winning NSF C-SPECC grant

→

- Established world class laboratories for:
  Secure cloud computing &
  Malware research

In collaboration with:
College of Engineering
College of Business
College of Education
Open Cloud Institute
Cyber Center for Security & Analytics
National Security Collaboration Center
Partnership with 4 NISD High Schools:
Harlan, Woodson, Taft, Business Careers

Cyber Security Perspective

Cyber Security in a Nutshell

"My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that."

— Lewis Carroll, Alice in Wonderland

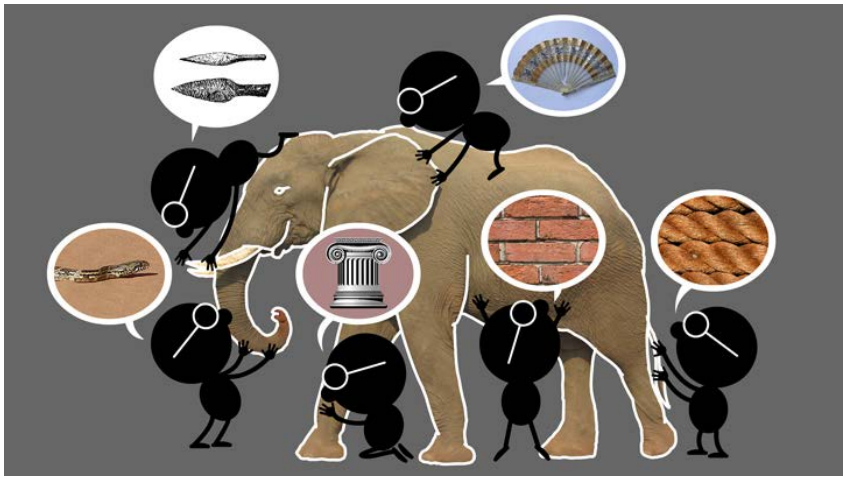
Cyber Security in a Nutshell

"My dear, here we must run as fast as we can, just to stay in place. And if you wish to go anywhere you must run twice as fast as that."

— Lewis Carroll, Alice in Wonderland

Natural vs Cyber Science

Elephant Problem



Cyber-Elephant Problem

Applied vs Foundational Science: Cyber-elephants require applied and foundational combined

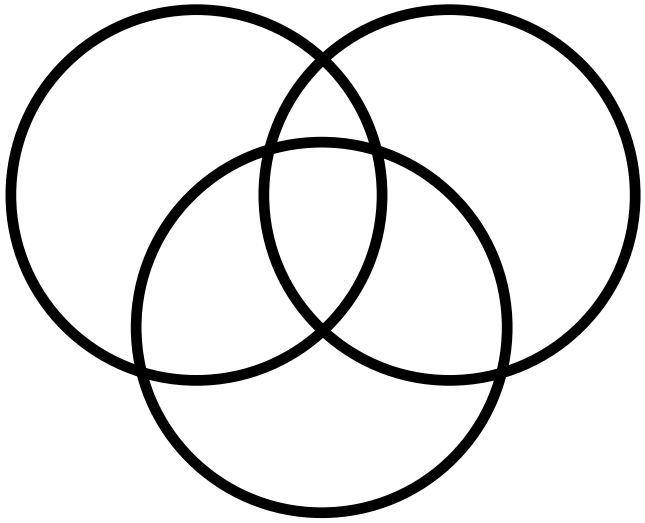
Present vs Future Focus: Rapidly evolving cyber-elephants require future focus

Success Stories

- The ATM (Automatic Teller Machine) system is
  - secure enough
  - global in scope

- US President's nuclear football

Security Objectives



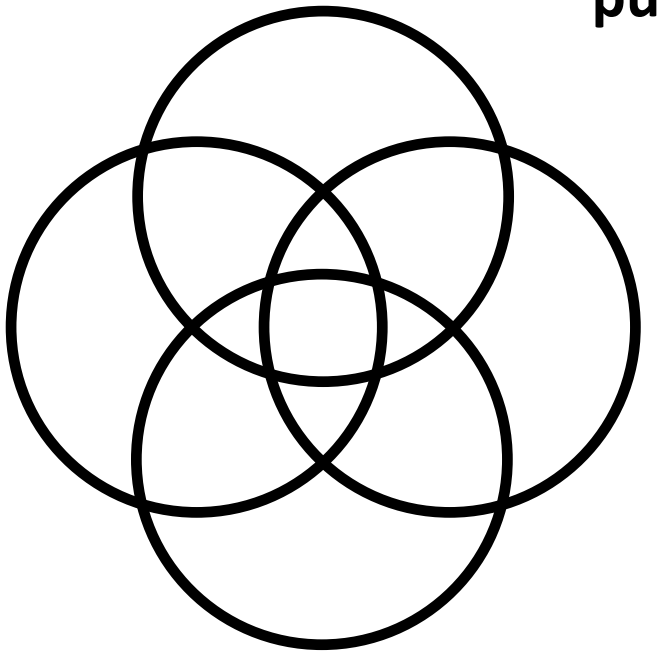
INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives

