DOS AND DDOS
Lecture 14

COMPSCI 726
Network Defence and Countermeasures

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

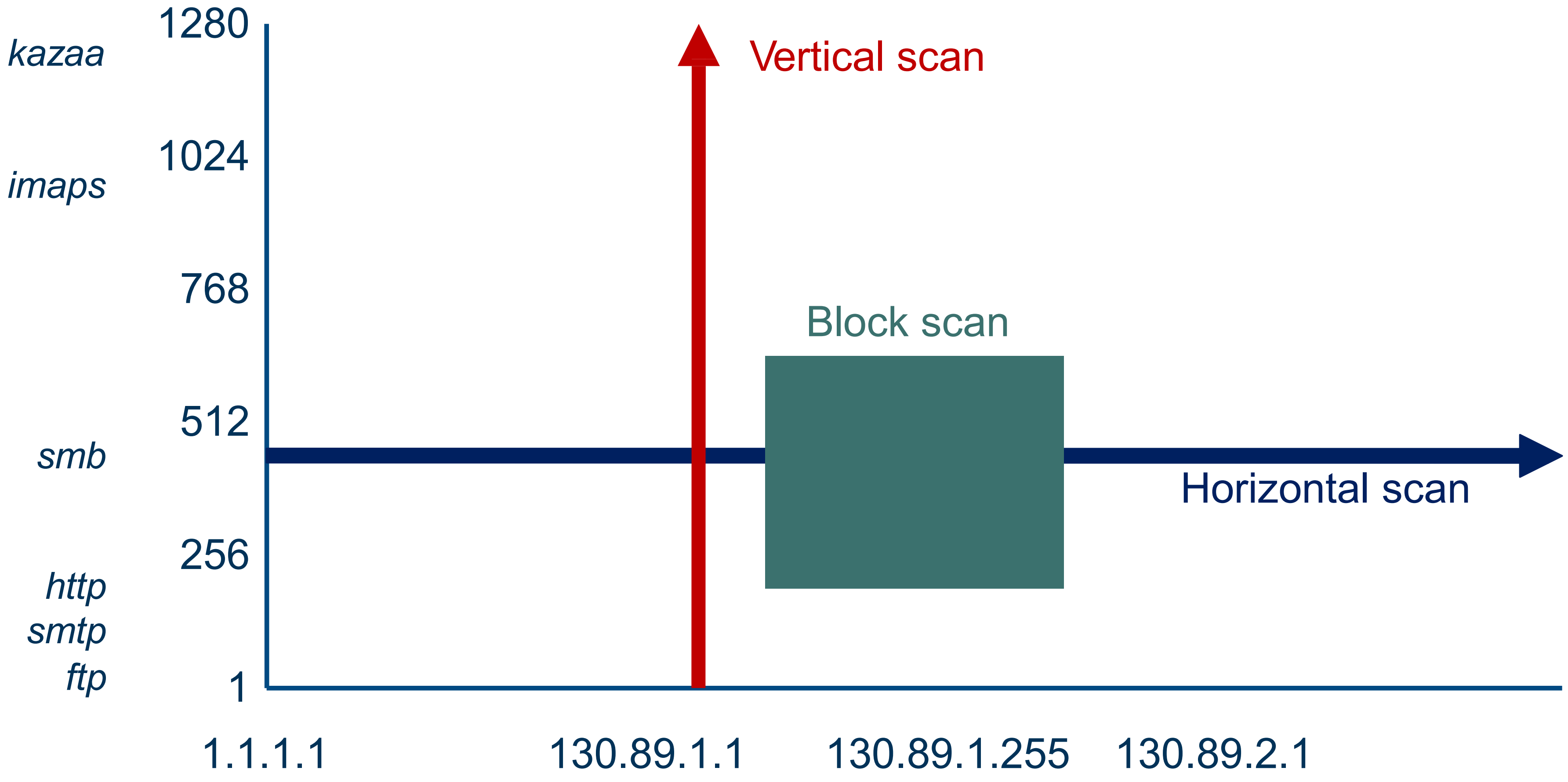
August 18, 2021

Source of some slides: **CMU**, **Stanford University**, and **University of Twente**

