Chapter 7
Denial of Service
Denial of Service

• denial of service (DoS) an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as central processing units (CPU), memory, bandwidth, and disk space
• attacks
  – network bandwidth
  – system resources
  – application resources
• have been an issue for some time
Classic Denial of Service Attacks

- can use simple flooding ping
- from higher capacity link to lower
- causing loss of traffic
- source of flood traffic easily identified
Source Address Spoofing

• use forged source addresses
  – given sufficient privilege to “raw sockets”
  – easy to create

• generate large volumes of packets

• directed at target

• with different, random, source addresses

• cause same congestion

• responses are scattered across Internet

• real source is much harder to identify
SYN Spoofing

• other common attack
• attacks ability of a server to respond to future connection requests
• overflowing tables used to manage them
• hence an attack on system resource
TCP Connection Handshake

1. Client sends SYN (seq = x)
2. Server receives SYN (seq = x)
   and sends SYN-ACK (seq = y, ack = x+1)
3. Client receives SYN-ACK
   and sends ACK (ack = y+1)
4. Server receives ACK (ack = y+1)
SYN Spoofing Attack

1. Attacker sends a SYN packet with a spoofed source (seq = x).
2. Server sends a SYN-ACK (seq = y, ack = x+1).
3. Spoofed client resends the SYN-ACK after timeouts.
4. Assume failed connection request.
5. SYN-ACK's to non-existent client discarded.
SYN Spoofing Attack

• attacker often uses either
  – random source addresses
  – or that of an overloaded server
  – to block return of (most) reset packets

• has much lower traffic volume
  – attacker can be on a much lower capacity link
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
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
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
DNS 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
DoS Attack Defenses

- 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 preemption
  - attack detection and filtering
  - attack source traceback and identification
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