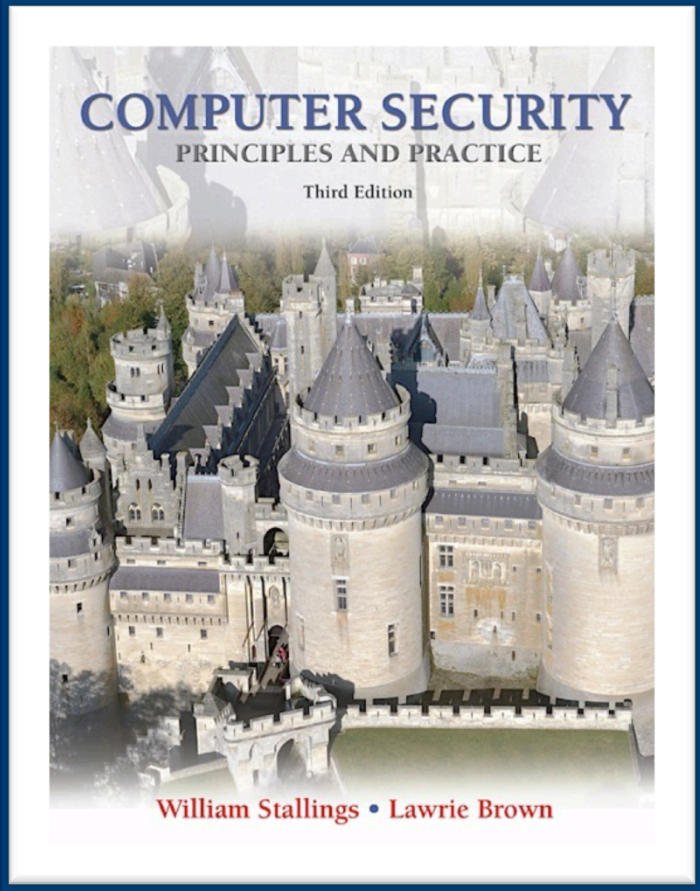
Lecture 17
Denial of Service Attacks



modified from slides of Lawrie Brown

Denial-of-Service (DoS) Attack

- DoS: a form of attack on the availability of some service
- In the context of computer and communication security, it focuses on **network services** that are attacked over their **network connection**
- Different from attacks that cause damage or deconstruction of IT infrastructure

Denial-of-Service (DoS) Attack

- The NIST Computer Security Incident Handling Guide defines a DoS attack as:

"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."

Denial-of-Service (DoS)

- a form of attack on the availability of some service
- categories of resources that could be attacked are:

network bandwidth

- relates to the capacity of the network links connecting a server to the Internet
- for most organizations this is their connection to their Internet Service Provider (ISP)

