RMIT UNIVERSITY

Centre for Cyber Security Research and Innovation

RMIT Cyber Series

Professor Ravi Sandhu

Tuesday 30 March 2021

What's next...

Acknowledgement of Country

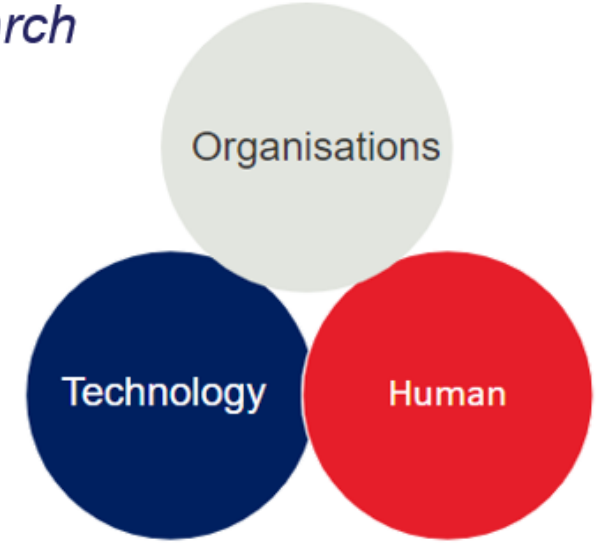
We acknowledge the people of the Woi wurrung and Boon wurrung language groups of the eastern Kulin Nation, on whose unceded lands we conduct the business of RMIT University, and the lands that I am speaking from today.

As we gather virtually across many different parts of the world, we also encourage you to acknowledge the lands in which you are joining us from.

We respectfully acknowledge the first nations people of the five Kulin Nations, their Ancestors and Elders, past, present and emerging.

RMIT Centre for Cyber Security Research and Innovation (CCSRI)

Carries out quality multi-disciplinary research relating to the organisational, human and technology aspects of Cyber Security;



Develops and promotes understanding of strategies, policies, and law issues of the Cyber Security challenges for Australia;

Contributes to the Cyber Security Innovation eco-system within Australia and globally;

Actively engages with industry and government within Australia and globally.

RMIT UNIVERSITY
Centre for Cyber Security Research and Innovation

RMIT Cyber Series:

Professor Ravi Sandhu

University of Texas, San Antonio

I·C·S
The Institute for Cyber Security

C·SPECC
Center for Security and Privacy Enhanced Cloud Computing

What Technologists Should Learn from the History of Cyber Security

Ravi Sandhu

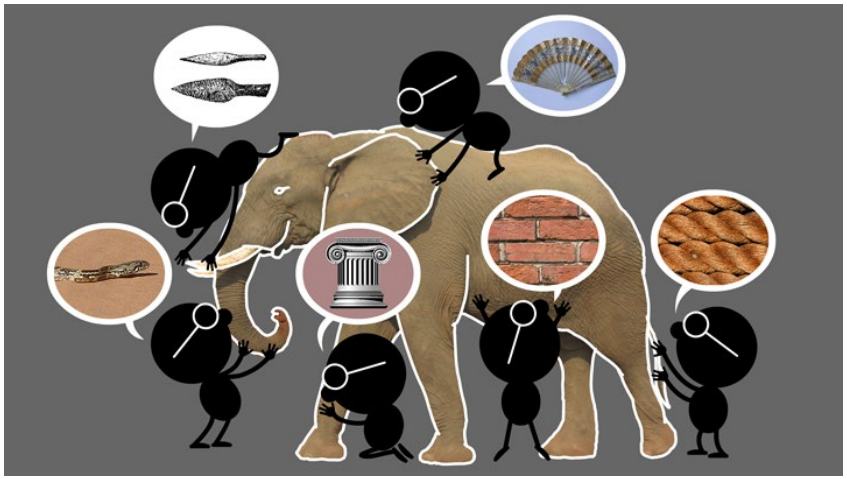
Professor of Computer Science
Lutcher Brown Chair in Cyber Security
Executive Director, Institute for Cyber Security

RMIT University Centre for Cyber Security Research and Innovation
Seminar Series
March 29, 2021

