Attacks on Different OSI Layer Protocols

Attacks at Network Layer

Mohammad Ashiqur Rahman

Department of Computer Science
College of Engineering
Tennessee Tech University
Agenda

- Idea of DDoS
- Attacks at Network Layer
  - Attacks on Routing Protocol
  - ICMP-based Attacks
  - DHCP-based Attacks
DDoS

- Distributed Denial of Service

DDoS: Master and Slave Technique

- Maximize Damage and Hide Identity

http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html
DDoS: Master and Slave Technique (2)

Scan for systems to attack

Handler systems: Install software to scan, compromise, and infect agents

Agent systems: agents get loaded with remote control attack software
Botnet

- Zombie army

- About bots:
  - Bots of 10,000+ machines are reported
  - Bots are common
  - Bots are *rented* per hour
  - Bots are used for a variety of attacks, DDoS, Spam, as web servers which serve illegal content,...
DoS Tools

- Many public tools for flooding a victim with unwanted traffic
  - LOIC (Low Orbit Ion Canon)
    - Used by the popular hackers group Anonymous
    - A single user can perform attack on small servers
  - XOIC
    - It performs a DOS attack an any server with an IP address, a user-selected port, and a user-selected protocol.
  - Trin00 (Trinoo)
  - TFN – Tribe Flood Network
  - Stacheldraht
    - German for “Barbed Wire”
DDoS Tool: TrinOO

- Password protected options, encrypted daemon list
  - Startup, remote control, and kill
  - Attacker talks to masters (clients) using tcp
  - Master and zombies (daemons/agents) use udp
  - All messages (commands) sent in clear.
    - Easy to fingerprint whether the network is infected.

- (Remote) OS Fingerprinting is the process of determining the operating system used by a host on a network.
Defense against DoS!

- **Stopping DoS Attacks**
  - Ingress filtering to stop attack packets
    - Limited ability of ingress filtering because link to ISP might become overloaded → next page
  - Egress filtering by attacker’s company or ISP
    - What if IP spoofing and/or very distributed!
    - Requires cooperating from attacker’s company or ISP
  - Requires a community response; victim cannot do it alone.
Defense against DoS: Difficulty

A network can apply defense at its border router/firewall!

1. ISP Access Line Saturated by Attack Packets
2. Attack Packets Blocked
3. Legitimate Packets Cannot Get Through
4. Attacks Must Be Stopped on the Internet
5. Other Companies Must Harden Hosts So They Are Not Compromised and Used in Attacks
Path selection is a process of selecting (predicting) the best route (from multiple routes) based on a routing metric.

- In the case of overlapping or equal routes?
  - An approach follows **prefix-length**: Longer subnet masks are preferred.
Attacks on Routing Table: Idea

- Attacker needs to get access to a router to do route hijacking.
  - Announcing a more desirable route
    - Z can lie about its route to A
    - A router announces that it originates a prefix that it does not actually originate.
      - Individual IP addresses are grouped together into a prefix (i.e., network address)
  - Route hijacking is a.k.a. IP hijacking, prefix hijacking, or BGP hijacking.
Attacks on Forwarding Table

- Routers keep a cache of recently used routes
  - Forwarding table
- Attacker sends many packets to many different destination prefixes through a router causing its forwarding cache to thrash
  - Attacker needs to be close to the router
  - Impact: If cache is small, causes loss of routes
ICMP

- Internet Control Message Protocol
- Designed for error control and query
- Functions:
  - Communication errors
    - When a datagram cannot reach its destination
  - Important (useful) events or special requests
    - When a gateway needs to direct the host to send traffic through an alternate route
  - Ping service
ICMP Header

- It is an adjunct to IP!

### ICMP packet

<table>
<thead>
<tr>
<th>Bit 0 - 7</th>
<th>Bit 8 - 15</th>
<th>Bit 16 - 23</th>
<th>Bit 24 - 31</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version/IHL</td>
<td>Type of service</td>
<td>Length</td>
<td></td>
</tr>
<tr>
<td>Identification</td>
<td></td>
<td>flags and offset</td>
<td></td>
</tr>
<tr>
<td>Time To Live (TTL)</td>
<td>Protocol</td>
<td>Checksum</td>
<td></td>
</tr>
</tbody>
</table>

**IP Header (20 bytes)**

- Source IP address
- Destination IP address

**ICMP Payload (8+ bytes)**

- Type of message
- Code
- Checksum
- Quench
- Data (optional)

