Denial of Service Attacks

ITS335: IT Security

Sirindhorn International Institute of Technology
Thammasat University

Prepared by Steven Gordon on 20 December 2015
its335y15s2l06, Steve/Courses/2015/s2/its335/lectures/dos.tex, r4287

Contents

Denial of Service Attacks

Classic Denial of Service Attacks

Flooding and Distributed DoS Attacks

Summary

Denial of Service Attacks

A denial of service (DoS) attack is an action that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources such as CPU, memory, bandwidth and disk space.

— NIST Computer Security Incident Handling Guide

DoS Attacks Resources

Network Resources

- Overload communications link or devices to server
- Link from organisation to ISP usually lower capacity than links within and between ISP routers
- As link reaches capacity, router will drop packets

System Resources

- Overload or crash network handling software by sending special packets that consume resources or triggers bug

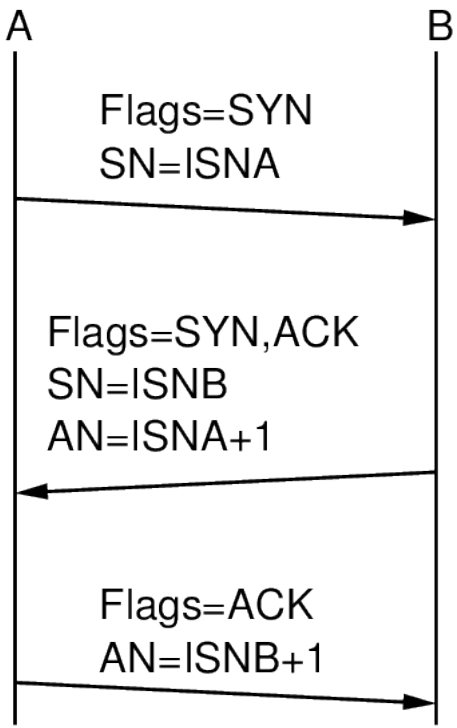
Application Resources

- Send packets to applications (e.g. servers) that force them to consume resources

Contents

TCP Connection Setup

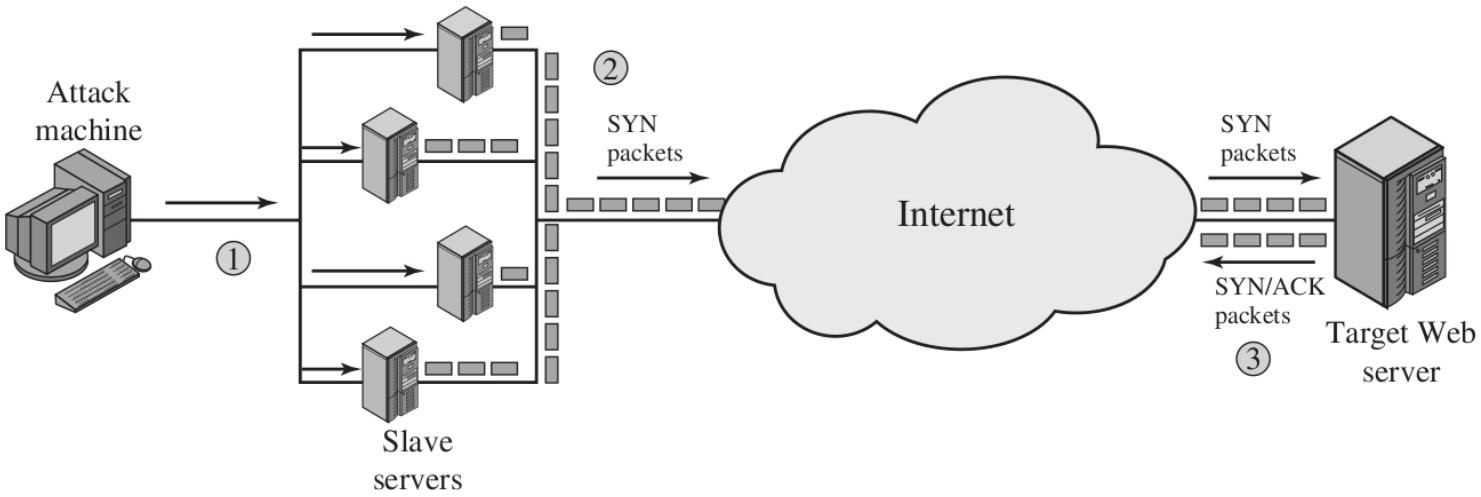
- TCP uses 3-way handshake to establish a connection
- Upon receiving SYN, server stores connection information in memory, and waits for ACK
- Re-send SYN-ACK if no ACK from client; eventually server deletes connection information if no ACK



