5. Network Security Basics

ENEE 657

Prof. Tudor Dumitraș
Assistant Professor, ECE
University of Maryland, College Park

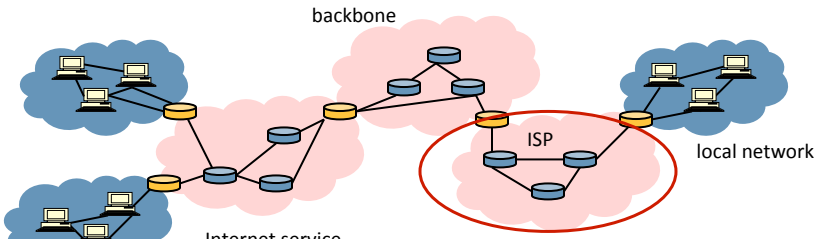
http://ter.ps/enee657

Today's Lecture

- Where we've been
  - Crypto basics
  - OS security basics
- Where we're going today
  - Network security
  - TCP/IP, BGP
  - Intrusion detection
- Where we're going next
  - Presenting security concepts (lab)

2

Internet Is a Network of Networks

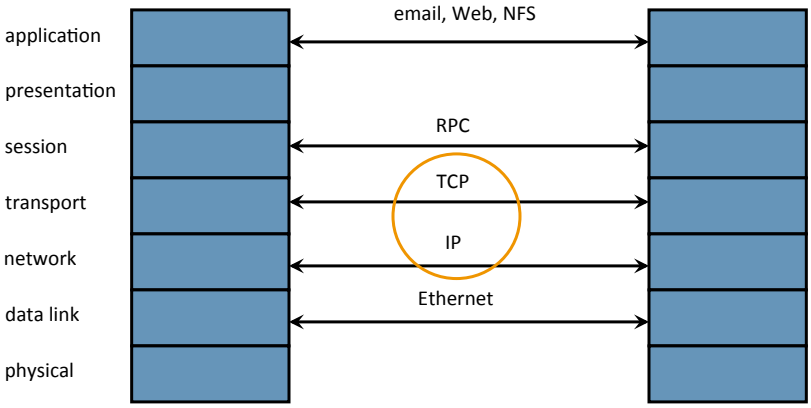


Autonomous system (AS) is a collection of IP networks under control of a single administrator (e.g., ISP)

- TCP/IP for **packet routing** and **connections**
- Border Gateway Protocol (BGP) for route discovery
- Domain Name System (DNS) for IP address discovery

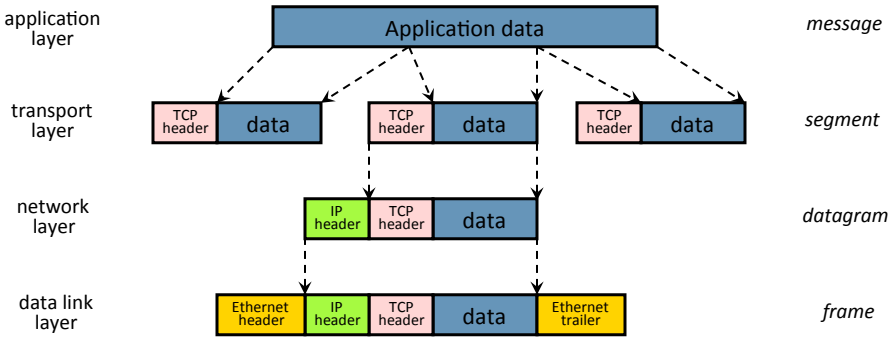
3

OSI Protocol Stack



4

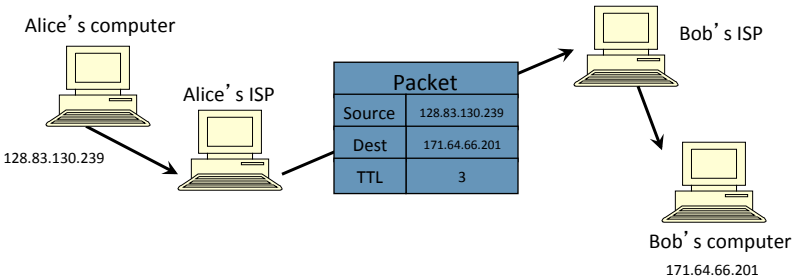
Data Formats



5

IP (Internet Protocol)