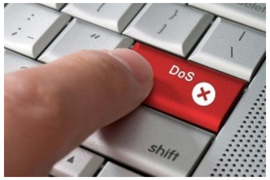
PORT SCANNING

- Scans refer to information gathering
  - Find vulnerable services/hosts
  - Discover network topology (used IP addresses)
- Can be combined with a “real” attack
  - E.g., a buffer overflow (ping of death)
- Tool for scanning
  - nmap

SCAN TYPES

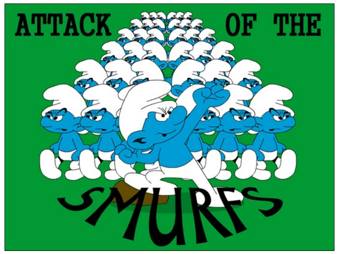

kazaa
imaps
smb
http
smtp
ftp
1280
1024
768
512
256
1
Vertical scan
Block scan
Horizontal scan
1.1.1.1
130.89.1.1
130.89.1.255
130.89.2.1

DENIAL OF SERVICE (DOS) ATTACK



- Crashing the server to make it unavailable
- Types
  - Brute-forcing
    - Send a lot of data (overload network), multiple queries (overload CPU), ...
  - Semantic
    - Exploit vulnerability (buffer overflow, …)
    - Send heavy requests (triggering complex operations)
- DoS can be applicable to any layer in the OSI model!
- Distributed DoS (DDoS)
  - Wide spread DoS

SMURF ATTACK



- Spoofed IP packets containing ICMP echo request
  - Source: Victim’s IP
  - Destination: Broadcast address

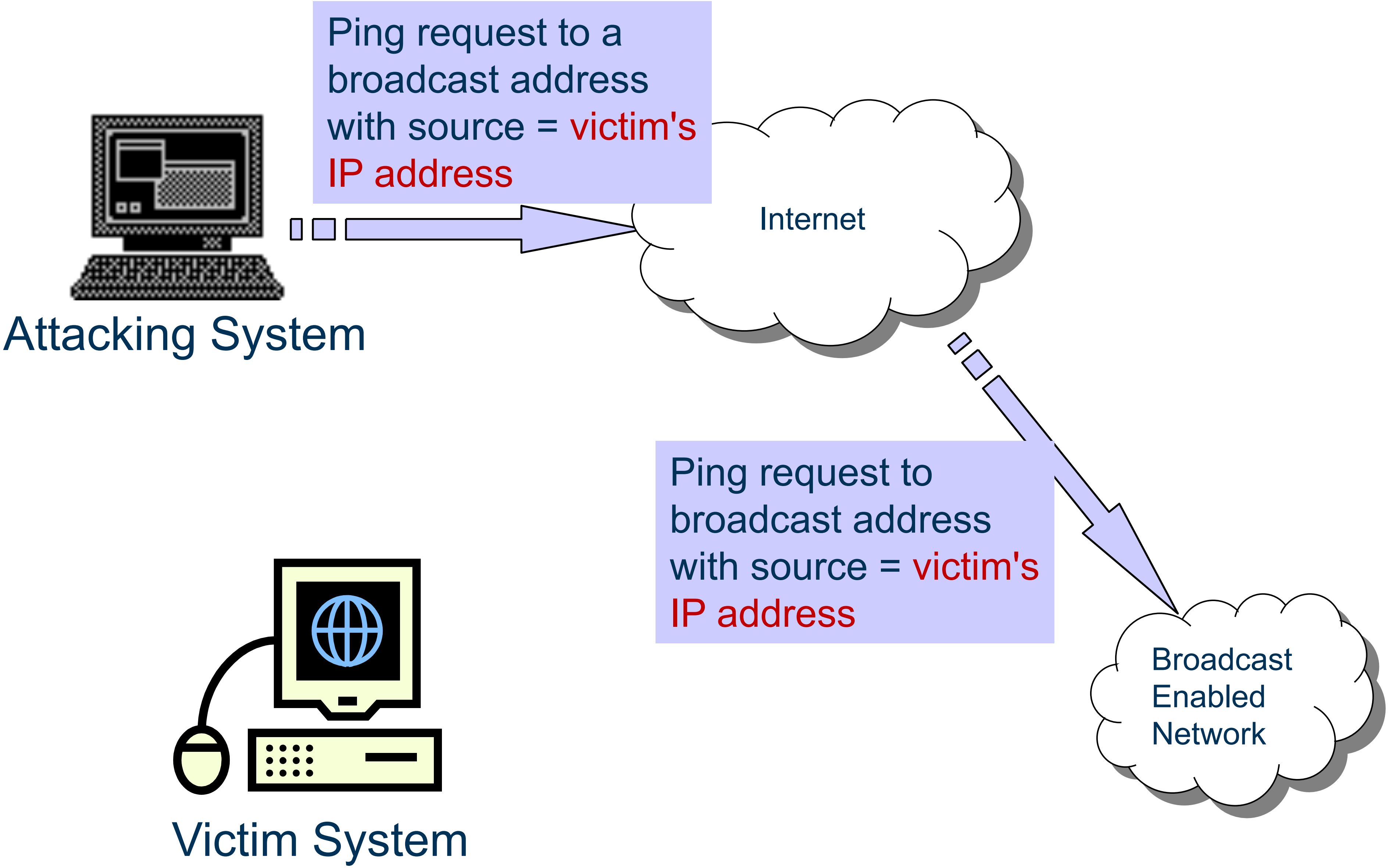
- Results in triggering all hosts included in the network to respond with ICMP response packets