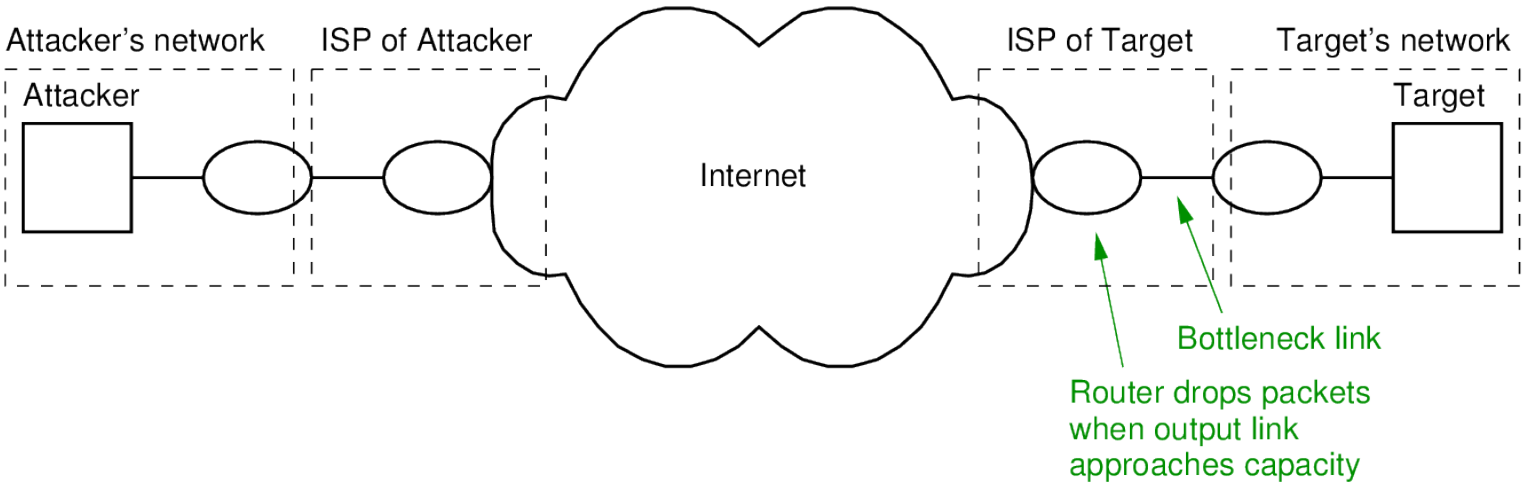
TCP SYN Flooding Attack

- Attacker sends TCP SYN segments to target
  - Source address spoofing is used on TCP SYN segments; no ACKs from client
  - Target becomes overloaded processing SYNs and storing connection information in memory
- Countermeasure: difficult; filter packets at routers; SYN cookies

TCP SYN Flooding Attack



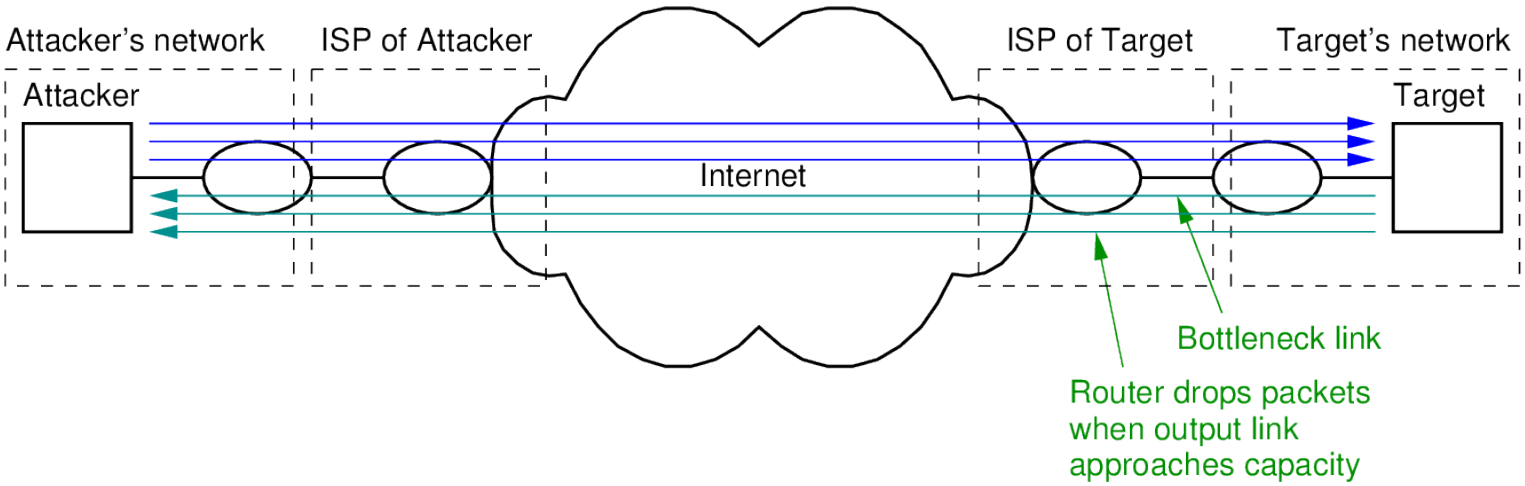
Simple Ping Flooding Attack



Assumptions

- Attacker has access to high capacity link
- Target's connection to Internet is lower capacity

