Module 1.5
Security Practice Stories and Lessons

Ravi Sandhu

Spring 2021

Low Assurance Systems

- The ATM (Automatic Teller Machine) system is
  - secure enough
  - global in scope
- Similarly
  - on-line banking
  - e-commerce payments

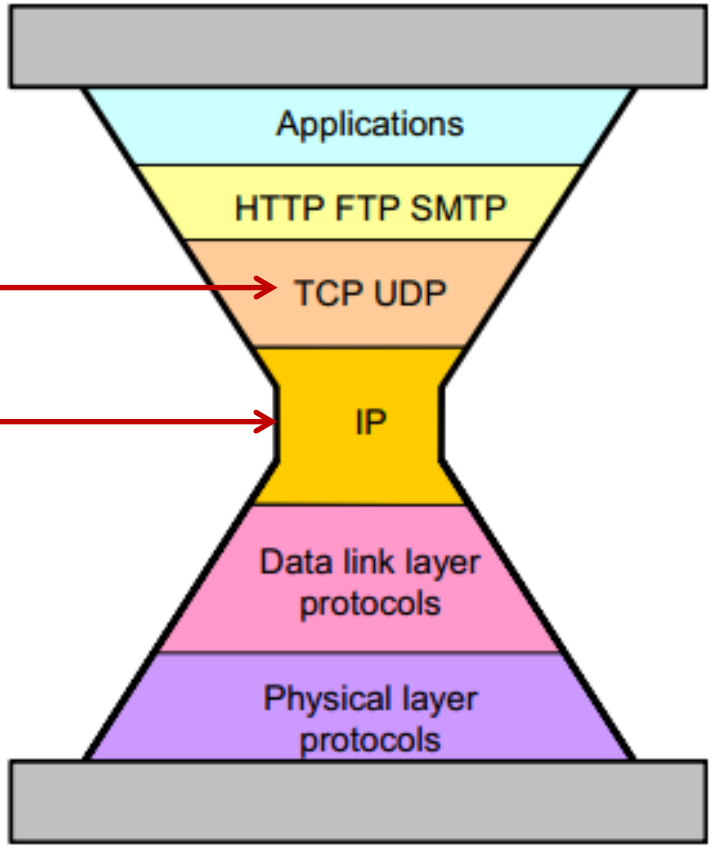
High Assurance Systems

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

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

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

Laws of Attackers

1. Attackers exist
   - ❖ You will be attacked
2. Attackers have sharply escalating incentive
   - ❖ Money, terrorism, war, espionage, sabotage, …
3. Attackers have an infinite supply
   - ❖ No limit to attacks
4. Attackers are lazy (follow path of least resistance)
   - ❖ Attacks will escalate BUT no faster than necessary
5. Attackers are innovative (and stealthy)
   - ❖ Eventually all feasible attacks will manifest
6. Attackers are copycats
   - ❖ Known attacks will be automated and proliferate
7. 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"