- Saturates the network with bogus traffic and delays

- Prevents legitimate traffic from reaching its destination

- An example of reflected attack

SMURF ATTACK



Ping request to a broadcast address with source = victim's IP address

Attacking System

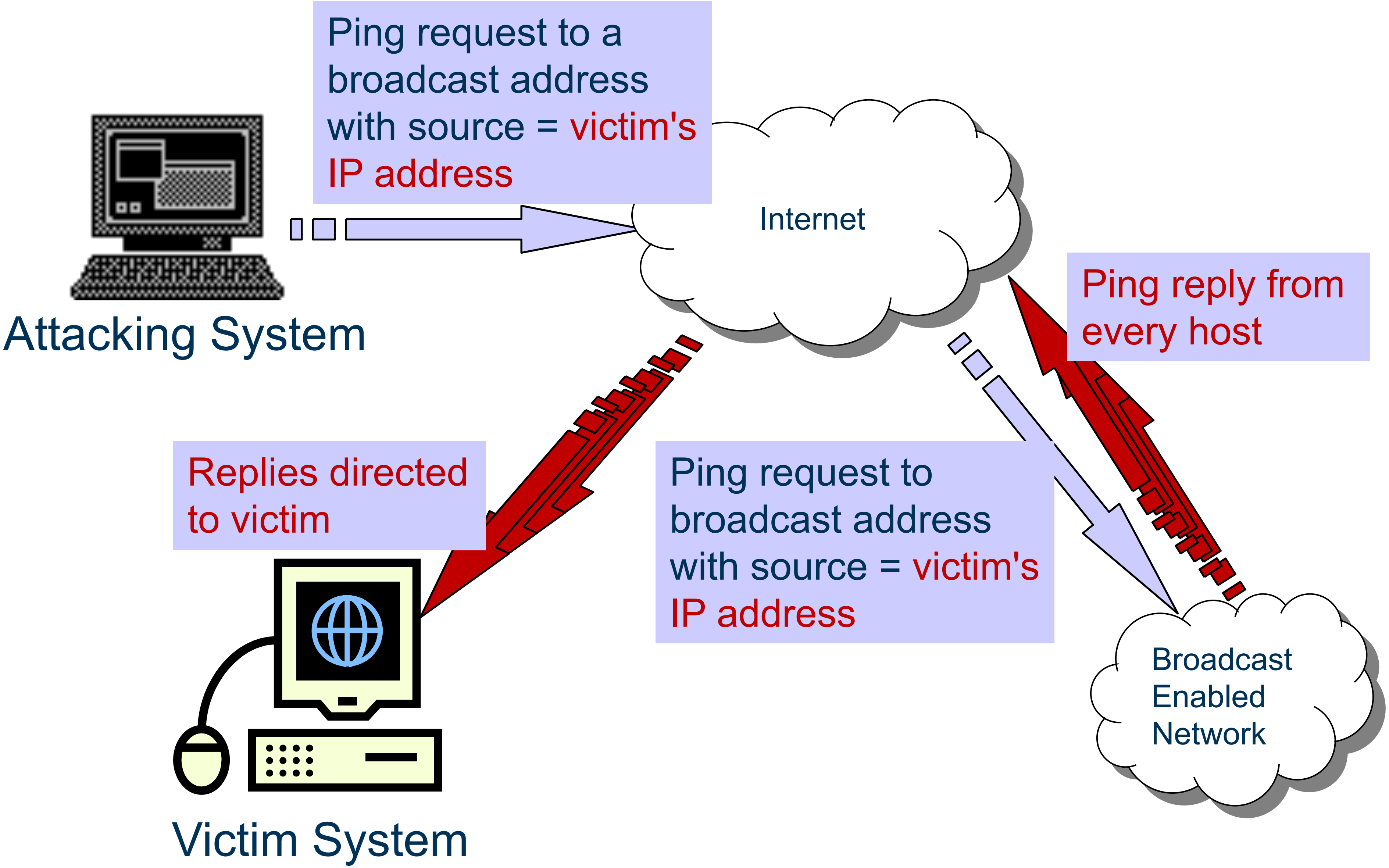
Internet

Ping request to broadcast address with source = victim's IP address

