



# Network II

## CS 184

IP and TCP Protocol Security

Department of Computer Science  
George Washington University

# Relevant Reading

- Relevant reading:
  - Security Problems in the TCP/IP Protocol Suite by Steve Bellovin. Computer Communications Review, Vol 19, No. 2, pp 22-48, April 1989.
  - Sequence Integrity using Hash Chains by Matt Barrie. <http://www.ee.usyd.edu.au/~mattb/2001/lectures/attacks.pdf>
  - Bugtraq Mailing list <http://online.securityfocus.com/popups/forums/bugtraq/faq.shtml>
  - Vulnerability Database <http://online.securityfocus.com/bid>
  - Crypto-Gram Newsletter <http://www.counterpane.com/crypto-gram.html>
  - CERT Statistics [http://www.cert.org/stats/cert\\_stats.html](http://www.cert.org/stats/cert_stats.html)

# What are Network Security Risks?

- Information disclosure:
  - IP addresses and DNS names of machines, active ports, network topology.
- Connection Capture (Man-in-the-middle)
  - TCP connection capture.
  - Modified DNS replies.
- DOS
  - Network traffic DOS
    - Ping, SYN-flood, ...

# In the News!

- HTTP TRACE Cross Site Scripting flaw -- Standard, but almost unknown part of HTTP protocol allows cookie stealing and impersonation attacks!
- Microsoft MSSQL remote buffer overflow takes down Internet! (Bank of America ATMs, XP Activation servers, ...)
- Sprint DSL modems have a remotely accessible admin user with the password 1234! (Spaceballs reference anyone?)
- Wireless router being used to steal money from an Israeli Post Office (bank).

# Security Bug Classification

- Network Security Bugs or Flaws can be divided into five classes:
  - Algorithm (DES is flawed)
  - Protocol (SSH or TCP is flawed)
  - Environmental (NFS on Secure LAN vs. insecure LAN)
  - Implementation (OpenSSH v3.1, or FreeBSD 3.4 is flawed)
  - Conceptual (Telnet sends passwords in the clear)
- We will rarely discuss the first class (that's crypto 101).
- The focus is on understanding and noticing the latter four.

# Protocol Flaws

- TCP Sequence number generation and increment.
- Routing:
  - Source Routing -- Universally disabled because of high security risk and low value.
  - RIP and other older routing protocols: generally lack any authentication or only provide source IP address authentication.
- ICMP
  - mostly DOS or network mapping attacks.
- DNS
  - Queries only protected by simple sequence number.
  - Cache poisoning possible.
- Ethernet ARP (Address Resolution Protocol)
  - ARP spoofing is easy -- requests are broadcast.
  - ARP storms are possible -- convince other nodes that the way to reach an IP address is through the broadcast ethernet address...

# TCP Connection Initialization

- Basic Algorithm:
  - C -> S: SYN(ISN<sub>c</sub>)
  - S -> C: SYN(ISN<sub>s</sub>), ACK(ISN<sub>c</sub>)
  - C -> S: ACK(ISN<sub>s</sub>)
  - C -> S: data or
  - S -> C: data
- What is security critical about this?
  - Can ISNs be guessed?
  - Can packets be intercepted?

# Basic TCP Seq Attack

- Assuming attacker X can guess ISNs, target is T.
  - X -> S: SYN(ISN<sub>x</sub>), SRC=T
  - S -> T: SYN(ISN<sub>s</sub>), ACK(ISN<sub>x</sub>)
  - X -> S: ACK(ISN<sub>s</sub>), SRC=T
  - X -> S: ACK(ISN<sub>s</sub>), SRC=T, bad data.
- Does T notice the attack?
  - Yes, it will receive S -> T and notice that a bad connection is being formed and will initiate a RST (reset) of the connection. So to succeed the attack must use a currently disconnected T, must block T from sending the packet, or must intercept the packet.
- Does S notice the attack?
  - No. Everything looks normal as long as ACK(ISN<sub>s</sub>) is correct.

