Distributed Denial of Service Attacks & Defenses

Guest Lecture by:
Vamsi Kambhampati

Fall 2011
Distributed Denial of Service (DDoS)

- Exhaust resources of a target, or the resources it depends on
  - Resources: CPU, Memory, Bandwidth
    - Legitimate clients cannot access the target server

- Should we care?
  - For researchers: interesting problem; difficult to solve.
  - For others: monetary loss, infrastructure security.
Example: Bandwidth Exhaustion DDoS Attack

- Attacker packets dropped
- Legitimate packets also dropped
- Congested router
- Legitimate client
- Destination
Well-behaved and misbehaving flow at router

- Legitimate flow
- Attacker flow

Rate: pkts/sec

Congestion at router
Well-behaved and misbehaving *traffic* at router

![Diagram](image)

- Congested router
- Well-behaved aggregate *looses* throughput
- Misbehaving aggregate *gains* throughput

**Rate**: pkts/sec

**Time**
Well-behaved and misbehaving traffic at destination

misbehaving traffic does not slow down when destination requests

well-behaved traffic slows down when destination requests

rate pkts/sec
destination

time
What is the problem?

• Well-behaved (i.e., legitimate) traffic follows protocol rules

• Misbehaving traffic does not follow protocol rules

• Internet lacks distributed enforcement of protocol rules
Defending DDoS Attacks

• Filtering
  – Ingress filtering, Traceback, Pushback

• Network capabilities
  – Stateless Internet flow filtering (SIFF)
  – Traffic validation architecture (TVA)

• Proof of work
  – Congestion puzzles, Defense by offense

• Location hiding
  – Secure overlay services (SOS), i3
DDoS defense with *traceback*

destination *constructs path* from edge information

routers insert *edge* information
DDoS defense with pushback

- **pushback** to contributing router
- Identify aggregate responsible for congestion
Network Capabilities

• Fundamental change to the Internet, so that sender must have authorization from receiver to send traffic
  – Receiver decides what traffic it wants to receive or not receive
  – Network enforces receiver’s decision
Phase 1: Request Capabilities
Pre-Capabilities

• Cryptographically generated at each router $R$
  – Each router can independently verify its own pre-capability

• Timestamp + Hash($\text{SrcIP, DstIP, time, } R_{\text{secret}}$)
  – $\text{SrcIP, DstIP}$ tie the capability to a flow
  – $R_{\text{secret}}$: secret key only known to the router (the same secret is used for all pre-capabilities)
    • $R_{\text{secret}}$ changed twice per timestamp roll over
Phase 2: Authorizing a source

attacker

source

destination

host-capability

SYN
Host-Capability

- Cryptographically generated at the destination using pre-capabilities

- Timestamp + Hash(pre-capabilities, N, T)
  - N is the number of packets authorized per capability
  - T is the time period for which the capability is valid

- Routers track N, and T
Phase 3: Send Traffic

- Source
- Attacker
- Destination

- Data
- Pre-capability verify
- Host-capability verify

- BOGUS
Traffic Classes

- Traffic classes
  - Request
    - Request packets (such as TCP SYN)
  - Regular
    - Packets with capabilities
  - Demoted
    - Packets with invalid capabilities
  - Legacy

- Separate bandwidth allocated to regular and request traffic at each router
Denial of Capabilities (DoC)

• Attacker sends flood of request packets
  – Legitimate requests get lost before reaching the destination

• TVA solution:
  – Path identifiers (Pi)
Path Identifiers

- Routers insider Pi bits into request packets
  - Kind of like pre-capabilities
- Next downstream router fair-queues on the Pi bits inserted at upstream routers
  - Number of Pi queues = number of upstream routers
Simulation Topology

10 legitimate clients

1 ~ 100 attackers

10Mbps, 10ms bottleneck link

destination

colluder
Simulation Results (1)

As number of attackers increase, legitimate clients suffer

Legitimate clients are unaffected
Simulation Results (2)

Request traffic floods
Summary

• DDoS attacks are a major threat to the Internet
• Capabilities make fundamental changes to the Internet to defend DDoS attacks
  – Sender needs authorization from receiver to send traffic
• Capabilities setup is challenging
  – Denial of Capability attacks