Broadcast Enabled Network

Victim System

SMURF ATTACK



Ping request to a broadcast address with source = victim's IP address

Internet

Attacking System

Ping reply from every host

Replies directed to victim

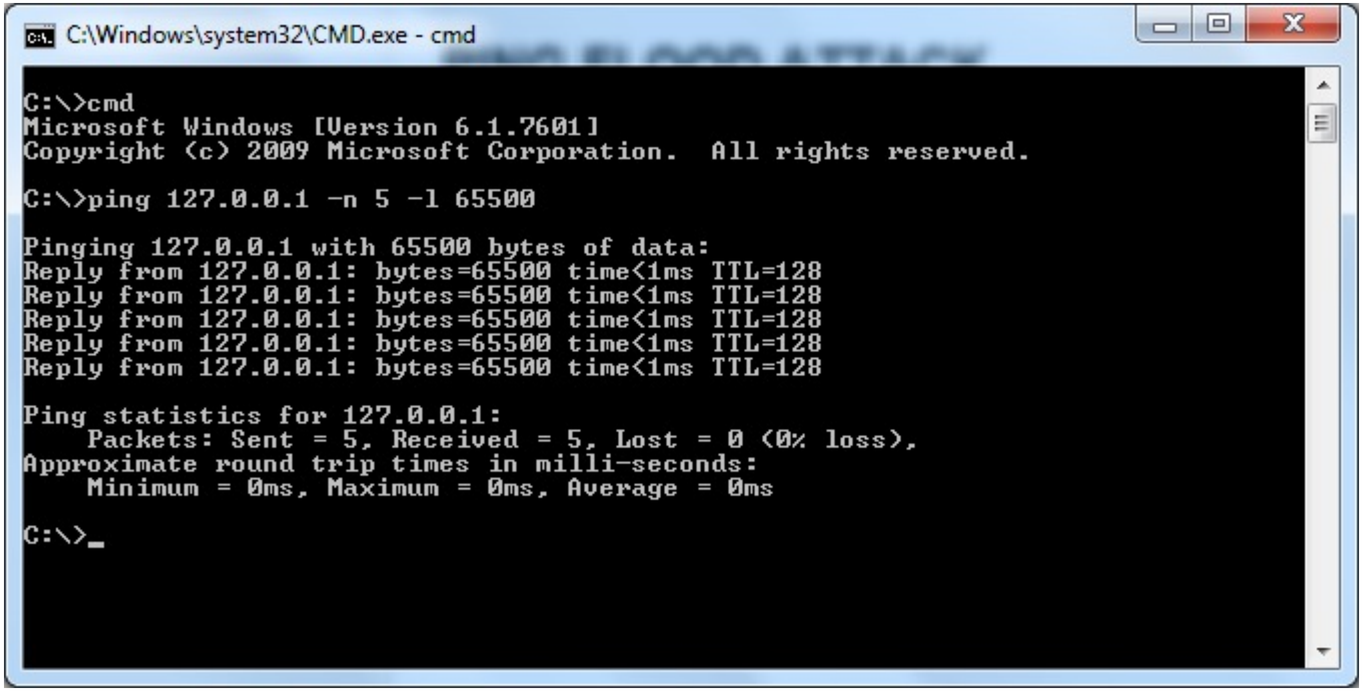
Ping request to broadcast address with source = victim's IP address