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

Natural vs Cyber Science

Elephant Problem

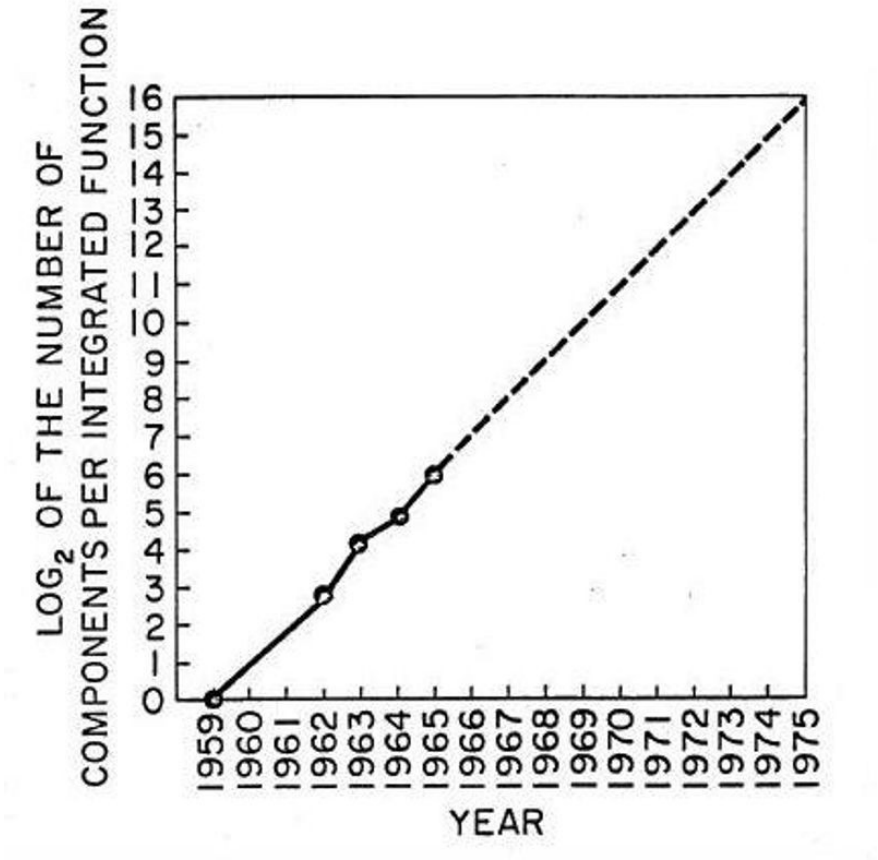


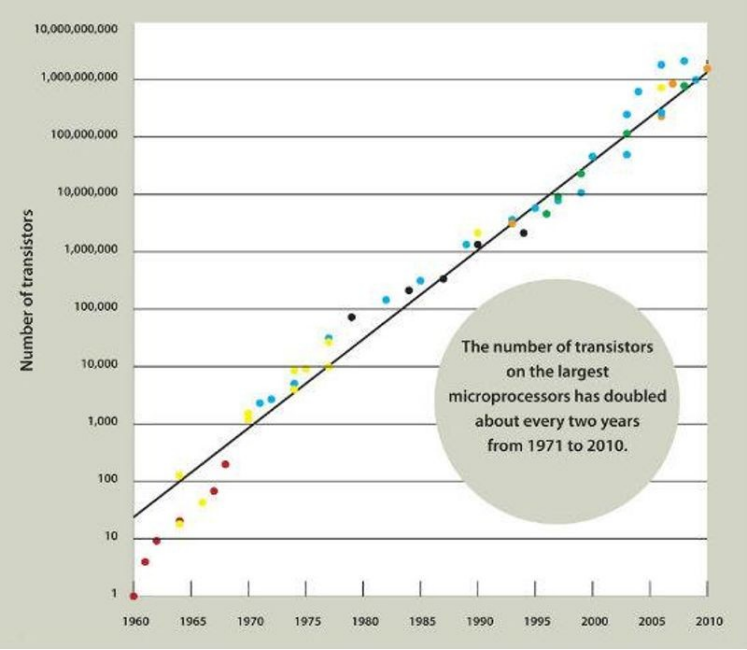
<u>Applied vs Foundational Science</u>: Cyber-elephants require applied and foundational combined

<u>Present vs Future Focus</u>: Rapidly evolving cyber-elephants require future focus

