CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

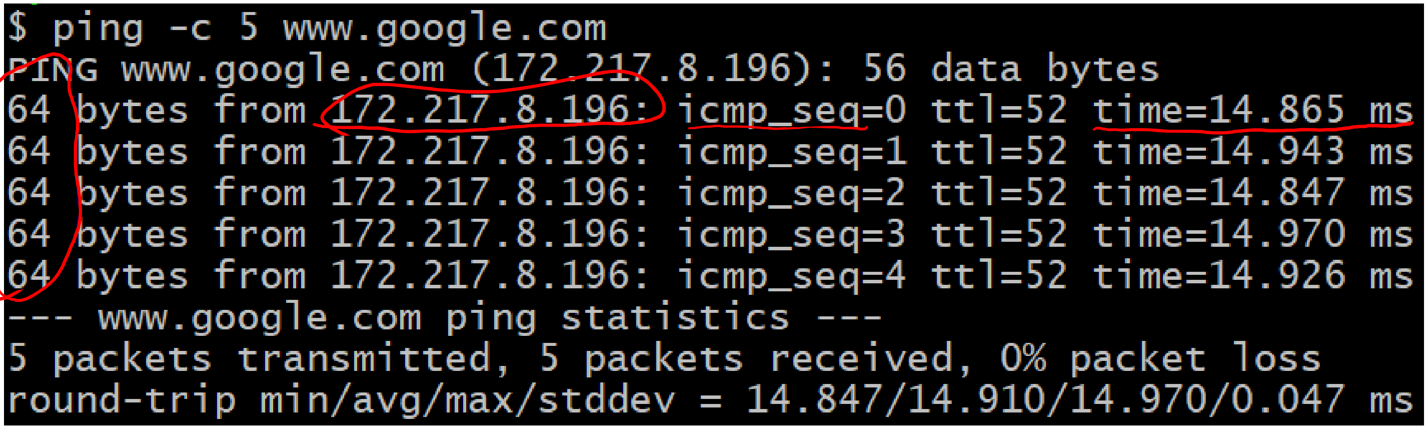
Malicious Software and Denial of service attacks

ICMP DoS Attack

Video Summary

- Ping Test
- Simple Ping Flooding Attack
- Source Address Spoofing

Ping Test



```
$ ping -c 5 www.google.com
PING www.google.com (172.217.8.196): 56 data bytes
64 bytes from 172.217.8.196: icmp_seq=0 ttl=52 time=14.865 ms
64 bytes from 172.217.8.196: icmp_seq=1 ttl=52 time=14.943 ms
64 bytes from 172.217.8.196: icmp_seq=2 ttl=52 time=14.847 ms
64 bytes from 172.217.8.196: icmp_seq=3 ttl=52 time=14.970 ms
64 bytes from 172.217.8.196: icmp_seq=4 ttl=52 time=14.926 ms
--- www.google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 14.847/14.910/14.970/0.047 ms
```

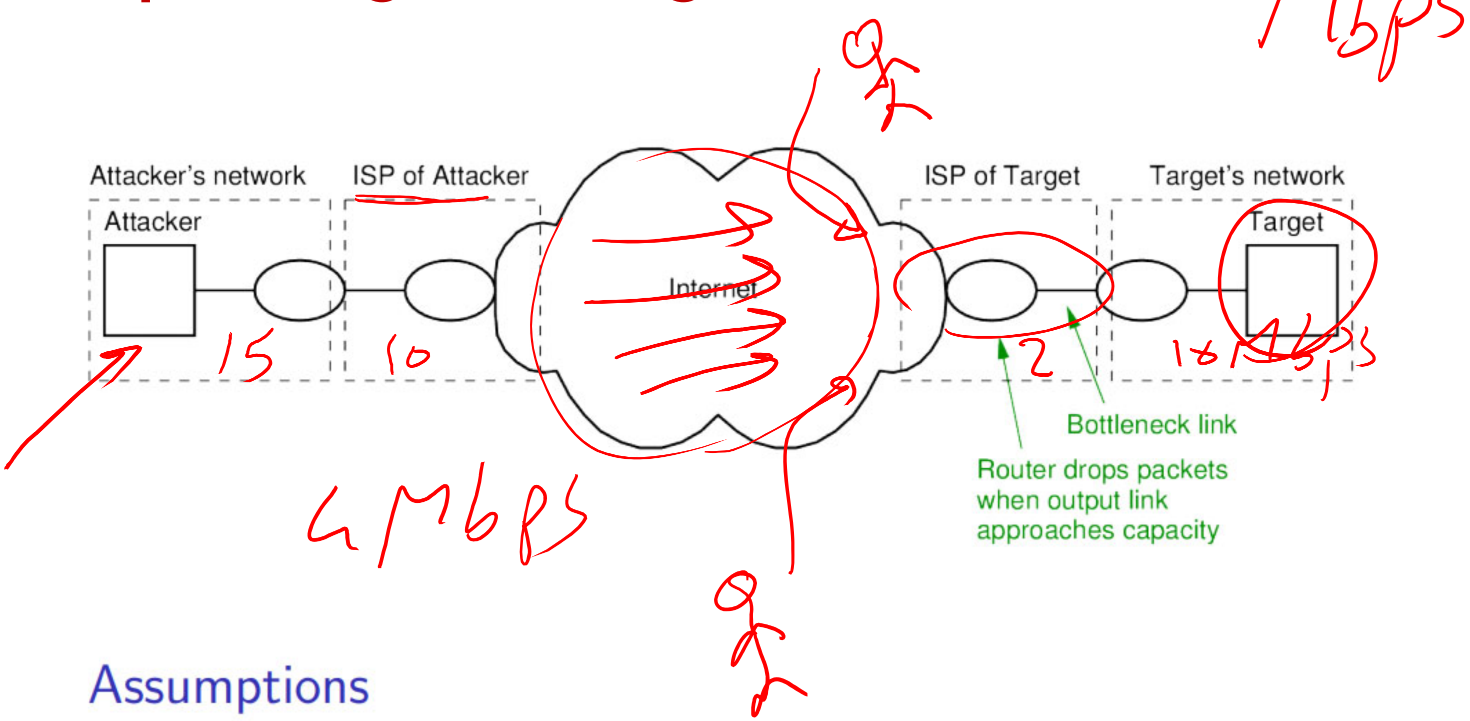
ICMP (Internet Control Message Protocol) is an error-reporting protocol network devices like routers use to generate error messages to the source IP address.

