Defending Against DDoS Attacks

CSE 4471: Information Security
Instructor: Dr. Adam C. Champion
Outline

• Review: What is a DDoS attack?

• How to defend against a DDoS attack?
What is a DDoS Attack?

• DoS attacks: Attempt to prevent legitimate users of a service from using it

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

• Distributed Denial-of-Service (DDoS) Attacks
  – Many machines involved in attack against one or more victim(s)
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
Strategies: Defending Against DDoS Attacks

- Ingress Filtering
  - P. Ferguson and D. Senie, RFC 2827 (May 2000); D. McPherson et al., RFC 6959 (May 2013)
  - Block packets with illegitimate source addresses
  - Disadvantage: Overhead makes routing slow
- Identify attack origin(s) – Traceback problem
  - IP spoofing enables attackers to hide their identity
  - Many IP traceback techniques are suggested
- Mitigation during attack
  - Pushback: Tell upstream routers to stop attack traffic
IP Traceback

• Allows victim to identify attackers’ origins (and attack paths)

• Several approaches:
  • ICMP trace messages
  • Probabilistic Packet Marking*,
  • Hash-based IP Traceback, etc.

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 $R$

1: // Probability $p \in (0, 1)$
2: for each packet $w$ do
3:   $x \leftarrow$ random real number in $[0, 1)$
4:   if $x < p$ then
5:     $w.head \leftarrow$ IP address of $R$
6:     $w.distance \leftarrow 0$
7:   else
8:     if $w.distance == 0$ then
9:       $w.tail \leftarrow$ IP address of $R$
10:    end if
11:   end if
12: end if
13: end for
PPM (2)
PPM (3)

Legitimate user

Attacker

Victim
PPM: An Example

For each “balloon”:
\[ w\text{-}distance = h \]

- What happens if all routers set \( x > 0.8 \)?

Balloon E is special: no head, no tail are specified!
w.distance is not set by any router!
PPM Extensions

• What if $p$ is not the same among routers?
• PPM needs 9 bytes to mark info in packet ($w.head + w.tail + w.distance$). Can we develop a new marking scheme that needs fewer bytes?
• PPM assumes all routers are cooperative and run PPM. What would happen if some routers do not run PPM or are even malicious?
Pushback

• Mechanism that allows a router to request adjacent upstream routers to limit the rate of traffic

• How it works:
  – Congested router requests other adjacent routers to limit traffic rate for particular aggregate traffic
  – Router sends pushback message
  – Received routers propagates pushback

• More details:
Conclusion

• What is a DDoS attack?
• Defending a DDoS attack
  – Ingress filtering
  – Trace-back: PPM
  – Push-back