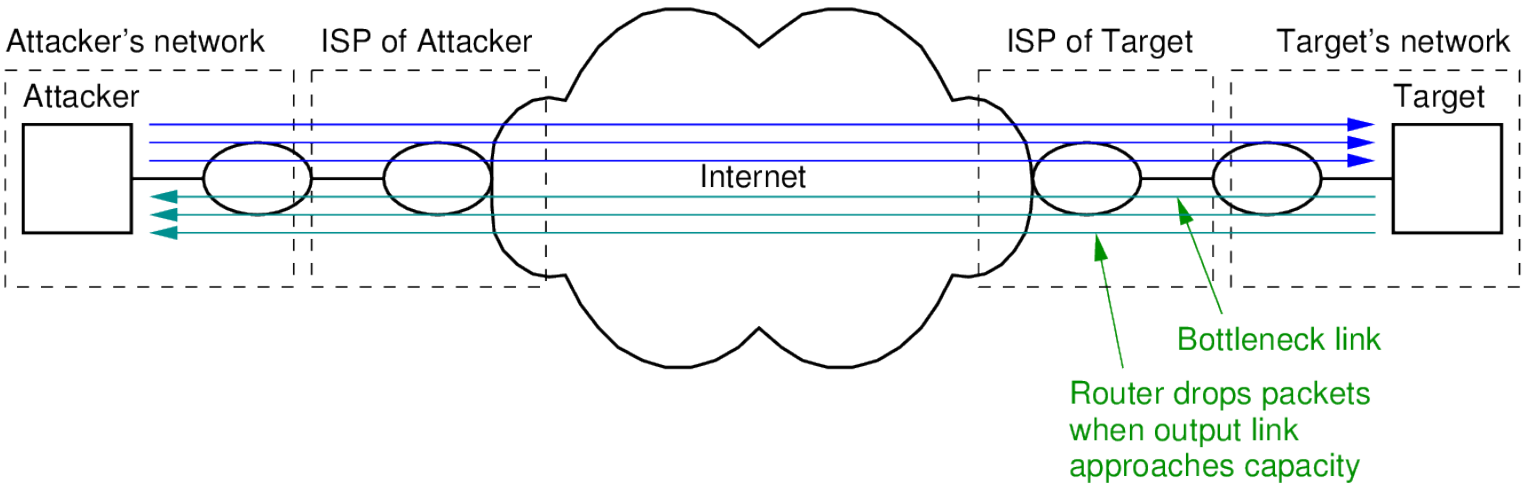
Simple Ping Flooding Attack



Attack

- Flood the server: Attacker uses `ping` to send many ICMP requests to target server
- Link from ISP to router is overloaded; router drops (valid) packets

Simple Ping Flooding Attack



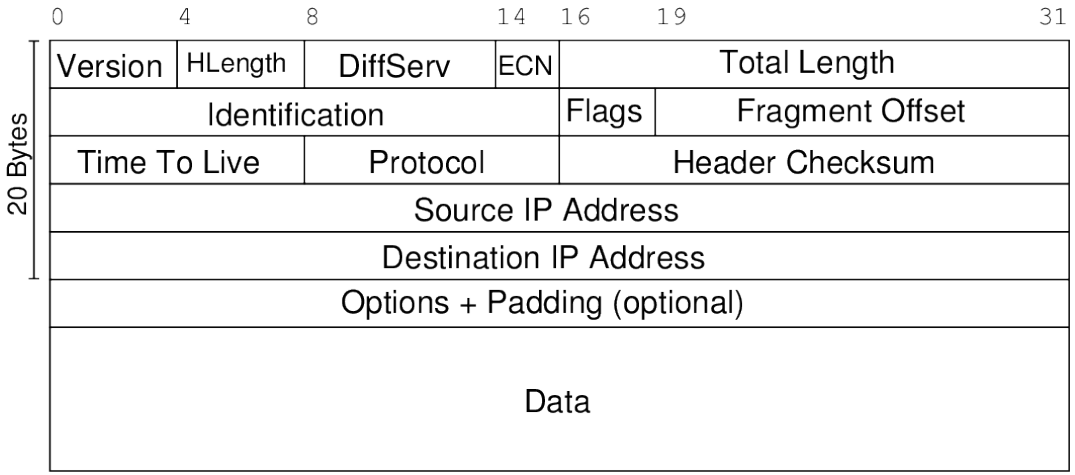
Countermeasures

- ISPs block ping (ICMP) packets
- Target can identify the source: inform ISP, take legal action
- ICMP responses sent back to attacker, affecting their network performance