Ping uses the Internet Control Message Protocol (ICMP) to generate requests and handle responses.

ICMP is an error-reporting protocol network devices like routers use to generate error messages to the source IP address and also it is used to measure delay

Advantage: most computers will respond to the ping request

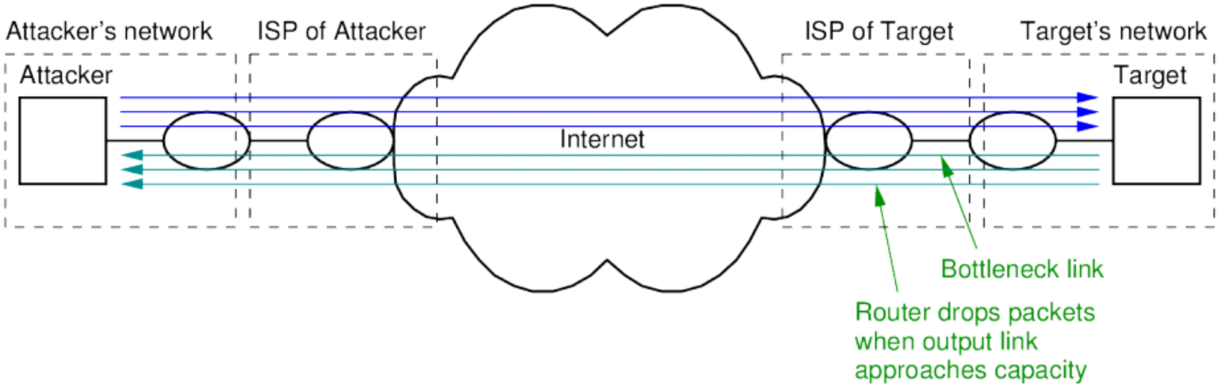
Simple Ping Flooding Attack



Assumptions

