DDoS Attacks and Defenses

CSE 4471: Information Security

Prof. Dong Xuan
Modifications by Adam C. Champion

Some slides from Arbor Networks
Outline

• What is a DDOS attack?
• How do we defend against a DDoS attack?
What is a DDoS attack?

• Internet DDoS attack is real threat
  – On websites
    o Yahoo, CNN, Amazon, eBay, etc. (Feb. 2000)
    o Services were unavailable for several hours
  – On Internet infrastructure
    o 13 root DNS servers (Oct, 2002)
    o 7 were shut down, 2 others partially unavailable

• Lack of defense mechanisms on current Internet
What is a DDoS Attack?

• Denial-of-Service (DoS) attacks:
  – Attempt to prevent legitimate users of a service from using it

• Examples of DoS include:
  – Flooding a network
  – Disrupting connections between machines
  – Disrupting a service

• Distributed Denial-of-Service (DDoS) Attacks
  – Many machines are involved in the attack against one or more victim(s)
Example: Smurf Attack

Reflector Network

ICMP Echo Request

<table>
<thead>
<tr>
<th>SRC</th>
<th>DST</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.3.3.100</td>
<td>2.2.2.255</td>
</tr>
</tbody>
</table>

ICMP Echo Replies

<table>
<thead>
<tr>
<th>SRC</th>
<th>DST</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.2.2.*</td>
<td>3.3.3.100</td>
</tr>
</tbody>
</table>

Attacker
1.1.1.100

Target
3.3.3.100
Example: TCP SYN Flood

- Normal sequence for TCP connection establishment (3-way handshake)

Client

CLOSED

SYN_SENT

SYN 141:141

ACK 142

SYN_RCVD

ESTABLISHED

Server

CLOSED

SYN 182:182

ACK 183

ESTABLISHED
Example: TCP SYN Flood (cont.)

Attacker

<table>
<thead>
<tr>
<th>SYN 141:141</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYN 241:241</td>
</tr>
<tr>
<td>SYN 341:341</td>
</tr>
<tr>
<td>SYN 441:441</td>
</tr>
<tr>
<td>SYN 541:541</td>
</tr>
<tr>
<td>SYN 641:641</td>
</tr>
<tr>
<td>SYN 741:741</td>
</tr>
</tbody>
</table>

Server

<table>
<thead>
<tr>
<th>SYN 182:182</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK 142</td>
</tr>
<tr>
<td>SYN 282:282</td>
</tr>
<tr>
<td>ACK 242</td>
</tr>
<tr>
<td>SYN 382:382</td>
</tr>
<tr>
<td>ACK 342</td>
</tr>
</tbody>
</table>

Listen Queue

- SYN_RCVD
- SYN_RCVD
- SYN_RCVD
- SYN_RCVD
- SYN_RCVD
- SYN_RCVD
- SYN_RCVD
- SYN_RCVD

What Makes DDoS Attacks Possible?

- Internet was designed with functionality & not security in mind
- Internet security is highly interdependent
- Internet resources are limited
- Power of many greater than power of a few
Addressing DDoS attacks

• **Ingress filtering**
  – P. Ferguson and D. Senie, RFC 2267, Jan 1998
  – Block packets that has illegitimate source addresses
  – Disadvantage : Overhead makes routing slow

• **Identification of origin (Traceback problem)**
  – IP spoofing enables attackers to hide their identity
  – Many IP traceback techniques are suggested

• **Mitigating the effect during the attack**
  – Pushback
IP Traceback

• Allows victim to identify attackers’ origin
• Several approaches
  – ICMP trace messages
  – Probabilistic Packet Marking (PPM)*
  – Hash-based IP traceback
  – …

PPM (1)

• PPM scheme:
  – Probabilistically inscribe local path information
  – Use constant space in the packet header
  – Reconstruct attack path with high probability

Marking at router $R$

// Probability $p \in (0, 1)$
for each packet $w$ do
  $x \leftarrow$ random real number in $[0, 1)$
  if $x < p$ then
    $w$.head $\leftarrow$ IP address of $R$
    $w$.distance $\leftarrow$ 0
  end if
  else
    if $w$.distance $==$ 0 then
      $w$.tail $\leftarrow$ IP address of $R$
    end if
    $w$.distance $\leftarrow$ $w$.distance + 1
  end if
end for
PPM (2)
PPM (3)
PPM (4)
PPM (5)
What is Pushback?

• Mechanism that lets a router ask adjacent upstream routers to limit the traffic rate
How Does it Work?

• A congested router asks other adjacent routers to limit the rate of traffic for that particular aggregate.
• Router sends pushback message
• Received routers propagates pushback
Conclusion

• What is a DDoS attack?
• Defending against a DDoS attack
  – Ingress filtering
  – Traceback
  – Pushback