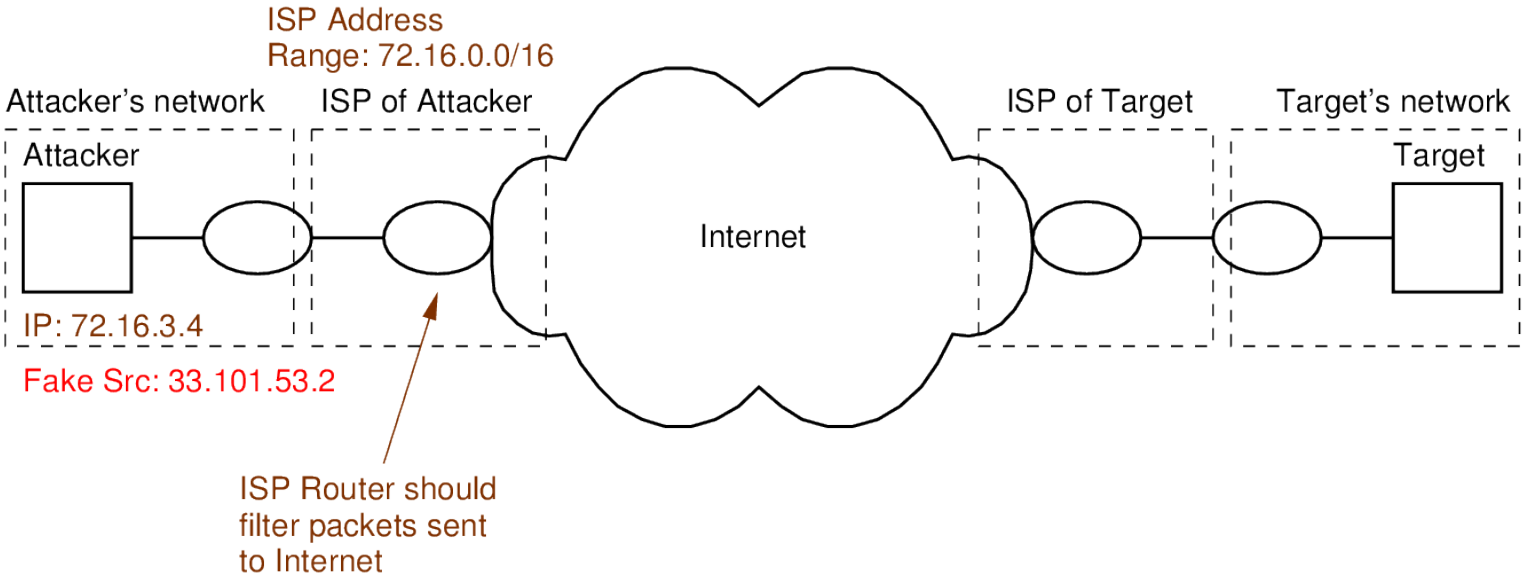
Contents

Source Address Spoofing

- Attacker sends packets with fake (or spoofed) source address
  - Target does not (immediately) know who performed attack
  - Responses are not sent to attacker
  - Source address may be of actual host or non-existent