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

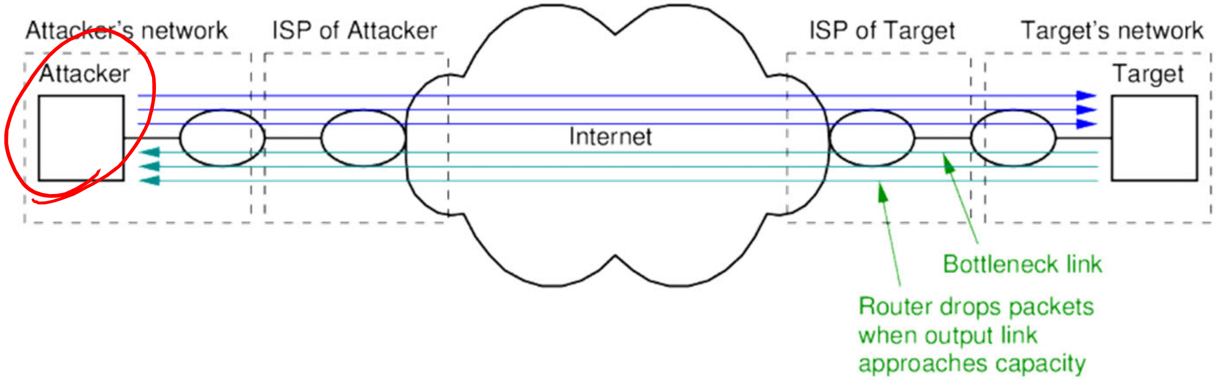
Simple Ping Flooding Attack



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

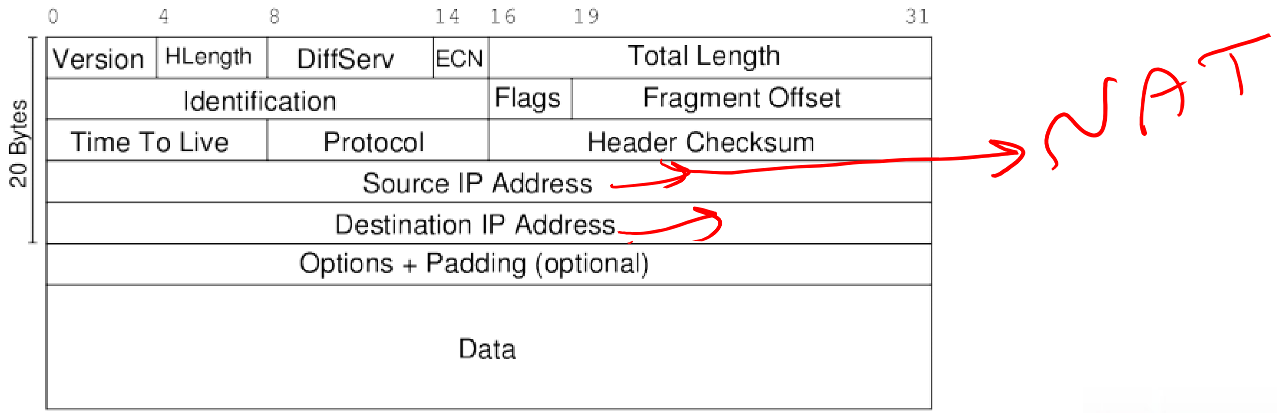


Countermeasures

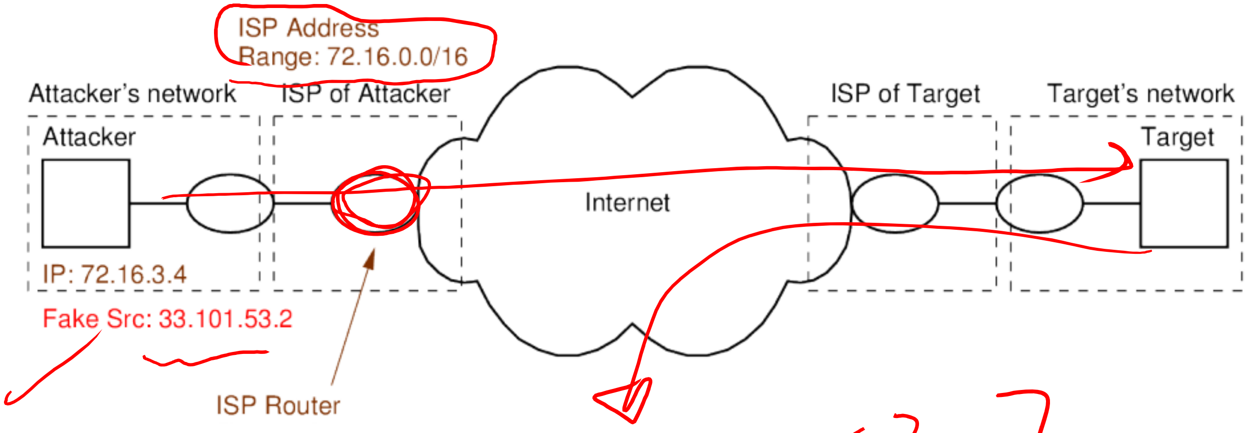
- ISPs block ping (ICMP) packets
- Target can identify the source: inform ISP, take legal action
- ICMP responses sent back to attacker, affecting their network performance