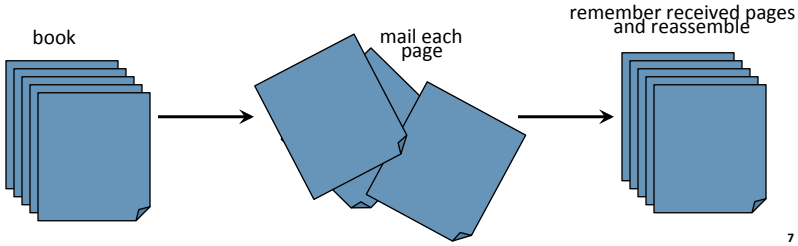
- Connectionless
  - Unreliable, "best-effort" protocol
- Uses numeric addresses for routing
- Typically several hops in the route



6

TCP (Transmission Control Protocol)

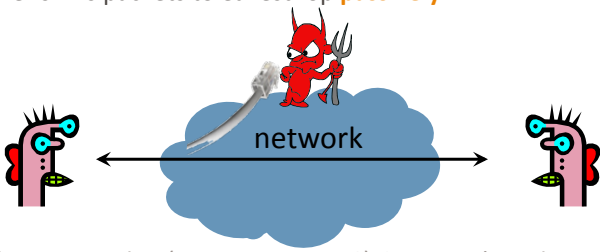
- Sender: break data into packets
  - Sequence number is attached to every packet
- Receiver: reassemble packets in correct order
  - Acknowledge receipt; lost packets are re-sent
- Connection state maintained on both sides



7

Threat #1: Eavesdropping on Network Connections

- Goal: extract information from network packets
- Many applications send data unencrypted
  - ftp, telnet send **passwords in the clear**
- Network interface card (NIC) in "promiscuous mode" reads all passing data
  - Attacker sniffs packets to eavesdrop **passively**



Solution: encryption (e.g., IPsec, HTTPS), improved routing

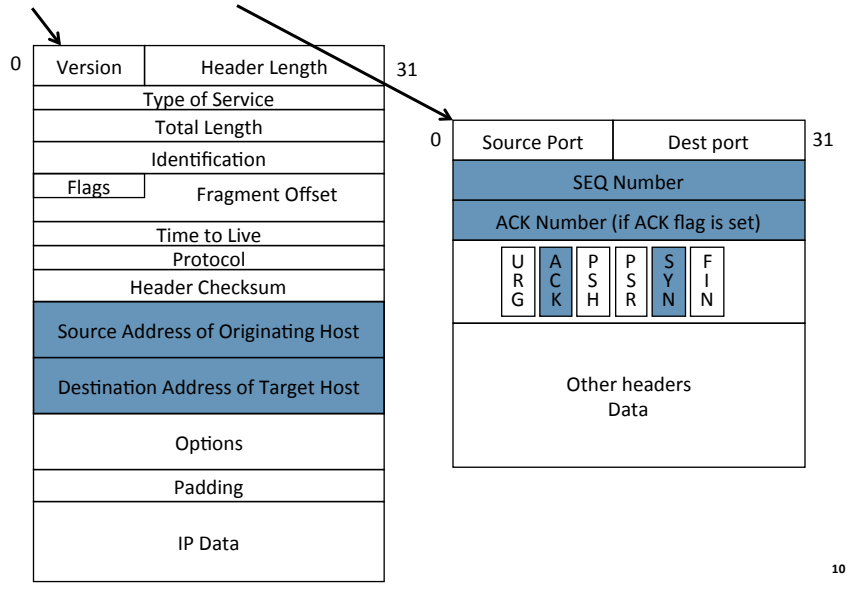
8

Threat #2: Denial of Service (DoS)

- Goal: take out a large site with little computing work
- DoS can happen at any layer
  - Link
  - TCP/UDP
  - Application
- DoS solutions for one layer cannot always be replicated at other layers
  - This means that DoS cannot be solved with end-to-end solutions
  - Need cooperation from the network