Broadcast Enabled Network

Victim System

PING FLOOD ATTACK

- Ping of death
- Over-sized packets to crash (or reboot) the system

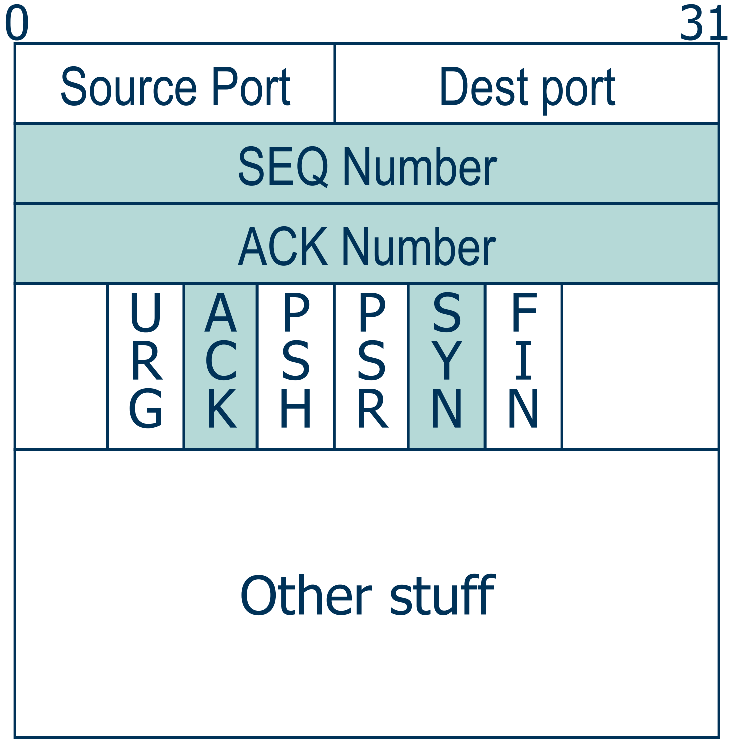


```
C:\>cmd
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ping 127.0.0.1 -n 5 -l 65500

Pinging 127.0.0.1 with 65500 bytes of data:
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128
Reply from 127.0.0.1: bytes=65500 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 5, Received = 5, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\>_
```

