Computer Security: Principles and Practice

Chapter 7 – Denial of Service

Denial of Service

- **DoS** is a form of attack on the availability of some service
- by exhausting resources such as
  - 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

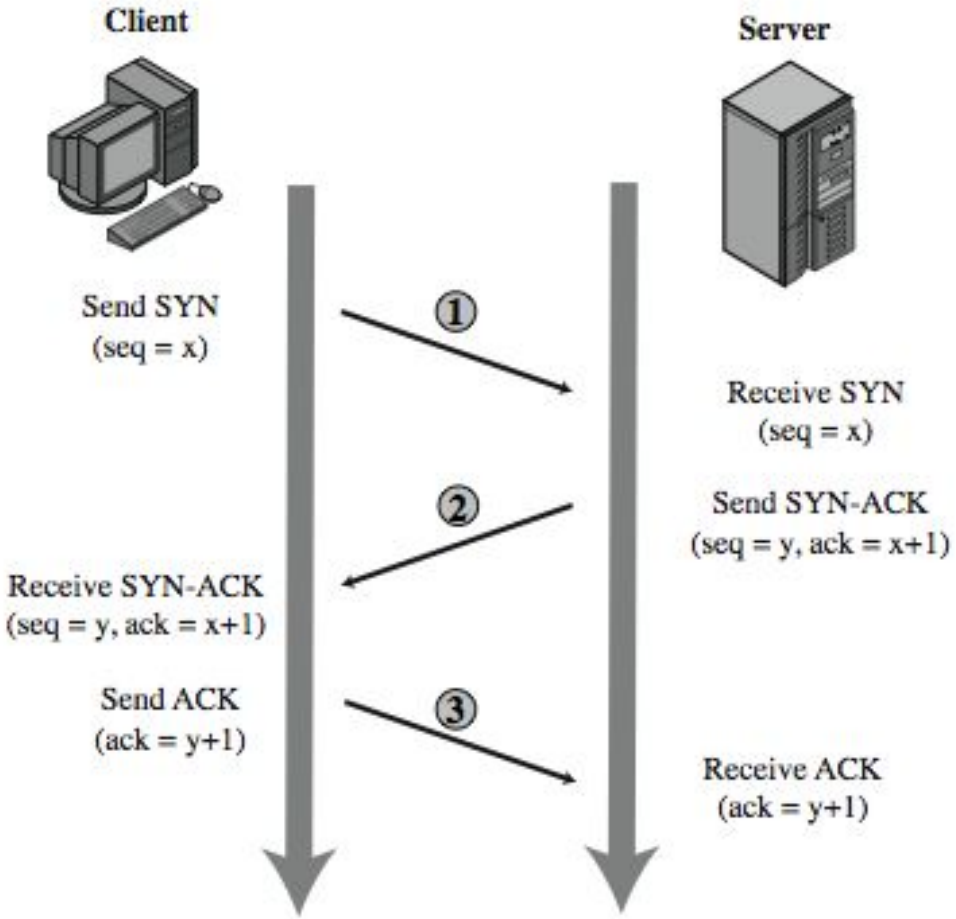
Source Address Spoofing

- use forged source addresses
  - easy to create
- generate large volumes of packets
- directed at target
- with different, random, source addresses
- cause same congestion
- real source is much harder to identify