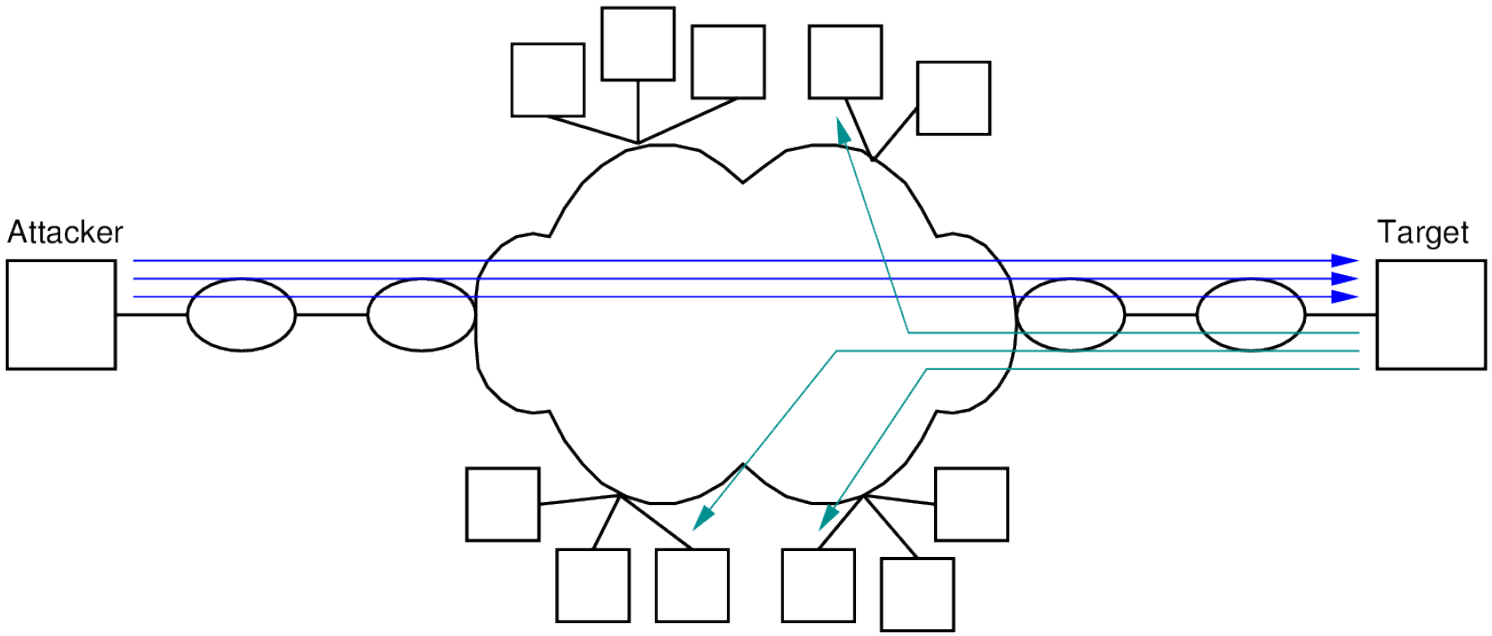
Source Address Spoofing



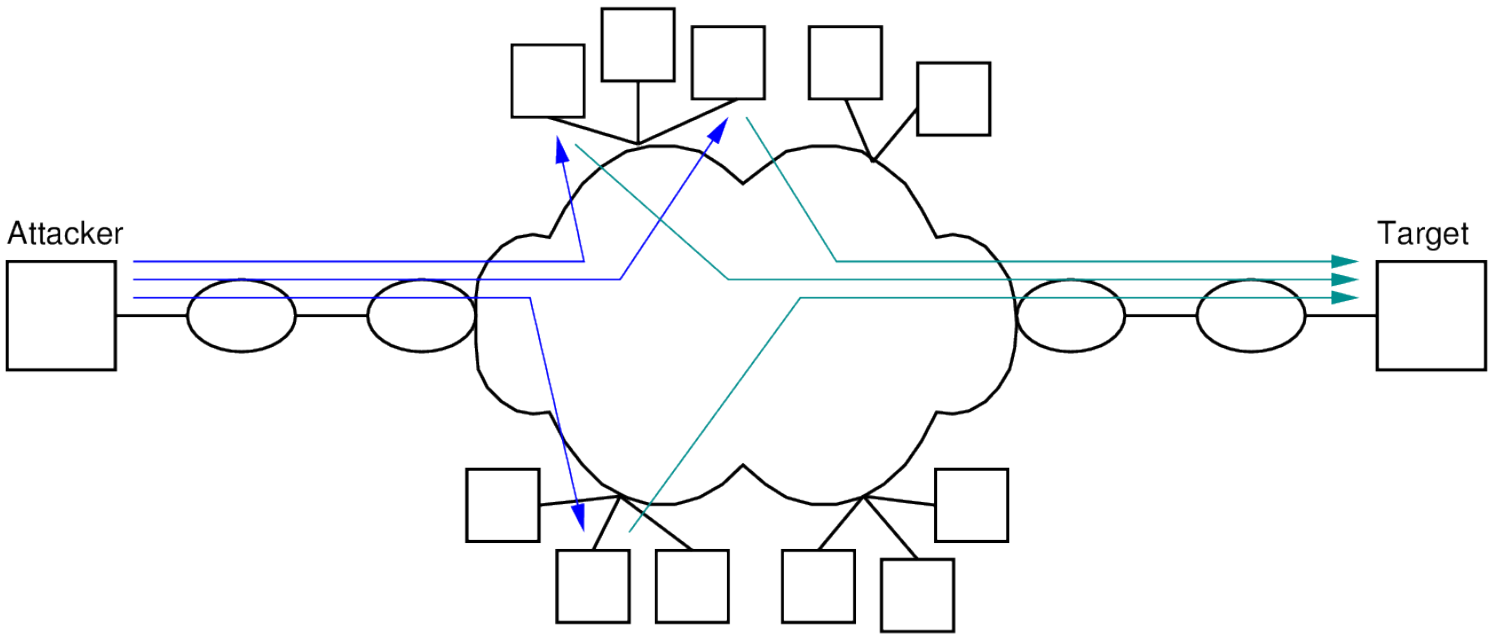
Countermeasure

- ISPs filter (drop) packets that come from invalid source address

Ping Flooding with Source Address Spoofing



