Computer Systems Security

Computer Systems Security

Network Security

- Sub topics
  - Network Device Security
  - Common Security attacks and counter measures
    - Denial of Service attacks
    - TCP Attacks
    - Packet sniffing
    - Social problems
  - Firewalls
  - VPN Security
  - Wireless Network Security

Network Security - Introduction

- Computer networks are typically a shared resource used by many applications representing different interests.
- The Internet is particularly widely shared:
  - competing businesses,
  - mutually antagonistic governments, and
  - opportunistic criminals.
- Unless security measures are taken, a network conversation or a distributed application may be compromised by an adversary.

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Pharmaceutical companies
- Government and defense agencies
- Contractors to various government agencies
- Multinational corporations
- **ANYONE ON THE NETWORK**

Common security attacks and their countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

Dictionary Attack

- We can run a dictionary attack on the passwords
  - The passwords in /etc/passwd are encrypted with the crypt(3) function (one-way hash)
  - Can take a dictionary of words, crypt() them all, and compare with the hashed passwords
- This is why your passwords should be meaningless random junk!
  - For example, “sdfo839f” is a good password
    - That is not my andrew password
    - Please don’t try it either

Denial of Service

- Purpose: Make a network service unusable, usually by overloading the server or network
- Many different kinds of DoS attacks
  - SYN flooding
  - SMURF
  - Distributed attacks

Denial of Service

- SYN flooding attack
- Send SYN packets with bogus source address
  - Why?
- Server responds with SYN ACK and keeps state about TCP half-open connection
  - Eventually, server memory is exhausted with this state
- Solution: use “SYN cookies”
  - In response to a SYN, create a special “cookie” for the connection, and forget everything else
  - Then, can recreate the forgotten information when the ACK comes in from a legitimate connection

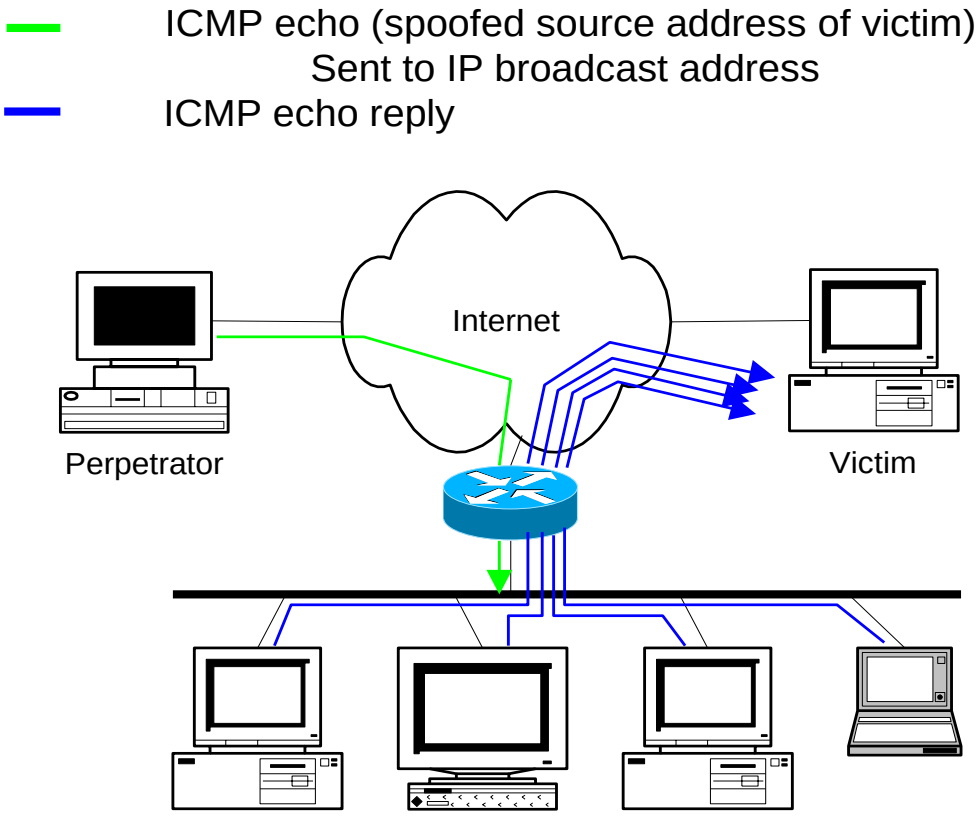
- A SYN (seq x) ======➔ B
- {B: SYN (seq. y),Ack (x+1)}====➔ A
- A: Ack (y+1)===➔ B

Denial of Service

- SMURF
  - Source IP address of a broadcast ping is forged
  - Large number of machines respond back to victim, overloading it

Denial of Service

- Smurf attack



Denial of Service

- Distributed Denial of Service
  - Same techniques as regular DoS, but on a much larger scale
  - Example: Sub7Server Trojan and IRC bots
    - Infect a large number of machines with a “zombie” program
    - Zombie program logs into an IRC channel and awaits commands
    - Example:
      - Bot command: !p4 207.71.92.193
      - Result: runs ping.exe 207.71.92.193 -l 65500 -n 10000
      - Sends 10,000 64k packets to the host (655MB!)
    - Read more at: http://grc.com/dos/grcdos.htm

Denial of Service

- How can we protect ourselves?
  - Ingress filtering
    - If the source IP of a packet comes in on an interface which does not have a route to that packet, then drop it
    - RFC 2267 has more information about this
  - Stay on top of CERT advisories and the latest security patches
    - A fix for the IIS buffer overflow was released **sixteen days before** CodeRed had been deployed!