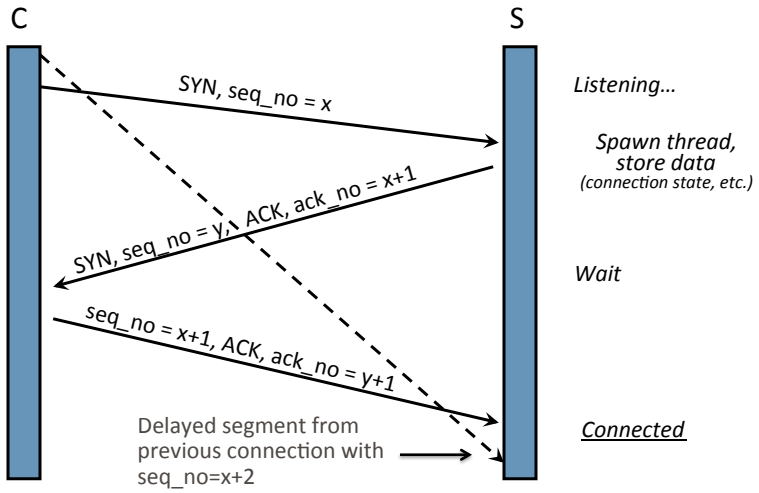
9

IP and TCP Headers



10

TCP Handshake



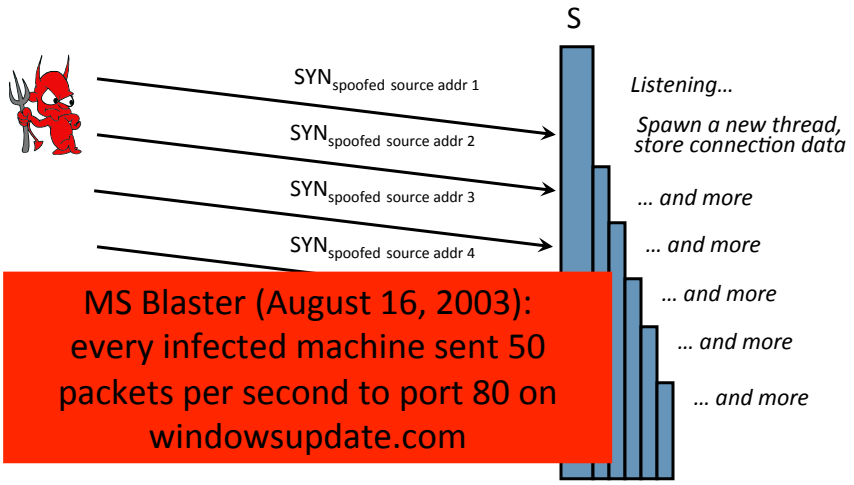
Recommendation: Increment the initial sequence number every 4 ms (**why**?) [11]

TCP Flow Control

- TCP uses a sliding window mechanism
- Receiver advertises a window of size W
- Sender can send up W unacknowledged bytes
  - Can be split among multiple segments, if data is not yet available
- Receiver can delay sending ACKs until it has data to transmit
  - ACKs will be piggybacked on the data packets
  - ACK will correspond to the next byte it expects to receive => this may acknowledge multiple packets received previously

[12]

DoS Attack #1: TCP SYN Flood



MS Blaster (August 16, 2003): every infected machine sent 50 packets per second to port 80 on windowsupdate.com

13

SYN Flooding Explained

- Attacker sends many connection requests with spoofed source addresses
- Victim allocates resources for each request
  - New thread, connection state maintained until timeout
  - Fixed bound on half-open connections (backlog)
- Once resources exhausted, requests from legitimate clients are denied
- This is a classic denial of service pattern
  - It costs nothing to TCP initiator to send a connection request, but TCP responder must spawn a thread for each request - **asymmetry**!