system resources

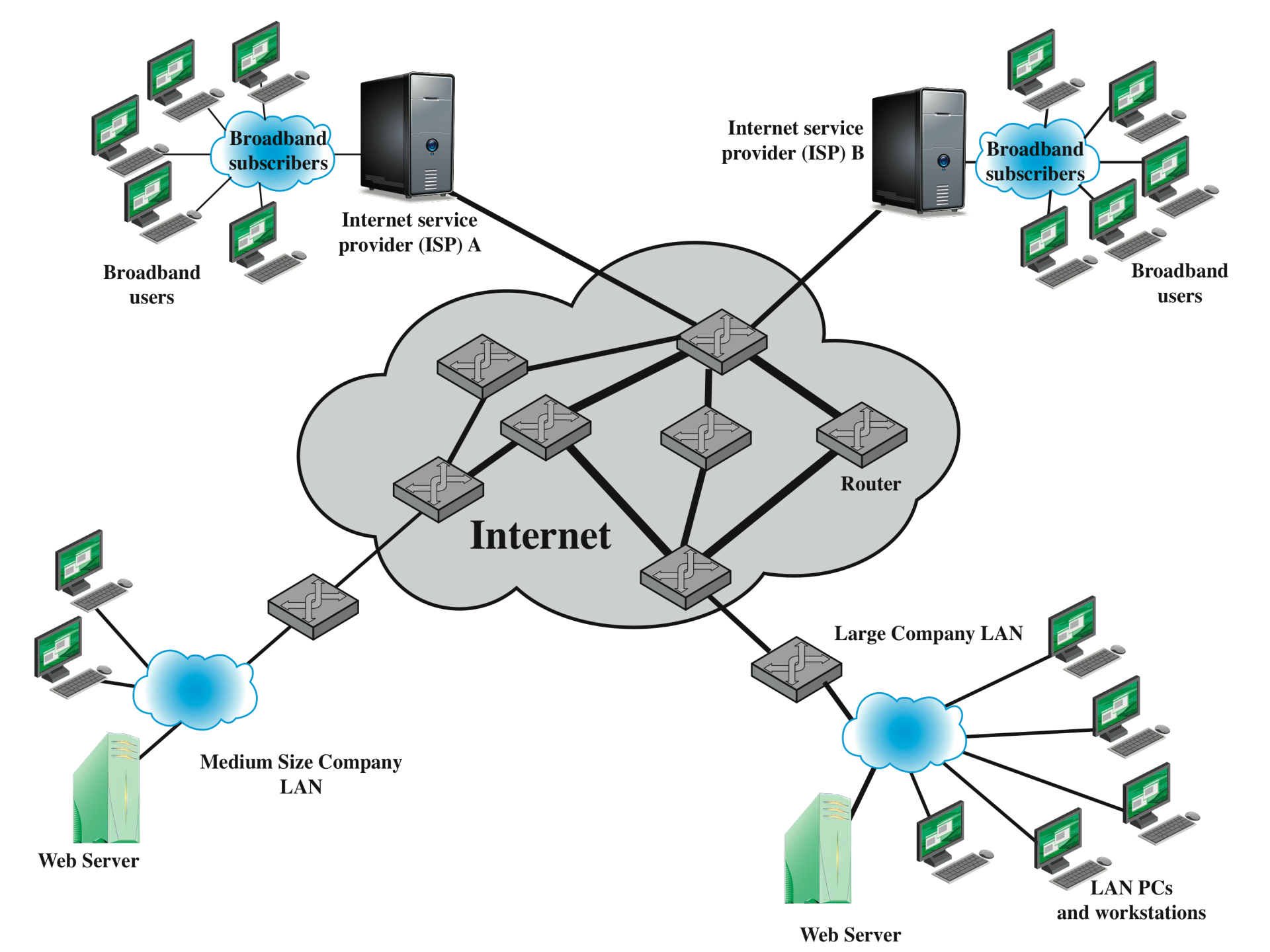
- aims to overload or crash the network handling software

application resources

- typically involves a number of valid requests, each of which consumes significant resources, thus limiting the ability of the server to respond to requests from other users

Denial-of-Service (DoS)

- Network bandwidth
  - The capacity of the network links connecting a server to the wider Internet
  - For most organizations, this is their connection to their Internet service provider (ISP)
  - Usually this connection will have a lower capacity than the links within and between ISP routers--**it is possible for more traffic to arrive at the ISP's routers over these higher-capacity links than can be carried over the link to the organization**


Broadband subscribers
Broadband users
Internet service provider (ISP) A
Internet service provider (ISP) B
Broadband subscribers
Broadband users
Internet
Router
Medium Size Company LAN
Web Server
Large Company LAN
LAN PCs and workstations
Web Server

Denial-of-Service (DoS)

- Network bandwidth attack
- System resource attack
- Application resource attack

Denial-of-Service (DoS)

- Network bandwidth Attack
  - the router must discard some packets, delivering only as many as can be handled by the link (between ISP and organizations)
  - A random portion of these organizations/users will experience a degraded or nonexistent service as a consequence
  - Attack happens when malicious traffic overwhelms legitimate traffic on limited network bandwidth

Denial-of-Service (DoS)