- Issue: Attacker could easily be identified

REVIEW: TCP HEADER FORMAT

- TCP
  - Session based
  - Congestion control
  - In order delivery



0 31

Source Port Dest port

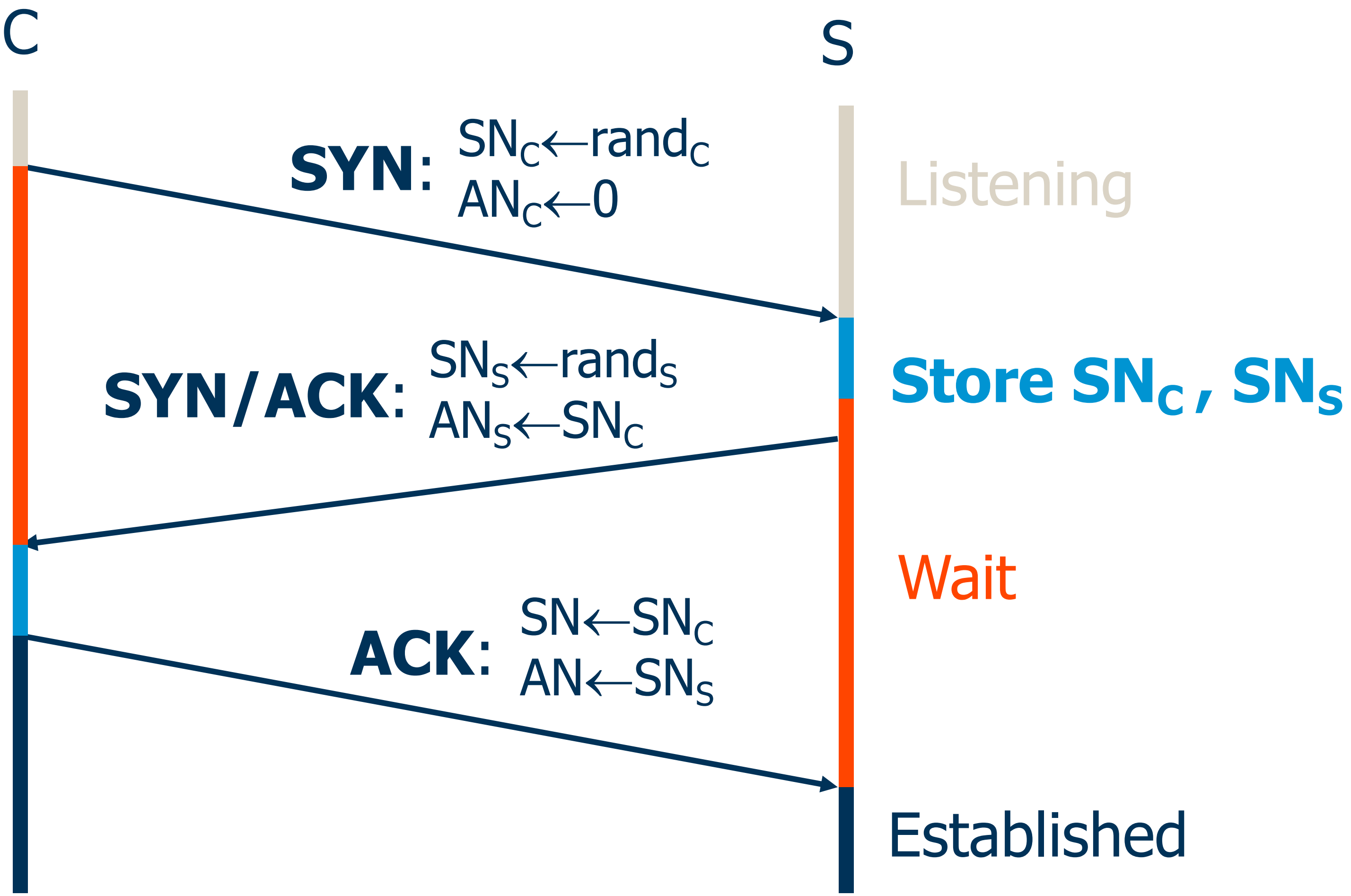
SEQ Number

ACK Number

URG ACK PSH PSR SYN FIN

Other stuff

REVIEW: TCP HANDSHAKE


C
S
SYN: $SN_C \leftarrow rand_C$
$AN_C \leftarrow 0$
Listening
SYN/ACK: $SN_S \leftarrow rand_S$
$AN_S \leftarrow SN_C$
Store SN_C , SN_S
Wait
ACK: $SN \leftarrow SN_C$
$AN \leftarrow SN_S$
Established