14

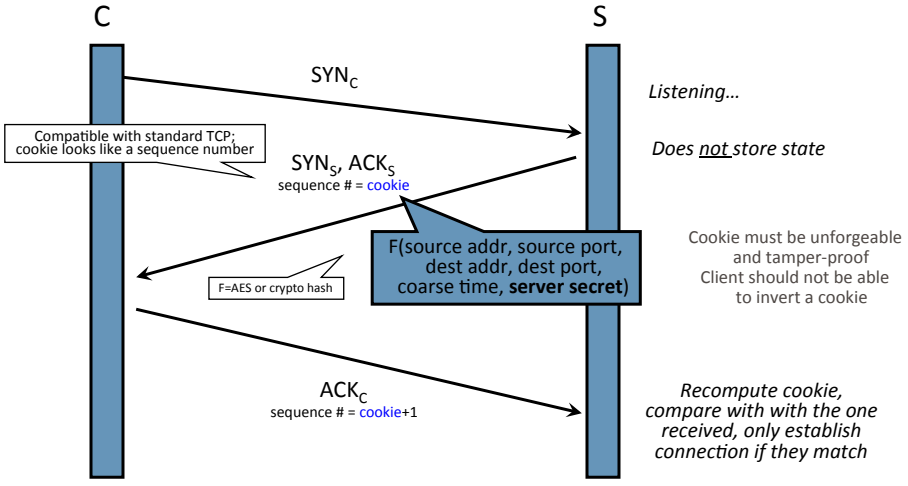
Preventing Denial of Service

- DoS is caused by asymmetric state allocation
  - If responder opens new state for each connection attempt, attacker can initiate thousands of connections from bogus or forged IP addresses
- **Cookies** ensure that the responder is stateless until initiator produced at least two messages
  - Responder's state (IP addresses and ports of the connection) is stored in a cookie and sent to initiator
  - After initiator responds, cookie is regenerated and compared with the cookie returned by the initiator

15

SYN Flooding Defense: SYN Cookies

[Bernstein and Schenk]



More info: http://cr.yp.to/syncookies.html

16

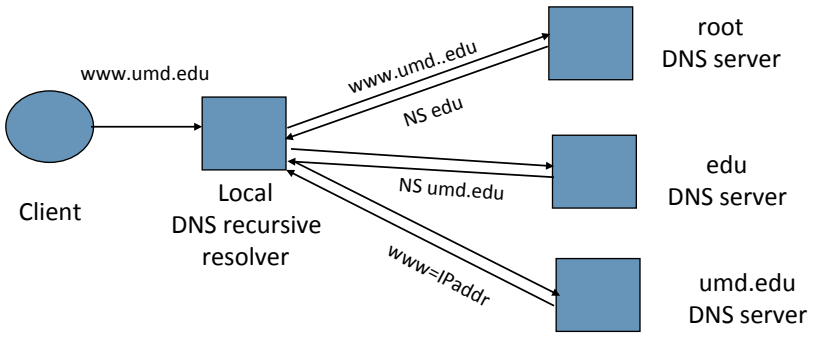
Anti-Spoofing Cookies: Basic Pattern

- Client sends request (message #1) to server
- Typical protocol:
  - Server sets up connection, responds with message #2
  - Client may complete session or not - potential DoS!
- Cookie version:
  - Server responds with hashed connection data in message #2
  - Client confirms by returning hashed data
    - If source IP address is bogus, attacker can't confirm
  - Need an extra step to send postponed message #2, except in TCP (can piggyback on SYN-ACK in TCP)

17

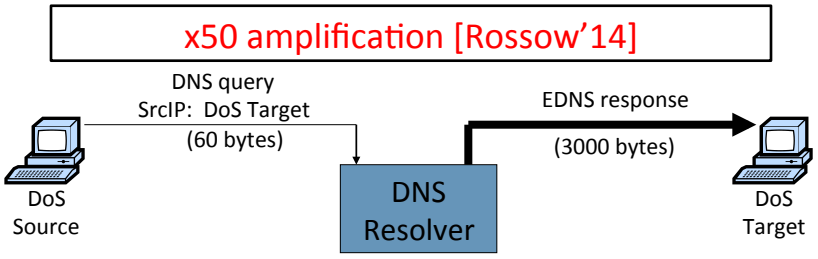
Domain Name Service (DNS)

DNS maps symbolic names to numeric IP addresses
(for example, www.umd.edu ↔ 54.83.56.209)



18

DoS Attack #2: DNS Amplification Attack



- DNS runs over UDP (rather than TCP) => can spoof source IP
- **Open DNS resolvers**: answer queries from any host
  - 2006: 0.58M open resolvers on Internet (Kaminsky-Shiffman)
  - 2013: **28M** open resolvers (openresolverproject.org)
- March 2013: **300 Gbps DDoS** attack on Spamhaus
- There are other protocols that amplify traffic (more on this later)

19

Other DNS Vulnerabilities

- DNS servers can be DDoS'ed
  - Oct '02: ICMP flood took out 9 root servers for 1 hour
- Kaminski attack: poison DNS caches
  - Attacker guesses transaction ID used to match queries with replies
  - Solution: randomize ports and transaction IDs
- DNS implementations have vulnerabilities
  - Reverse query buffer overrun in old releases of BIND
  - MS DNS for NT 4.0 crashes on chargen stream
- Can use "zone transfer" requests to download DNS database and map out the network
  - Solution: block port 53 on corporate name servers