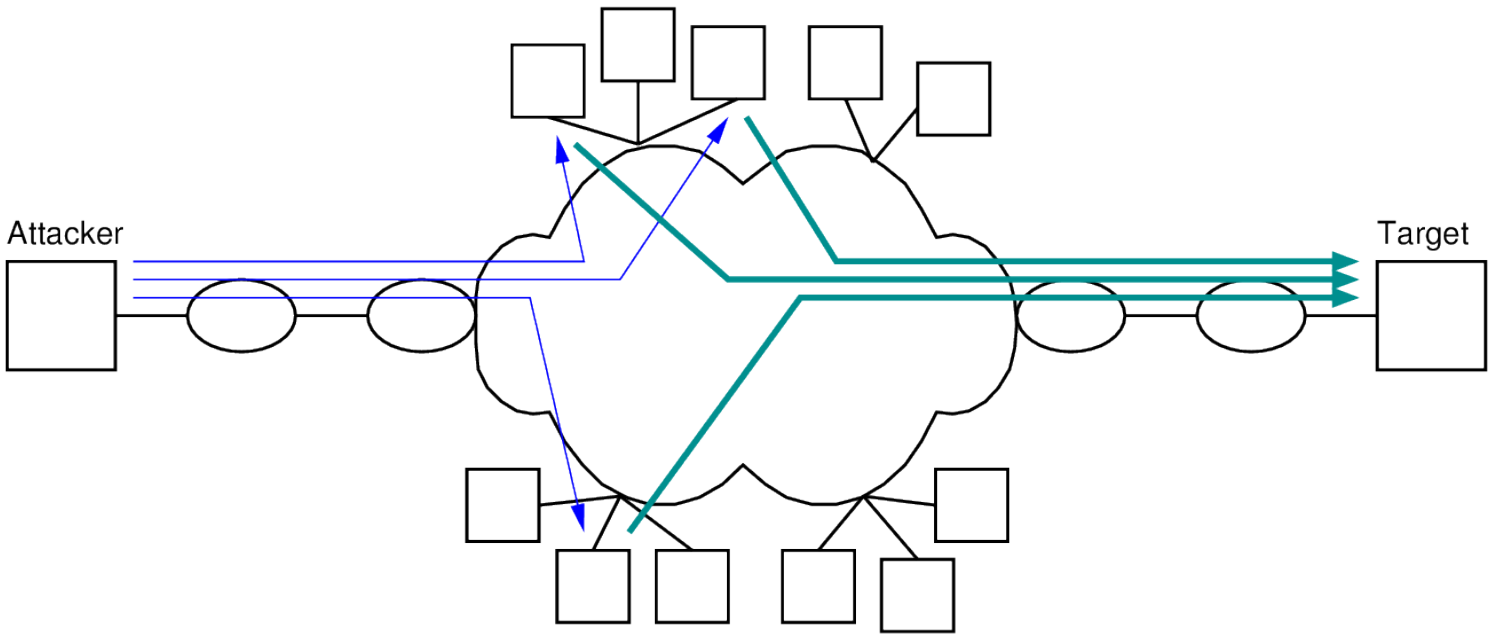
Reflector Attack



Bounce Messages Off Normal Hosts

- Send protocol messages to multiple normal hosts using spoofed source address set to targets
- All hosts respond to target