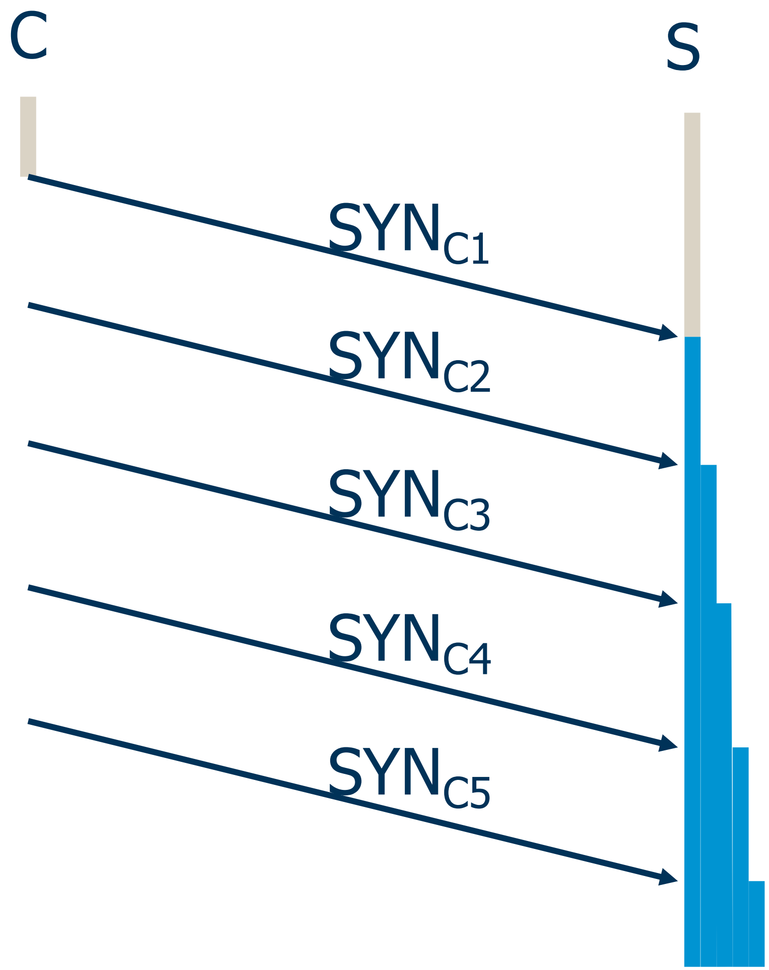
TCP SYN FLOOD

- Attacker sends many connection requests with spoofed source addresses

- Victim allocates resources for each request
  - New thread, connection state maintained until timeout
  - Fixed bound on half-open connections

- Once resources exhausted, requests from legitimate clients are denied

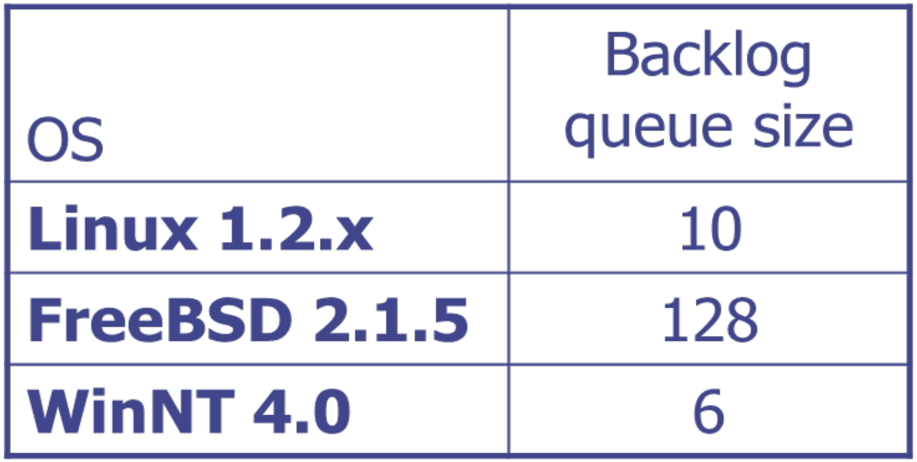
TCP SYN FLOOD



Single machine:

- SYN packets with **Random source IP addresses**
- Fills up backlog queue on server
- No further connections possible