Cyber-Elephant Problem

Moore's Law & Future Focus





History Rhymes

History doesn't repeat itself but it often rhymes. - Mark Twain

#SayQuotable

Cyber Security Success is Possible

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

Consumer Grade Assurance

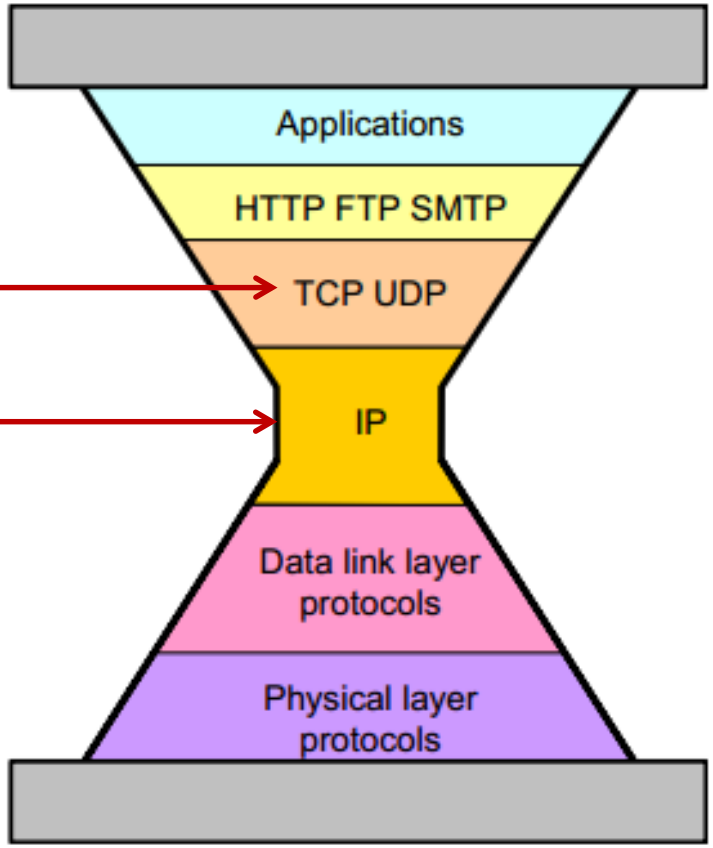
- US President's nuclear football

Military Grade Assurance