# Can you know ISNs?

- Some old IP stacks incremented ISNs too slowly, so it was easy to calculate.
- Even if incremented quickly (RFC requires 250,000 times per second), still possible.
  - Send a ‘valid’ connection request to S, see what ISNs is. Then send attack packet with a larger ISNs based on RTT between X and S and a guess at processing delays. If you have stable RTT latency, after only a few thousand tries you will likely hit one that works. (Note: Attack gets easier as machines and networks get faster...)
- Increment by “random” amount for each connection.
  - Requires cryptographic operations and a ‘secure’ key (time of day at boot is not sufficient)

# Sequence numbers Part 2

- Even with good Initial Sequence Numbers, the sequence numbers on each data packet also matter.
- Normally, TCP increments the sequence number with each byte of data.
- TCP accepts a packet if it's SN is between  $SN_b \dots SN_b + WINDOW$ .
- Otherwise it is rejected. So SN form a type of authentication.

# TCP Session Hijacking

- Attack is a form of connection desynchronization.
- Steps:
  - Attacker (X) listens to connection between A and B.
  - At certain time, attacker adds new packets to A and B so that they will now think the current sequence number is different from what the other one thinks.
  - X listens to both A and B's packets, modifies them if desired, and resends them on with 'corrected' sequence numbers.
- Also results in ACK storm caused by each host sending ACKs for "missing" packets caused by desynchronized sequence numbers.

# TCP Hijacking "Early" attack

- Specific attacks:
  - “Early” RST packet after 2nd step of TCP establishment.
    - A -> B: SYN(ISN<sub>a</sub>)
    - B -> A: ACK(ISN<sub>a</sub> + 1), SYN(ISN<sub>b</sub>)
    - X<sub>a</sub> -> B: ACK(ISN<sub>b</sub> + 1), RST ; b now thinks a's disconnected
    - X<sub>a</sub> -> B: SYN(ISN<sub>x<sub>a</sub></sub>) ; new connection between “a” and b
    - B -> A: ACK(ISN<sub>x<sub>a</sub></sub> + 1), SYN(ISN'<sub>b</sub>) ; A ignores
    - X<sub>a</sub> -> B: ACK(ISN'<sub>b</sub> + 1) ; now X<sub>a</sub> is in the middle

# TCP Hijacking "Null" attack

- A -> B : ACK(SNb)
- B -> A : ACK(SNa)
- Xa -> B : ACK(SNb + 1) ; null one byte data
- ...
- Xa -> B : ACK(SNb + n) ; null one byte data
- Total is n bytes data that B received thinking it was from A but it was really from X. So B's sequence number is now n larger than A thinks it should be.

# Denial of Service Attacks

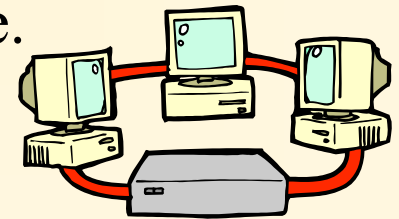
- SYN flooding
  - The attacker sends the initial SYN packet of a TCP connection, but never completes it. It just keeps initiating more TCP connections. Target's memory/kernel resources have to track all of the potential connections and get overwhelmed.
  - Solved in some OS's by SYNcookies. The target now does not store anything about SYN initial connections, but sends the necessary info in a 'cookie' to the initiator who will then return it.
  - Attacks one machine at a time. Magnification is because of asymmetric state maintenance.

# Denial of Service Attacks

- Smurf attacks (ICMP Ping)
  - The attacker sends ICMP ping packets with spoofed source addresses to the **broadcast** address of a subnet. Every machine in the subnet sends a ICMP response packet to the “target” source machine. If sufficient pings are sent by the attacker to a number of broadcast networks, the target gets flooded with ping response packets.
  - Magnification occurs because for each attack packet, N damage packets are sent to target. Occurs because the ping source address is trusted and “broadcast” pings are routed. Gradually being fixed by changing the RFC’s to prohibit routing “broadcast” pings. They can now only be used locally.

# Ethereal -- Network Analysis

- Ethereal is a network protocol analyzer and debugging tool. It is based on the widely used tcpdump and libpcap tools, and supports most unix varieties and MS Windows.
- Steps:
  1. Capture network packets
  2. Examine stream of packets and details about particular packets.
  3. Use sequence visualization, stream reconstruction, etc to assist understanding the network behavior.
  4. Store capture and notes for future reference.



# Information Slide

- Ethereum can be downloaded from [www.ethereal.com](http://www.ethereal.com). Versions for Windows and Unix are available.
- Remember HW1 is due on Friday Jan 16th at 4pm by email to [jstanton@gwu.edu](mailto:jstanton@gwu.edu).
- Lecture slides, exercises, and papers to read can be obtained at the course web page <http://www.seas.gwu.edu/~jonathan/courses/cs184/>