See http://cr.yp.to/djbdns/notes.html

20

Threat #3: Impersonate Other Hosts

- Goal 1: Defeat authentication that relies on IP-source address
  - Must spoof the source address
- Goal 2: Draw packets destined to other hosts
  - Allows conducting man-in-the-middle attacks (more on this later)
  - Must target the destination address

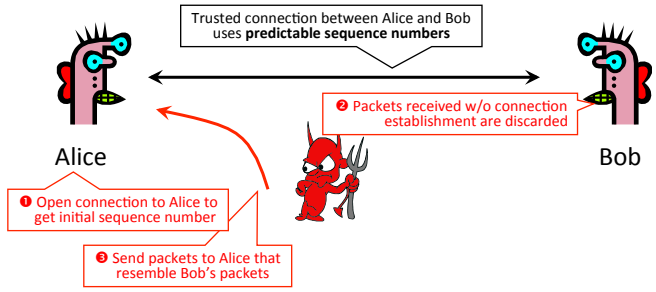
21

TCP Connection Spoofing

- Each TCP connection has associated state
  - Sequence number, port number
- TCP state is easy to guess
  - Port numbers standard, seq numbers predictable
- Can inject packets into existing connections
  - If attacker knows initial sequence number and amount of traffic, can guess likely current number
  - **How do you guess a 32-bit sequence number?**

22

"Blind" IP Spoofing Attack



- Can't receive packets sent to Bob, but can bypass Alice's IP address-based authentication
  - rlogin and other remote access tools, SPF defense against spam

23

Intrusion Detection Systems (IDS)

- Hard to prevent all network attacks; can we detect them?
  - Host-based / Network-based intrusion detection system (HIDS/NIDS)
- **Misuse** detection
  - Use attack "signatures" (need a model of the attack)
    - Sequences of system calls, patterns of network traffic, etc.
  - Must know in advance what attacker will do
  - Can only detect **known attacks**
- **Anomaly** detection
  - Using a model of normal system behavior, try to detect deviations and abnormalities
    - E.g., raise an alarm when a statistically rare event(s) occurs
  - Can **potentially** detect unknown attacks

Intrusion Detection Errors

- False negatives: attack is not detected
  - Big problem in signature-based misuse detection
- False positives: harmless behavior is classified as an attack
  - Big problem in statistical anomaly detection
- All intrusion detection systems (IDS) suffer from errors of both types
- Which is a bigger problem?
  - Attacks are fairly rare events
  - Thus IDS often suffer from the base-rate fallacy

Conditional Probability

- Suppose two events A and B occur with probability Pr(A) and Pr(B), respectively
- Let Pr(AB) be probability that both A and B occur
- What is the conditional probability that A occurs assuming B has occurred?

$$Pr(A \mid B) = \frac{Pr(AB)}{Pr(B)}$$

Bayes's Theorem

- Suppose we have two events, A and B
- Then the probability of both events occurring is

$$Pr(A|B) \bullet Pr(B) = Pr(AB) = Pr(B|A) \bullet Pr(A)$$

- Can rewrite this formula as

$$Pr(B \mid A) = \frac{Pr(A \mid B) \bullet Pr(B)}{Pr(A)}$$

Base-Rate Fallacy

- 1% of traffic is SYN floods; IDS accuracy is 90%
  - IDS classifies a SYN flood as attack with prob. 90%, classifies a valid connection as attack with prob. 10%
- What is the probability that a connection flagged by IDS as a SYN flood is actually valid?

$$Pr(valid \mid alarm) = \frac{Pr(alarm \mid valid) \bullet Pr(valid)}{Pr(alarm)}$$

$$= \frac{Pr(alarm \mid valid) \bullet Pr(valid)}{Pr(alarm \mid valid) \bullet Pr(valid) + Pr(alarm \mid SYN\ flood) \bullet Pr(SYN\ flood)}$$

$$= \frac{0.10 \bullet 0.99}{0.10 \bullet 0.99 + 0.90 \bullet 0.01}$$

= 92% chance raised alarm is false!!!

Review of Lecture

- What did we learn?
  - IP spoofing
  - TCP handshake and flow control
  - TCP cookies
  - Various eavesdropping and denial-of-service attacks
  - Base rate fallacy
- Sources
  - Vitaly Shmatikov
- What's next?
  - Presenting security topics

29