Internet Protocols

TCP RFC 793
Sept. 1981

IPv4 RFC 791
Sept. 1981



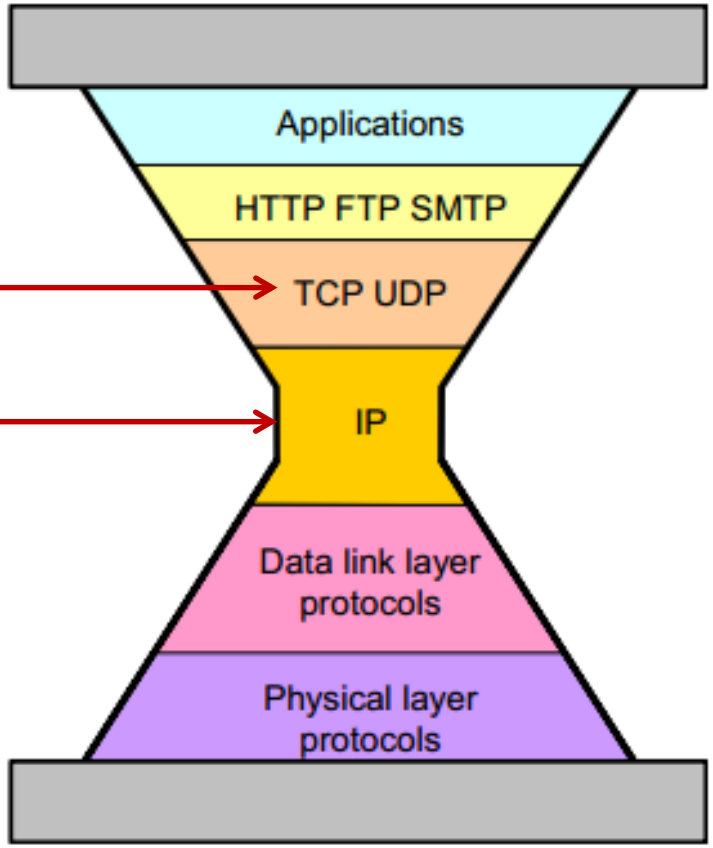
IP Spoofing Story

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

World Wide Web Protocols



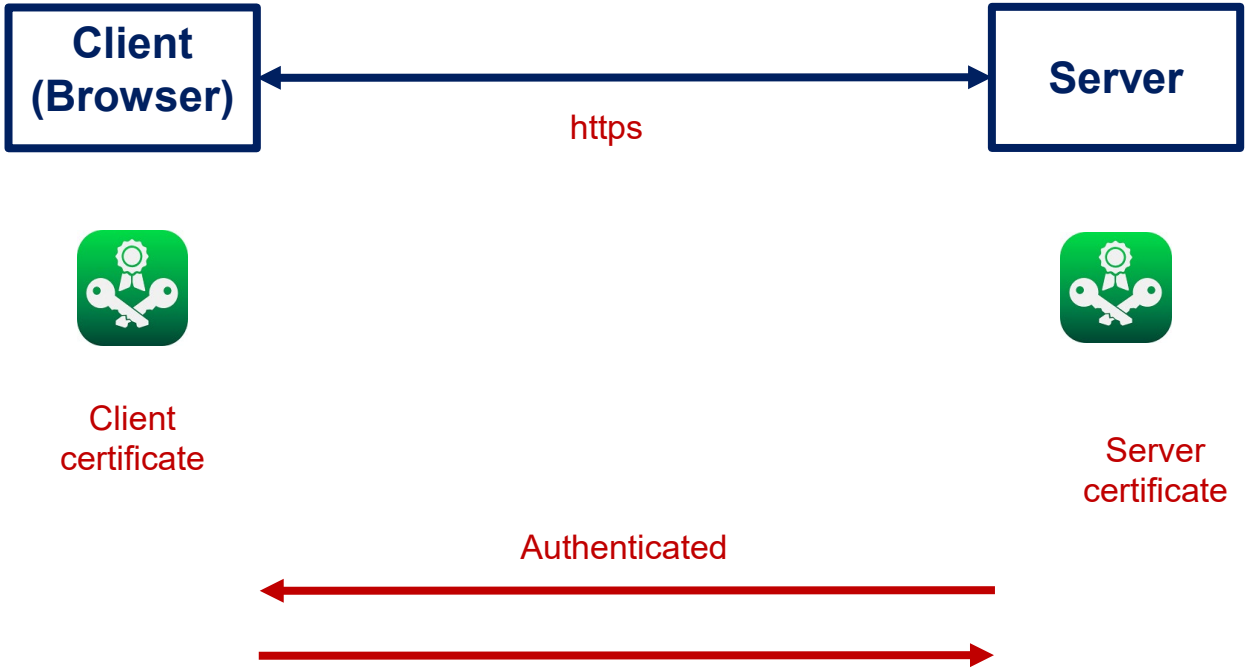
TCP RFC 793
Sept. 1981

IPv4 RFC 791
Sept. 1981

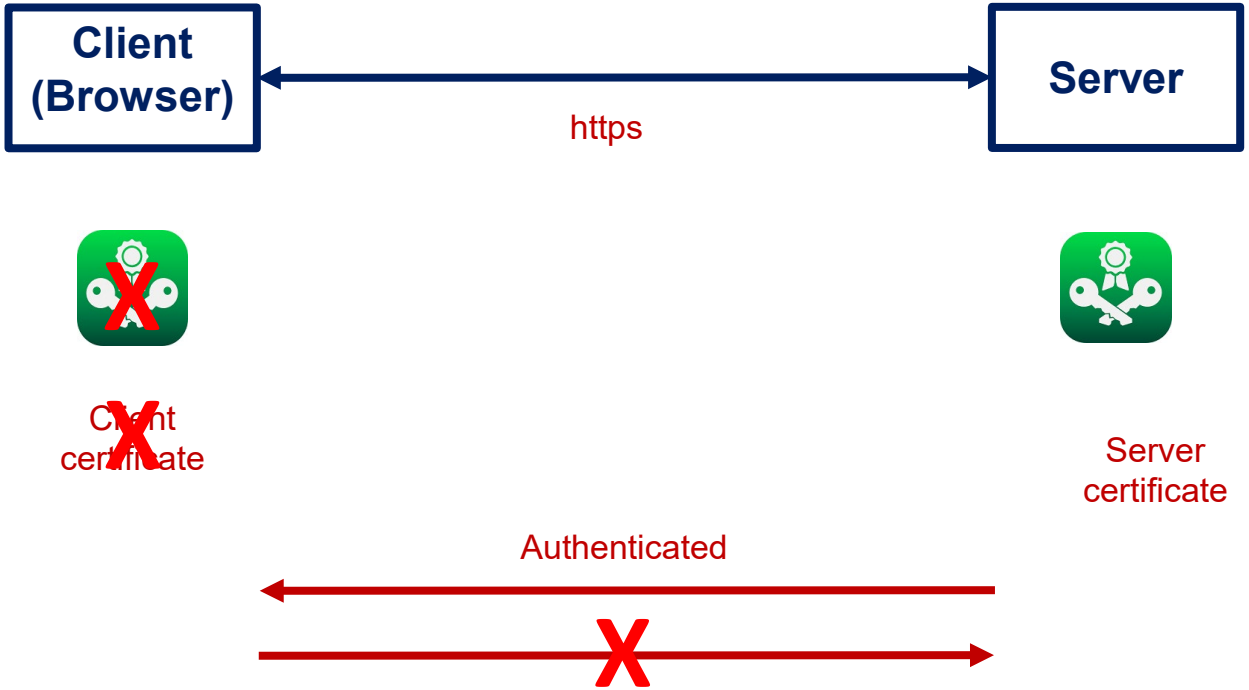
http versions
1989 onwards

https