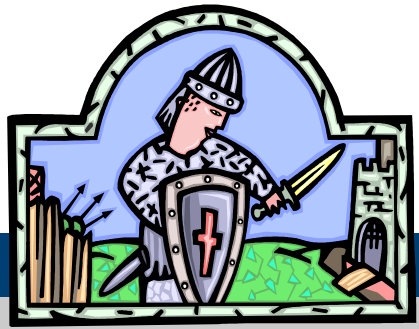
- System resource attack
  - Rather than consuming bandwidth with large volumes of traffic, specific types of packets are sent to consume the limited resource at the system
  - SYN spoofing attack: targets at the table of TCP connections on the server
  - Poison packet: uses packets whose structure triggers a bug in the system's software, causing it to crash

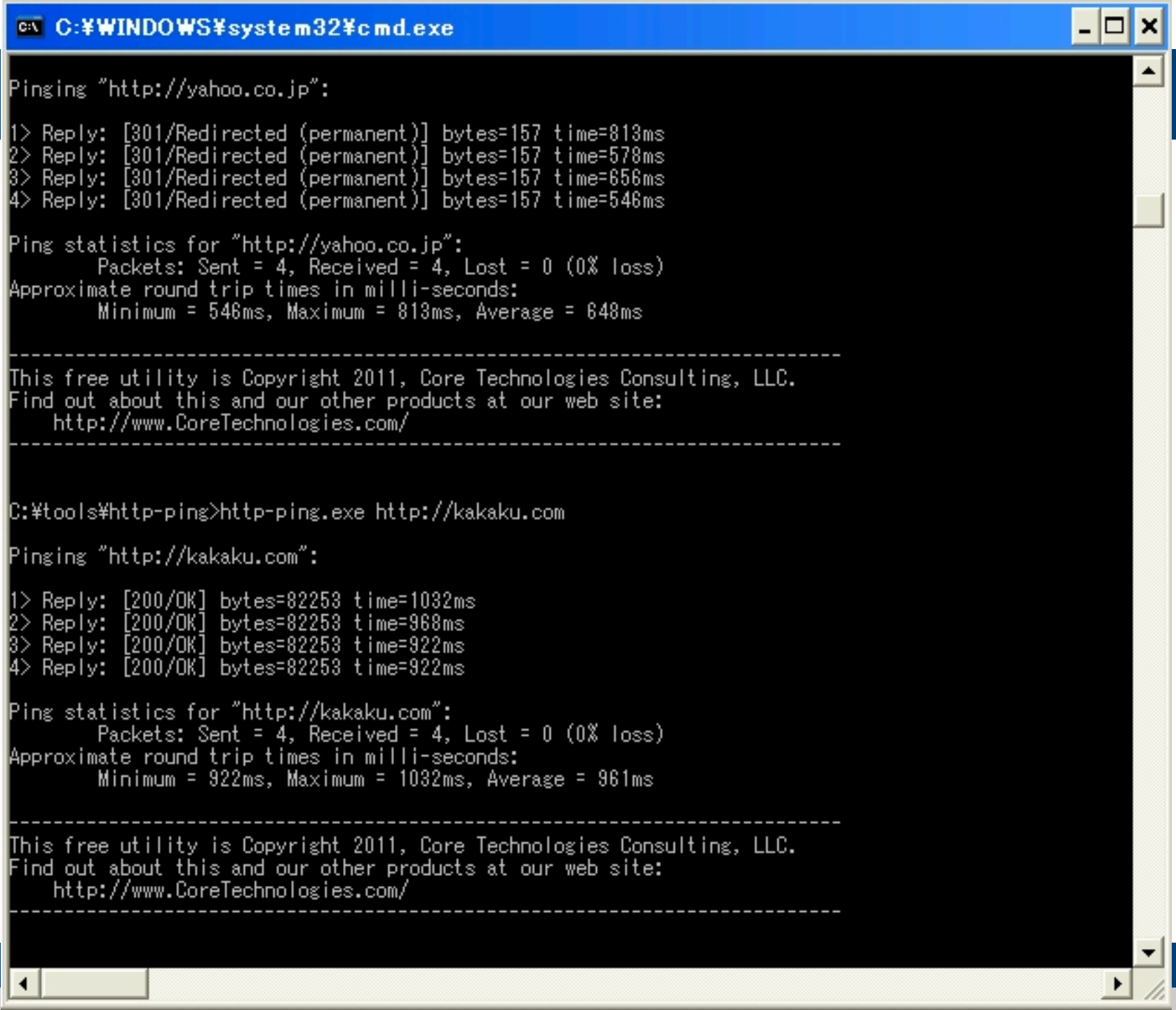
Denial-of-Service (DoS)