USAGE
purpose



Covers privacy and intellectual property protection

INTEGRITY
modification

AVAILABILITY
access

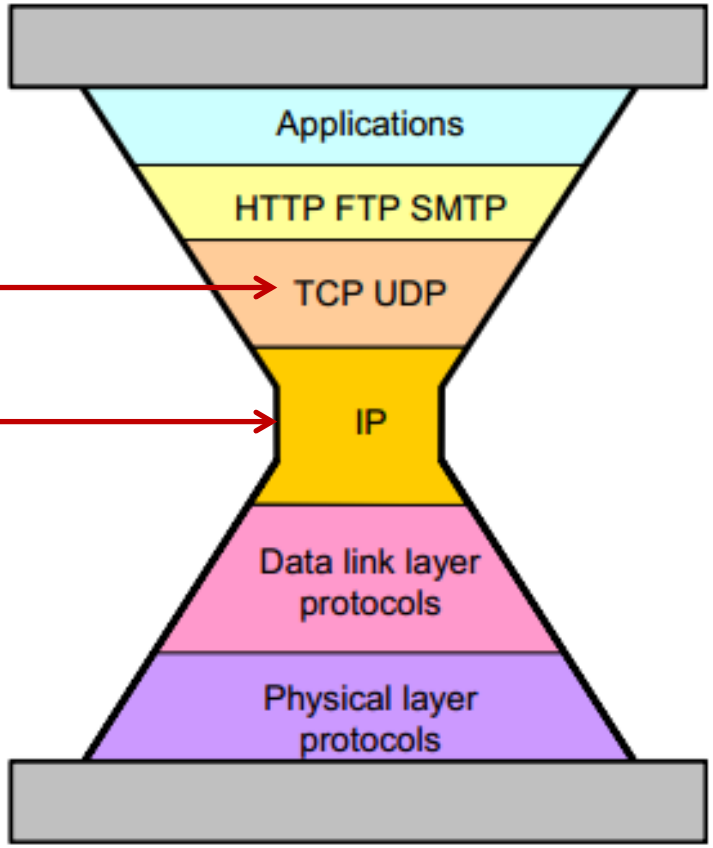
CONFIDENTIALITY
disclosure

What can Security Technologists learn from the History of the Internet?

Internet Protocols

TCP RFC 793
Sept. 1981

IPv4 RFC 791
Sept. 1981



The TCP/IP Lesson

- Agility trumps perfection

Not quite the same as

- Good enough trumps perfect

Agility =
Good enough for now
+
Future-proof for uncertain future

IP Spoofing Story

ALLOW GOOD GUYS IN
KEEP BAD GUYS OUT

- IP Spoofing predicted in Bell Labs report ≈ 1985
- Unencrypted Telnet with passwords in clear
- 1st Generation firewalls deployed ≈ 1992
- IP Spoofing attacks proliferate in the wild ≈ 1993
- Virtual Private Networks emerge ≈ late 1990's
- Vulnerability shifts to the client PC
- Network Admission Control ≈ 2000's

- Persists as a Distributed Denial of Service mechanism
- Most of these fixes have not changed or extended IPv4

Laws and Principles of Cyber Security

Laws of Attackers

1. Attackers exist
   - ❖ You will be attacked
2. Attackers have sharply escalating incentive
   - ❖ Money, terrorism, war, espionage, sabotage, …
3. Attackers are lazy (follow path of least resistance)
   - ❖ Attacks will escalate BUT no faster than necessary
4. Attackers are innovative (and stealthy)
   - ❖ Eventually all feasible attacks will manifest
5. Attackers are copycats
   - ❖ Known attacks will proliferate widely
6. Attackers have asymmetrical advantage
   - ❖ Need one point of failure

Principles of Defense

A. Prepare for tomorrow's attacks, not just yesterday's
   - ❖ Good defenders strive to stay ahead of the curve, bad defenders forever lag

B. Take care of tomorrow's attacks before next year's attacks
   - ❖ Researchers will and should pursue defense against attacks that will manifest far in the future BUT these solutions will deploy only as attacks catch up

C. Use future-proof barriers
   - ❖ Defenders need a roadmap and need to make adjustments

D. It's all about trade-offs
   - ❖ Security, Convenience, Cost

Beware of "silver bullets"