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

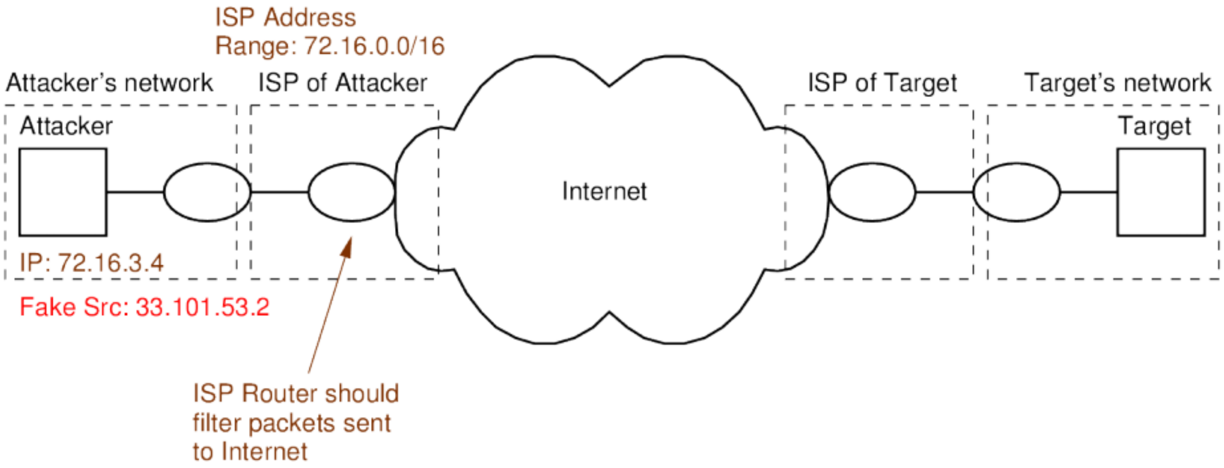


Source Address Spoofing



33.101.53.2

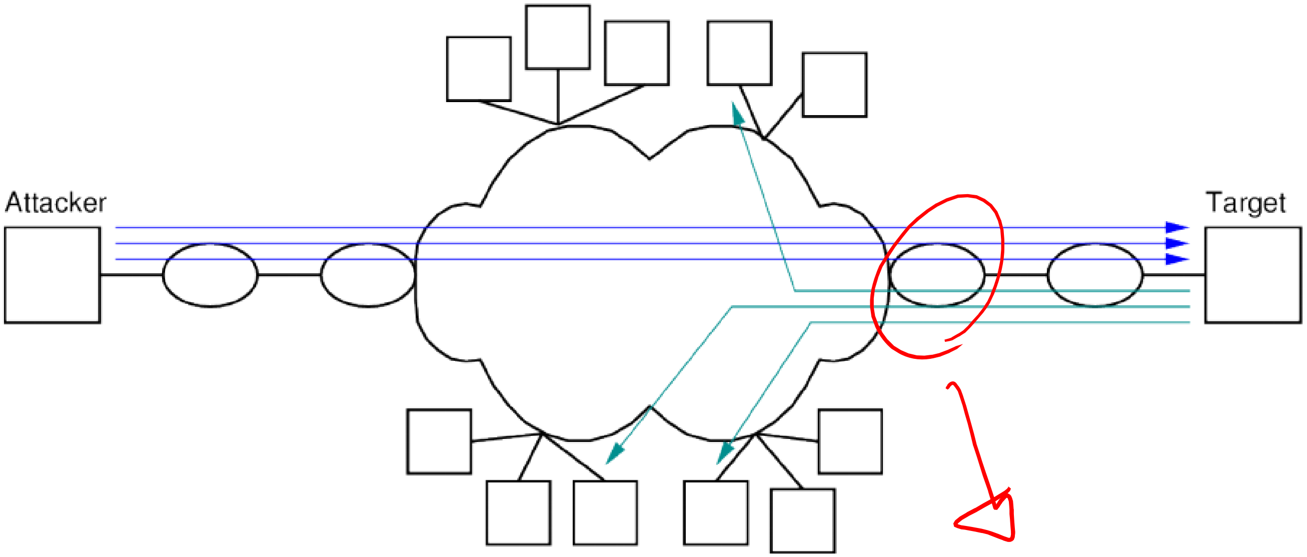
Source Address Spoofing



Countermeasure

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

Source Address Spoofing



1GPS

Simple Ping Flooding Attack

- **How we can send pings at a rate that exceeds 1 Gbps to a certain webserver?**

Ping Request: by default it sends one packet per second and its size is 64 bytes (8 header and 56 payload)

1000 Bytes

bit/sec

$$\text{Pings/sec} = \frac{1\times10^9}{1000\times8} = 125000$$

$-i \quad \frac{1}{125000}$

Simple Ping Flooding Attack

- **How we can send pings at a rate that exceeds 1 Gbps to a certain webserver?**

Ping Request: by default it sends one packet per second and its size is 64 bytes (8 header and 56 payload)

Let’s say we will change the size of the packet to be 1000 bytes

How many pings/sec to get 1 Gbps?

Pings/sec = 1000000000/(1000 x 8) = 125000

Note that one byte = 8 bits

Video Summary

- Ping Test
- Simple Ping Flooding Attack
- Source Address Spoofing