### ICMP Types

- 0 Echo Reply
- 3 Destination Unreachable
- 4 Source Quench
- 5 Redirect
- 8 Echo
- 12 Parameter Problem
- 13 Timestamp
- 14 Timestamp Reply
- 15 Information Request
- 16 Information Reply
- 17 Address Mask Request
- 18 Address Mask Reply
ICMP Based Attacks

- Path reconnaissance using traceroute, monitoring TTL
  - Traceroute attempts to map network devices (and hosts) on a route to a certain destination host.
  - Initially, an ICMP echo message is sent with TTL = 1.
    - The TTL value is incremented by one.
    - The process is repeated until it finds the correct destination address.

- Crafting fake ICMP error messages after sniffing IP traffic
  - Connection-Reset Attacks:
    - ICMP Destination Unreachable or ICMP Time Exceeded can cause denial of service
  - Throughput-Reduction Attacks:
    - ICMP Source Quench can create reduced throughput
  - Redirection Attacks:
    - ICMP Redirect Message can make traffic to be illicitly routed
The maximum allowable IP packet size is 65,535 bytes, including the packet header, which is typically 20 bytes long. An ICMP echo request has a pseudo header of 8 bytes.

- Therefore, the maximum allowable size of the data area of an ICMP echo request is 65,507 bytes.
- Unfortunately, many ping implementations allow the user to specify a packet size larger than 65,507 bytes.
ICMP Based Spoofing Attacks

- IP spoofing in addition with ICMP echo request and reply can cause Denial of service attack for the spoofed victim!
  - What can be the idea?
    - Spoofed echo request from multiple attackers for the same victim
    - Directed broadcast address: multiple echo requests ... coming from one victim?
      - SMURF attack
Smurf attack

- Victim’s IP is spoofed as source and used to send ICMP ping request as broadcast message.
- Victim swamped by ICMP echo reply.

Often limited to local network!
  - Usually, incoming ICMP packets are restricted.

http://www.technospot.net/blogs/types-of-dos-attacks-and-introduction-to-ddos/
About DHCP

- Dynamic Host Configuration Protocol
  - Assigns IP address to booting host
  - Administrative use
- Leases IP addresses to hosts requesting an address

Two databases for each DHCP server:

- Static IP pool
  - For devices with known hardware address
  - Same address for same device
  - Server checks static pool for match before dynamic pool
- Dynamic pool
  - For devices with unknown hardware address
  - Addresses are temporary (default lease = 1 hr)
  - After lease expires, client must ask for a renewal
  - If renewal is rejected, client must give up the IP address
  - DHCPv6 allows revocation (recalling of the grant/privilege) before lease expires
DHCP Operation

DHCP client broadcasts
discover message.

DHCP server unicasts
offer message.

DHCP client responds
with request message.

DHCP server completes the process
with acknowledgment message.

DHCP DISCOVER
client asking for an IP address

DHCP OFFER
Servers offering an IP address

DHCP REQUEST
client asking for IP address
confirmation

DHCP ACK
Server confirming the
IP address assignment

DHCP RENEW
client asking for same IP address to
be renewed for another lease period

DHCP ACK
server acknowledging renew
request

DHCP RELEASE
client request for releasing
assigned IP address

DHCP 4-way handshake
for IP address assignment

Address Renewal Process
(usually repeated multiple times)

Address Release Phase

Source: http://ciscodocuments.blogspot.com/2011/05/chapter-4-implementing-inter-vlan_19.html
Source: http://computernetworkingsimplified.com/application-layer/dhcp-protocol-overview-benefits/

M. Ashiq Rahman, Tennessee Tech University
DHCP Security Concerns

- DHCP Server DoS attack
  - Consume dynamic pool by repeatedly sending discover packets for fake hardware addresses.

- Rogue DHCP server
  - Could give out false (invalid/incorrect) information

- Posing as DHCP client
  - Could send fake release/lease packets from spoofed clients to cause chaos in network
THANKS

Acknowledgement:
- https://www.sans.org/security-resources/idfaq/how-can-attacker-use-icmp-for-reconnaissance/3/13
- Wikipedia, some figures are taken from different online sources.
- Ehab Al-Shaer, UNC Charlotte
- Dr. Ambareen Siraj, Tennessee Tech University