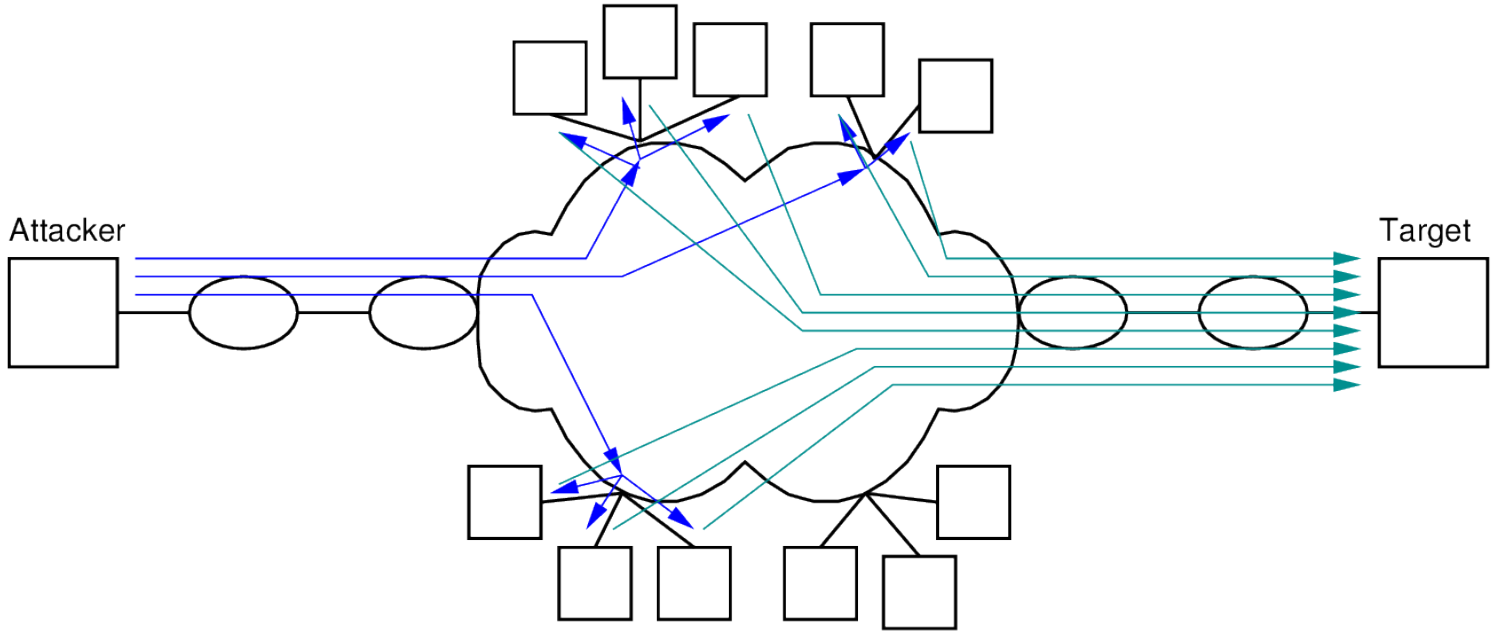
Reflector Attack



Response Larger than Request

- Use protocol/application where request (sent by attacker) is small, by response (sent to target) is large
- Increases amount of traffic sent to target
- E.g. DNS, SNMP, chargen, ISAKMP

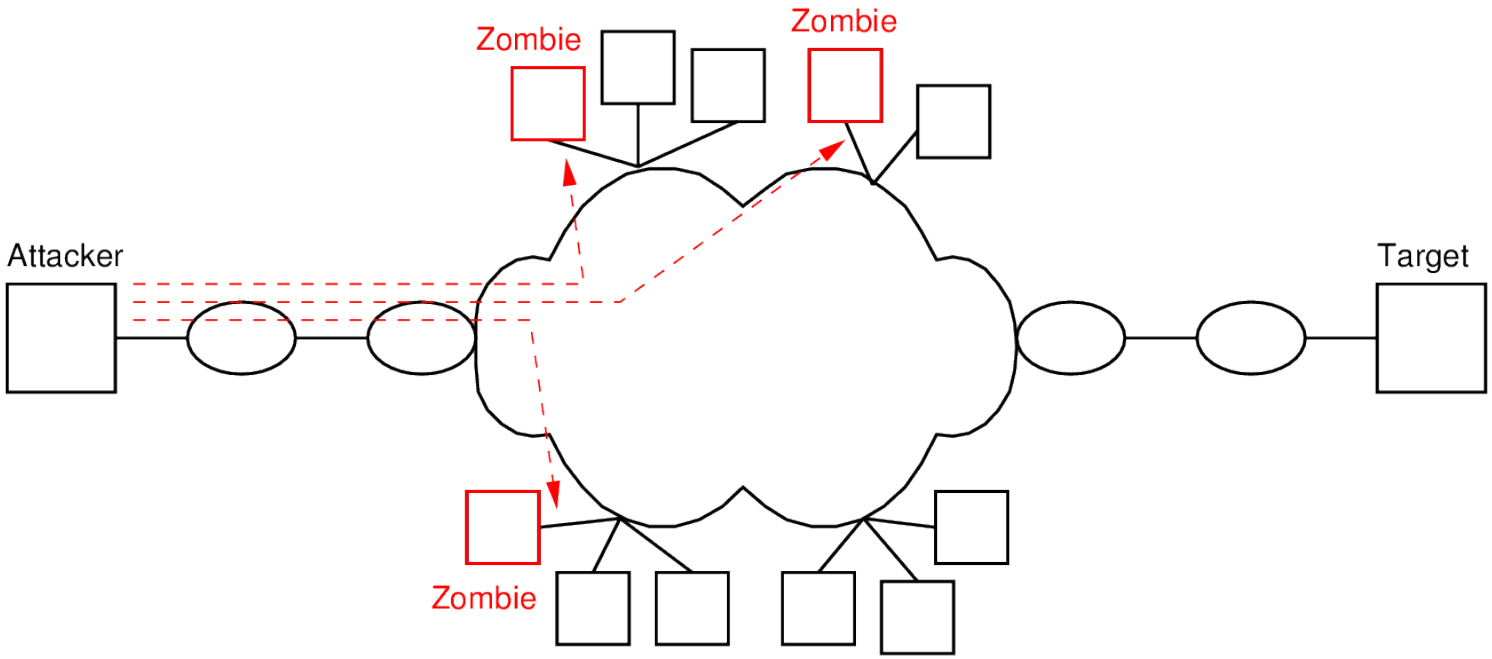
Amplification Attack using Broadcast



Send Request to Entire LAN

- Packets sent to directed broadcast IP addresses (e.g. `192.168.1.255`) are delivered to all hosts on subnet by router
- All hosts respond to target
- Countermeasure: Routers block directed broadcast from outside