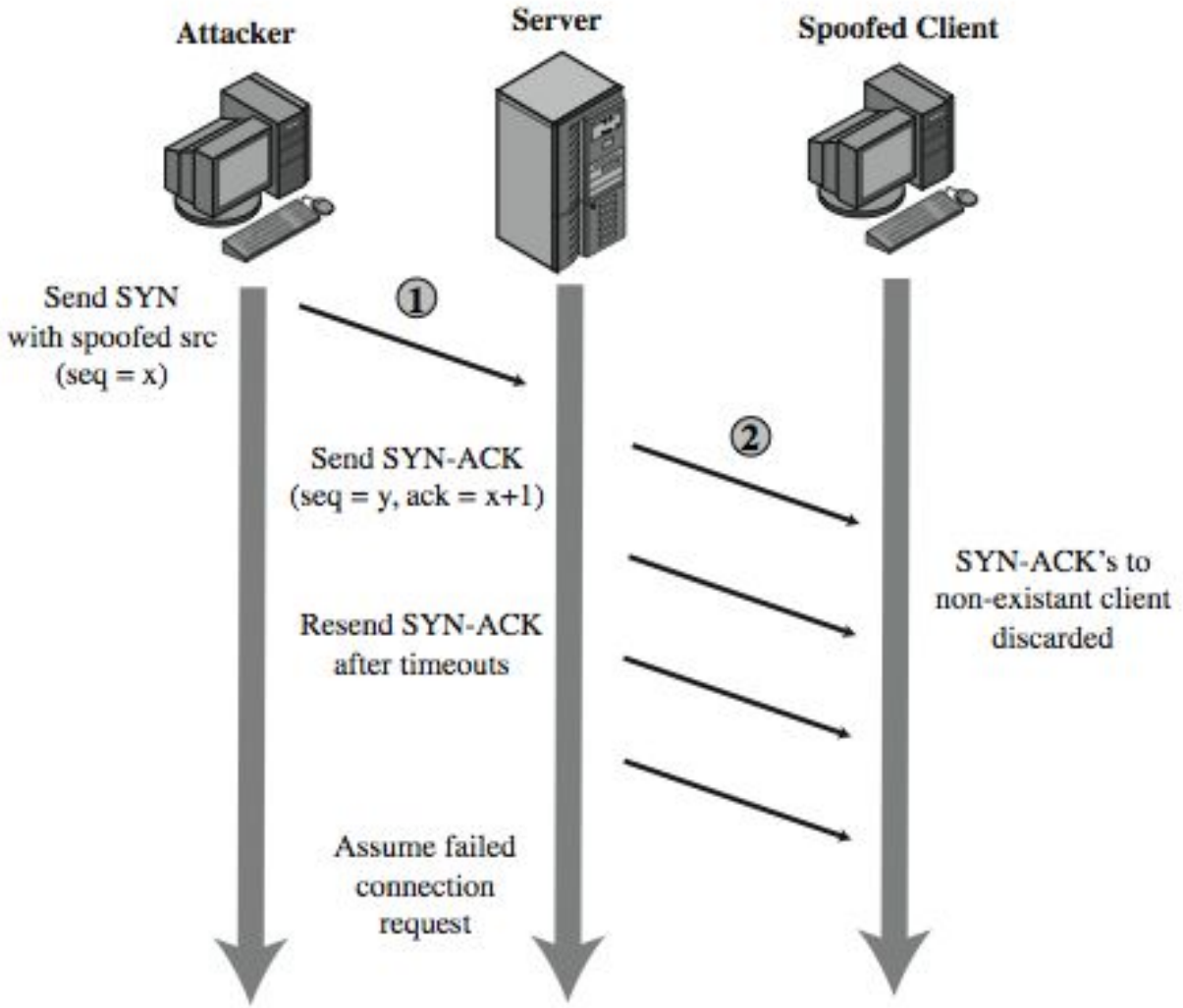
SYN Spoofing

- other common attack
- The attacker sends several connection requests
- 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



SYN Spoofing Attack



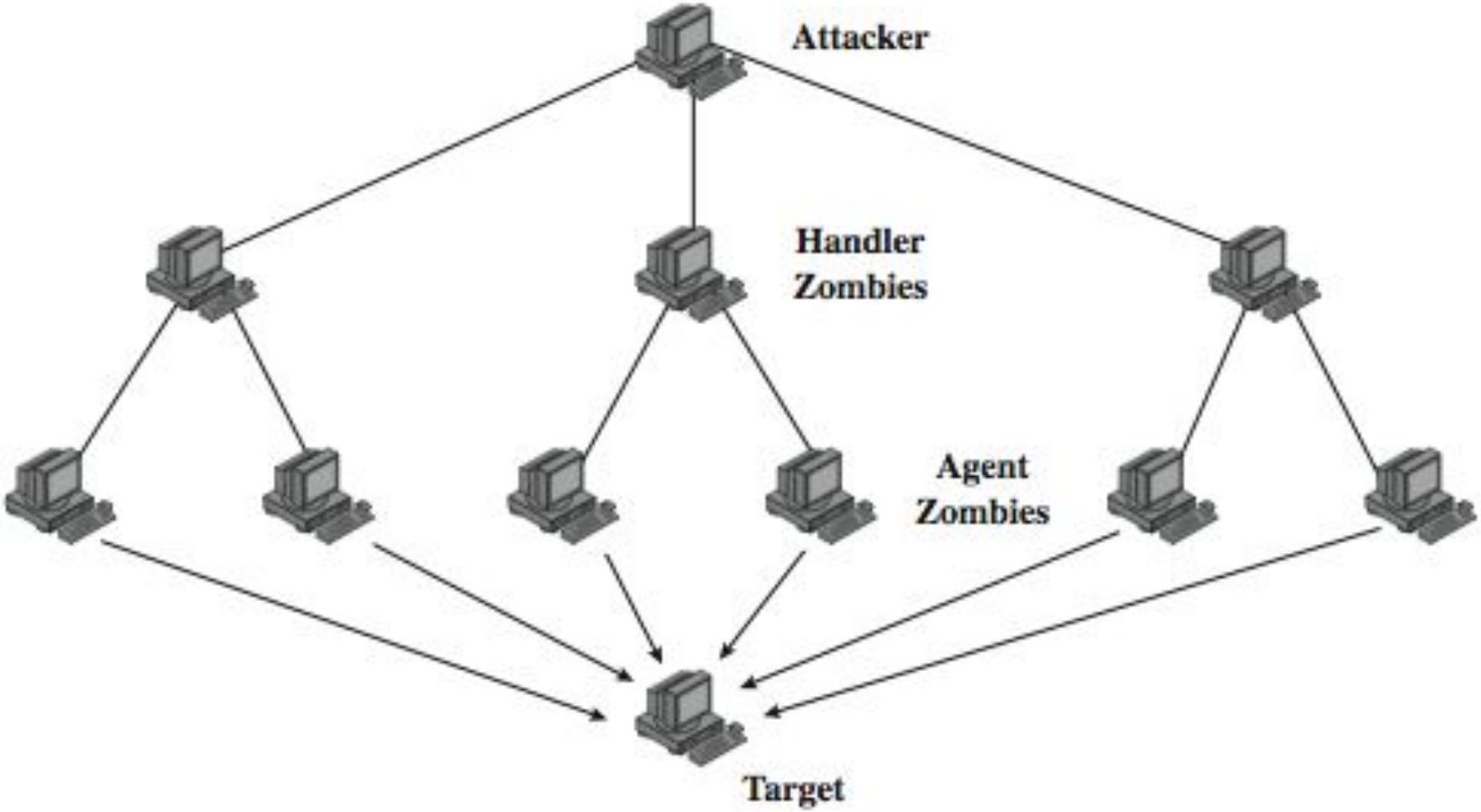
Types of Flooding Attacks

- 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

DDoS Control Hierarchy



Reflection & Amplification 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

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