Review

- Differentiating between DoS attack and perfectly normal scenario of service impairment is difficult
- Attacker tries to launch attacks without revealing itself and without expending too much of its own resources
- Smurf attacks
- TYP SYN spoofing attacks

Types of Flooding Attacks

- Classified based on network protocol used
- ICMP Flood
  - Uses ICMP packets, eg echo request
  - Typically allowed through, some required
- UDP Flood
  - Alternative uses UDP packets to some port
- TCP SYN Flood
  - Use TCP SYN (connection request) packets
  - But for volume attack
SYN Flooding Attack

• 90% of DoS attacks use TCP SYN floods
• Streaming spoofed TCP SYNs
• Takes advantage of three way handshake
• Server start “half-open” connections
• These build up... until queue is full and all additional requests are blocked

Recall TCP Handshake

SYN Flooding

SYN C
SYN S, ACK C
ACK S
Listening
Wait
Connected

C
S

SYN C1
SYN C2
SYN C3
SYN C4
SYN C5
Listening
Store data
Distributed Denial of Service Attacks

- Have limited volume if single source used
- Multiple systems allow much higher traffic volumes to form a Distributed Denial of Service (DDoS) Attack
- Often compromised PC’s / workstations
  - Zombies with backdoor programs installed
  - Forming a botnet
- E.g. Tribe Flood Network (TFN), TFN2K

DDoS Control Hierarchy

Can you find source of attack?

- Hard to find Attacker
  - Originator of attack compromised the handlers
  - Originator not active when DDoS attack occurs
- Can try to find agents
  - Source IP address in packets is not reliable
  - Need to examine traffic at many points, modify traffic, or modify routers
Source Address Validity

- Spoofed Source Address
  - Random source addresses in attack packets
  - Subnet Spoofed Source Address
    - random address from address space assigned to the agent machine’s subnet
  - En Route Spoofed Source Address
    - address spoofed en route from agent machine to victim
- Valid Source Address
  - used when attack strategy requires several request/reply exchanges between an agent and the victim machine
  - target specific applications or protocol features

Reflection Attacks

- Use normal behavior of network
- Attacker sends packet with spoofed source address being that of target to a server
- Server response is directed at target
- If send many requests to multiple servers, response can flood target
- Various protocols e.g. UDP or TCP/SYN
- Ideally want response larger than request
- Prevent if block source spoofed packets

Reflection Attacks

- Further variation creates a self-contained loop between intermediary and target
- Fairly easy to filter and block
Amplification Attacks

- Use DNS requests with spoofed source address being the target
- Exploit DNS behavior to convert a small request to a much larger response
  - 60 byte request to 512 - 4000 byte response
- Attacker sends requests to multiple well connected servers, which flood target
  - Need only moderate flow of request packets
  - DNS servers will also be loaded

DNS Amplification Attacks

- High traffic volumes may be legitimate
  - Result of high publicity, e.g. “slash-dotted”
  - Or to a very popular site, e.g. Olympics etc
- Or legitimate traffic created by an attacker
- Three lines of defense against (D)DoS:
  - Attack prevention and pre-emption
  - Attack detection and filtering
  - Attack source traceback and identification

DoS Attack Defenses
**Attack Prevention**

- Block spoofed source addresses
  - On routers as close to source as possible
  - Still far too rarely implemented
- Rate controls in upstream distribution nets
  - On specific packets types
  - E.g. some ICMP, some UDP, TCP/SYN
- Use modified TCP connection handling
  - Use **SYN cookies** when table full
  - Or selective or random drop when table full

**Attack Prevention**

- Block IP directed broadcasts
- Block suspicious services & combinations
- Manage application attacks with “puzzles” to distinguish legitimate human requests
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability required

**Responding to Attacks**

- Need good incident response plan
  - With contacts for ISP
  - Needed to impose traffic filtering upstream
  - Details of response process
- Have standard filters
- Ideally have network monitors and IDS
  - To detect and notify abnormal traffic patterns
Responding to Attacks

- Identify type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstream
  - Or identify and correct system/application bug
- Have ISP trace packet flow back to source
  - May be difficult and time consuming
  - Necessary if legal action desired
- Implement contingency plan
- Update incident response plan

Summary

- Introduced denial of service (DoS) attacks
- Classic flooding and SYN spoofing attacks
- ICMP, UDP, TCP SYN floods
- Distributed denial of service (DDoS) attacks
- Reflection and amplification attacks
- Defenses against DoS attacks
- Responding to DoS attacks