TCP SYN FLOOD



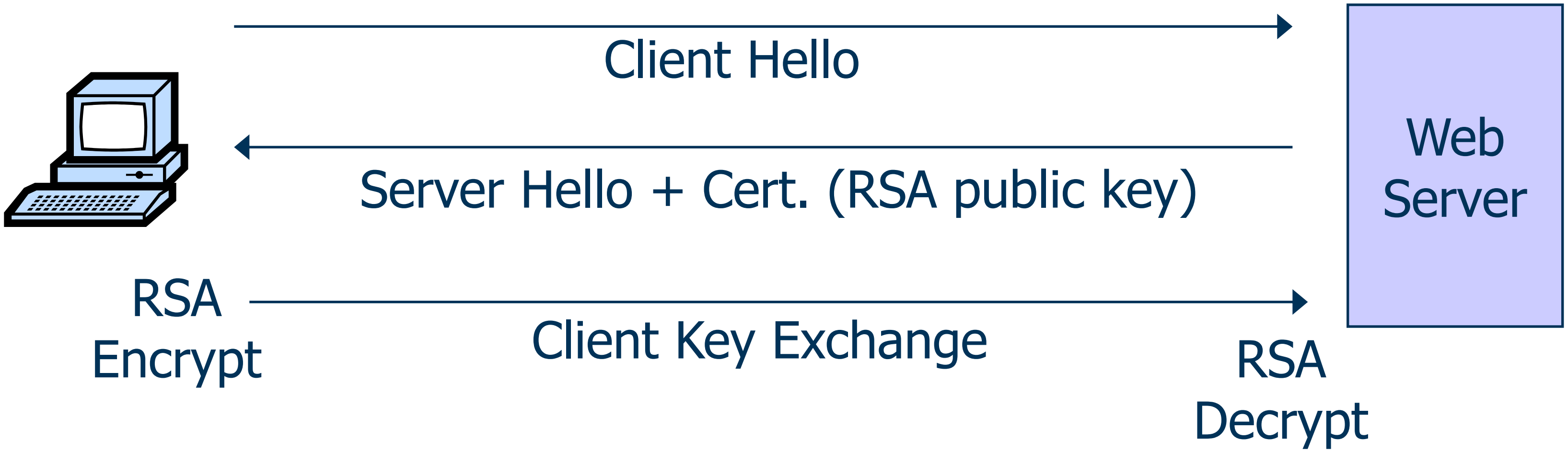
OS	Backlog queue size
Linux 1.2.x	10
FreeBSD 2.1.5	128
WinNT 4.0	6

Backlog timeout: 3 minutes

⇒ Attacker needs only to send 128 SYN packets every 3 minutes

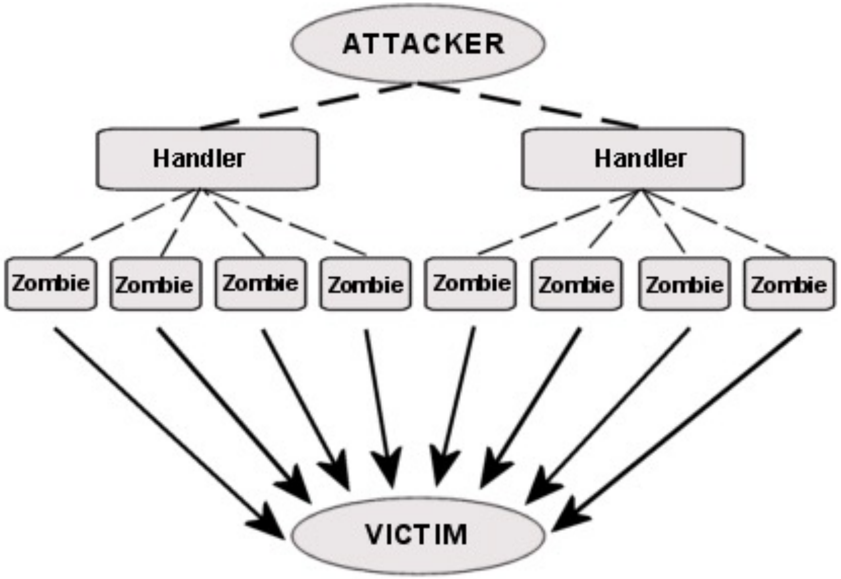
⇒ Low rate SYN flood

SSL/TLS HANDSHAKE



- RSA encrypt is 10× faster than RSA decrypt
- ⇒ Single machine can bring down 10 web servers

DDOS ATTACK



- Attacker **takes over** machines via viruses and launches DoS attacks from these “**zombies**” or “bots”

- Larger botnets can have **million of bots**

- Sustainability of botnets
  - Many owners are **unaware** that their machine is a zombie
  - Owners are **not motivated to patch** their machines to protect against malware in the absence of perceived harm

DNSSEC AND DDOS

- Amplification and reflection attacks
- See lecture slides on DNSSEC

TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!