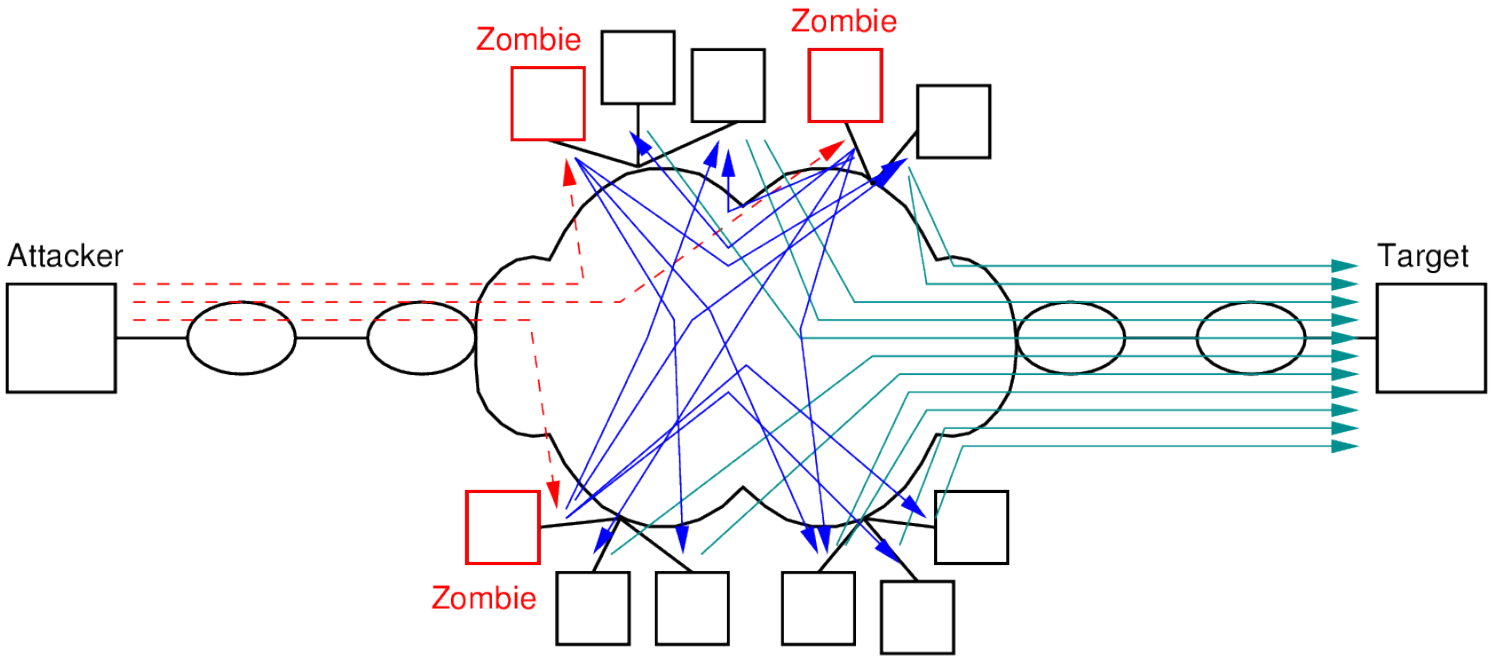
Using Compromised Hosts



Zombies and Botnets

- Attacker takes control of compromised hosts → zombies
- Attacker triggers zombies to initiate attack
- Collection of zombies called botnet

Using Compromised Hosts



Countermeasures

- ?

Constructing Attack Network

- Attacker must get many slave hosts under its control
- Infect the hosts with zombie software

1. Create software that will perform the attacks. This should:
   - Be able to run on different hardware architectures and OSes
   - Hide, that is not be noticeable to the normal user of the zombie host
   - Be able to be contacted by attacker to trigger an attack
2. Identify vulnerability (bug) in large number of systems, in order to install the zombie software
3. Locate vulnerable machines, using scanning:
   - Attacker finds vulnerable machines and infects with zombie software
   - Then the zombie software searches for vulnerable machines and infects with zombie software
   - And so on, until a large distributed network of slaves is constructed

Preventing DDoS Attacks

- Prevention
  - Allocate backup resources and modify protocols that are less vulnerable to attacks
  - Aim is to still be able to provide some service when under DDoS attack
- Detection
  - Aim to quickly detect an attack and respond (minimise the impact of the attack)
  - Detection involves looking for suspicious patters of traffic
- Response
  - Aim to identify attackers so can apply technical or legal measures to prevent
  - Cannot prevent current attack; but may prevent future attacks

Contents

Key Points

- DoS attack prevents normal use of network, system or applications
- Exhausts resources: CPU, memory, bandwidth, disk space
- Address spoofing to hide attacker and redirect traffic to others
- Reflect packets off normal hosts
- Amplify bytes sent to target (compared to bytes sent by attacker)
- Use zombies to initiate attacks; relies on malware to take control
- DoS easy to perform, difficult to prevent, easy to detect (but too late)

Security Issues

- DDoS attacks continue to grow in number and resources consumed
- Many new devices connected to Internet (home, electricity grid, sensors, factories) are potential zombies and target
- Require cooperation between ISPs and companies, as well as legal measures

Areas To Explore

- Detection and prevention: SYN cookies, traffic classification, blackhole, ...
- Spam and botnets
- Stuxnet and cyberwar