TCP Attacks

- Recall how IP works…
  - End hosts create IP packets and routers process them purely based on destination address alone
- Problem: End hosts may lie about other fields which do not affect delivery
  - Source address – host may trick destination into believing that the packet is from a trusted source
    - Especially applications which use IP addresses as a simple authentication method
    - Solution – use better authentication methods

TCP Attacks

- TCP connections have associated state
  - Starting sequence numbers, port numbers
- Problem – what if an attacker learns these values?
  - Port numbers are sometimes well known to begin with (ex. HTTP uses port 80)
  - Sequence numbers are sometimes chosen in very predictable ways

TCP Attacks

- If an attacker learns the associated TCP state for the connection, then the connection can be **hijacked**!
- Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source
  - Ex. Instead of downloading and running new program, you download a virus and execute it

Packet Sniffing

- Recall how Ethernet works …
- When someone wants to send a packet to some else …
- They put the bits on the wire with the destination MAC address …
- And remember that other hosts are listening on the wire to detect for collisions …
- It couldn’t get any easier to figure out what data is being transmitted over the network!

Packet Sniffing

- This works for wireless too!
- In fact, it works for any broadcast-based medium

Packet Sniffing

- What kinds of data can we get?
- Asked another way, what kind of information would be most useful to a malicious user?
- Answer: Anything in plain text
  - Passwords are the most popular

Packet Sniffing

- How can we protect ourselves?
- SSH, not Telnet
  - Many people still use Telnet and send their password in the clear (use PuTTY instead!)
  - Now that I have told you this, please do not exploit this information
  - Packet sniffing is, by the way, prohibited by Computing Services
- HTTP over SSL
  - Especially when making purchases with credit cards!
- SFTP, not FTP
  - Unless you ***really*** don't care about the password or data
  - Can also use KerbFTP
- IPSec
  - Provides network-layer confidentiality

Social Problems

- People can be just as dangerous as unprotected computer systems
  - People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
  - Most humans will breakdown once they are at the “harmed” stage, unless they have been specially trained
    - Think government here…

Network hardening

- Patches
  - Piece of software designed to fix problems
  - Can be part of software updates
  - Address newly discovered vulnerabilities
  - Should be applied in a timely fashion
- Switch Security
  - Switches: susceptible to ARP poisoning
  - ARP poisoning works by forging replies to ARP broadcasts.

Switch Security

- Example, ARP poisoning:
  - Two hosts
    - V: IP: 192.168.1.2, MAC: 00-AA-22-BB-12-06,
    - M: IP 176.20.1.3, MAC : 00-04-DC-BD-31-07
    - M broadcasts an ARP onto the network with V's IP but M's MAC.
  - Switches can be configured to allow only specific MAC addresses to send traffic through a specific port in a switch (port security)
  - Switches can be used to implement VLANs

Network hardening

- Access Control Lists
  - Routers can be used to perform packet filtering
  - ACLs can be used to permit or deny TCP and UDP traffic based on source IP, destination IP or both or on port numbers.
  - Router ACLs are not firewalls
  - Example: ACLs can be used on border routers and WAN links

Network hardening

- Unutilized services
  - Disable extraneous services on routers
  - Example: Cisco routers have proxy-arp service enabled by default
  - Proxy-arp: allows one host to respond to ARP requests on behalf of another host
  - Others: web server, finger server, boot server, tftp server services

Network hardening

- Internet Control Message Protocol
  - Provides mechanisms for reporting TCP/IP communication problems and utilities for testing IP connectivity
  - PING and Traceroute:
    - Echo requests and replies for testing connectivity
    - Can be used to scan networks and identify publicly available hosts
    - ICMP echo requests and replies have been used to create covert channels through firewalls

Network hardening

- Traceroute:
  - Used in mapping network path between source and destination hosts
  - Sends out consecutive packets with TTL field incremented each time
  - TTL packets can be used to identify open ports in a perimeter firewalls.
  - Attacks have been launched by hackers using TCP, UDP and ICMP packets that expire one hop beyond the perimeter wall (receiving ICMP TTL Exceeded message, Research on firewalk from www.packetfactroy.net)

Network hardening

- Directed Broadcast
  - Sending packets to network or broadcast addresses in a network
  - Forms the basis of Bandwidth amplification attacks
  - Example attack tools: Smurf and fraggle

Network hardening

- Other administrative practices
  - Banners displayed whenever a connection is established as part of the login process
  - Restricting remote access
  - Centralizing account management
  - Configuring SNMP consoles for management