http over SSL
1994 onwards

SSL: 2-Way

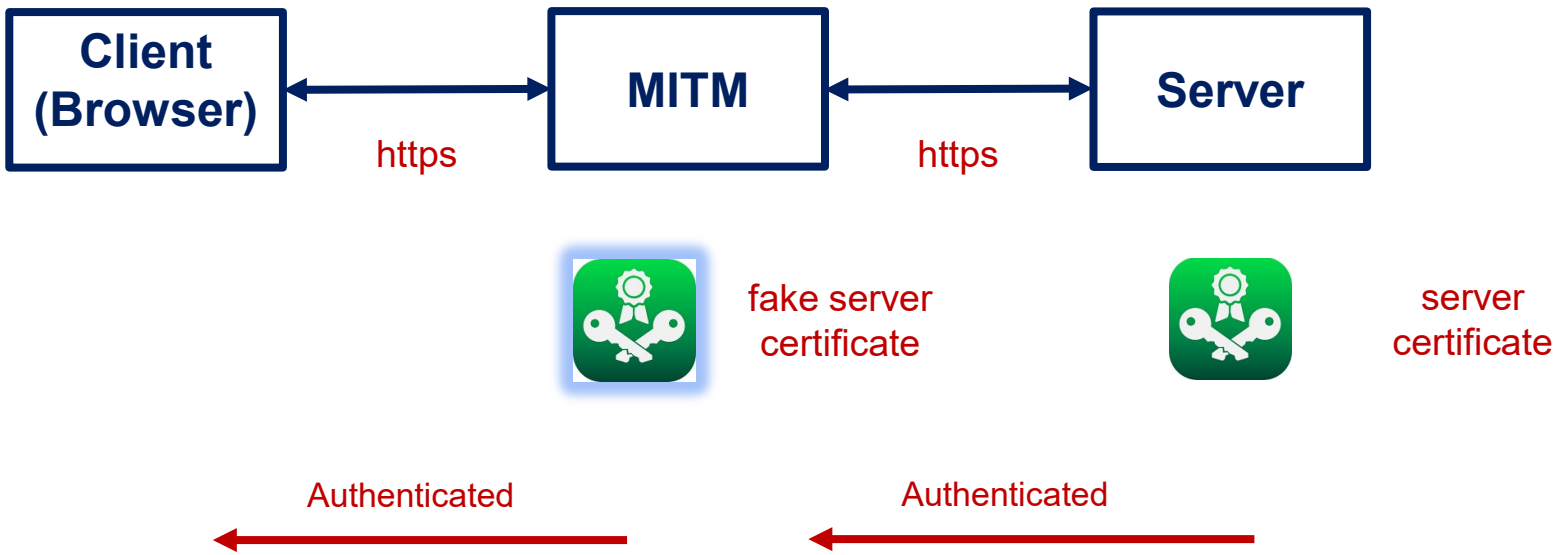


SSL: 1-Way



SSL: 1-Way Man-in-the-Middle (MITM)

Known since at least 1998



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"

Q & A

Professor Ravi Sandhu
University of Texas, San Antonio

Thank you for joining us today!

RMIT UNIVERSITY

Centre for Cyber Security Research and Innovation