# Networks 2: Security basics

Robert H. Sloan

# Recall 4-layer TCP/IP model

1.Physical/Link layer

**2.Network/Internetwork layer** (IP)

3.**Transport layer** (TCP, ICMP, UDP)

4.**Application layer** (DNS, POP, SSL, etc.)

# Why are networks vulnerable?

- Anonymity—attackers far away
- Many points of attack—both targets and origins
- Complexity of system
- Unknown perimeter—hosts come and go
- Unknown path—packet routing

# TCP connection establishment

- TCP packet headers have various binary flags, including SYN (synchronize) and ACK
- Connection established via 3-way handshake:

1. Requesting host sends SYN packet
2. Accepting host send SYN/ACK packet
3. Requesting host sends ACK packet

# Security implications

- That 3-way handshake occurs at Transport layer *before any* application gets access to the packet

- Hence handshake attacks *cannot* be fixed at the application layer.

# Top layer: Application Layer

- Where the protocol for the application lives
  - E.g., DNS, FTP, HTTP, IMAP and POP, SMTP, SSH, SSL
- Also where formatting values, compression, and cryptography live.

# Application layer protocols (1)

- Application protocols need to check security, but many, especially old ones, do so poorly.

- Telnet and ftp send passwords in the clear; rsh allows users to accept connections without password verification

  - Hence ssh for remote connections; sftp for file transfer, but ftp is still really common. (Telnet & rsh obsolete?)

# TLS

- **Transport Layer Security (TSL)** is standard application layer implementation of cryptography. (Formerly known as SSL; SSL 3.0 = TLS 1.0 still in wide use.)

- Most common use is to secure comm between web browser and web server; in this context HTTP over TSL (was SSL); hence https://

# TSL continued

- TSL contains:
  - Certificates (Only server, one sided)
    - Asymmetric encryption
  - Symmetric encryption
- Session oriented

# Application layer security bad; lower good!

- SSL/TLS, etc. must be explicitly invoked and managed by the app
  - Don't know if app did this right
  - Too high: E.g., discover TCP packet to be bogus at application layer, because it's a bad duplicate, and lower transport layer (where TCP lives) will discard good one when it finally arrives as a duplicate!

# Internet future: IPSec?

- Recall that Internet is running out of addresses; will be moving from IPv4 32-bit addresses to new IPv6.

- Things are/will get better at network layer: IPSec the Internet Protocol Security standard, is in limited use now; will be universal. (Optional in IPv4, now growing common, but required in IPv6.)

- Provides more secure network layer: encryption of packet body; authentication of packet header.

- Will it be used?

# Summary

- Packet-switched network traffic can be seen, modified, or removed by attackers
- Connections can originate from anywhere in the world.
- IP source and destination addresses are world readable
- Many protocols at all levels are not security minded