- Application resource attack
  - An attack on a specific application, such as a Web server, typically involves a number of valid requests, each of which consumes significant resources
  - This then limits the ability of the server to respond to requests from other users

Classic Denial-of-Service Attacks

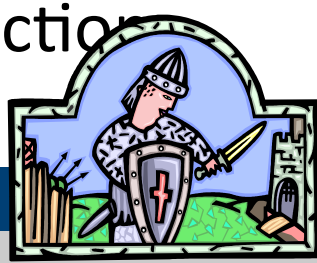
- flooding ping command
  - "Ping" a common command to test the connectivity to the specific destination
  - It sends TCP/IP ICMP echo request packets to the destination, and measures the time taken for the echo response packet to return
  - Usually they are sent at controlled rate; however, the flood ping allow them to be sent as fast as possible




C:¥WINDOWS¥system32¥cmd.exe
Pinging "http://yahoo.co.jp":
1> Reply: [301/Redirected (permanent)] bytes=157 time=813ms
2> Reply: [301/Redirected (permanent)] bytes=157 time=578ms
3> Reply: [301/Redirected (permanent)] bytes=157 time=656ms
4> Reply: [301/Redirected (permanent)] bytes=157 time=546ms
Ping statistics for "http://yahoo.co.jp":
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 546ms, Maximum = 813ms, Average = 648ms
This free utility is Copyright 2011, Core Technologies Consulting, LLC.
Find out about this and our other products at our web site:
http://www.CoreTechnologies.com/
C:¥tools¥http-ping>http-ping.exe http://kakaku.com
Pinging "http://kakaku.com":
1> Reply: [200/OK] bytes=82253 time=1032ms
2> Reply: [200/OK] bytes=82253 time=968ms
3> Reply: [200/OK] bytes=82253 time=922ms
4> Reply: [200/OK] bytes=82253 time=922ms
Ping statistics for "http://kakaku.com":
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
Minimum = 922ms, Maximum = 1032ms, Average = 961ms
This free utility is Copyright 2011, Core Technologies Consulting, LLC.
Find out about this and our other products at our web site:
http://www.CoreTechnologies.com/

Classic Denial-of-Service Attacks

- flooding ping command
  - aim of this attack is to overwhelm the capacity of the network connection to the target organization
  - The attack can be as simple as using a flooding ping command directed at the Web server in the target company—the target server needs to reply every ping request it receives
  - the attacker has access to a system with a higher-capacity network connection, and the target only has access to lower-capacity network connection—why?



Classic Denial-of-Service Attacks

- flooding ping command
  - When the attack is success, the ping requests from valid users cannot be answered--DoS
  - source of the attack is clearly identified in the ICMP echo (ping) request—leading to two disadvantages from the attacker's perspective
    - Since the source of the attacker is specified (required), it can be easily traced
    - The target system will respond to every ping request it receives, resulting large volume of responses at the attacker

Classic DoS Attack

ICMP packet

	Bit 0 - 7	Bit 8 - 15	Bit 16 - 23	Bit 24 - 31
IP Header (20 bytes)	Version/IHL	Type of service	Length	
	Identification		*flags* and *offset*	
	Time To Live (TTL)	Protocol	Checksum	
	Source IP address			
	Destination IP address			
ICMP Payload (8+ bytes)	Type of message	Code	Checksum	
	Quench			
	Data (*optional*)			

Source Address Spoofing

- A common characteristic of packet used in many types of DoS attacks is the use forged source addresses
  - usually via the raw socket interface on operating systems
  - makes attacking systems harder to identify
- attacker generates large volumes of packets that have the target system as the destination address
- congestion would result in the router connected to lower capacity link

Source Address Spoofing

- the ICMP echo response packets would no longer be reflected back to the source (attacker) system—scattered across the Internet
- Why such easy forgery of source addresses is allowed on the Internet?
  - It dates back to the development of TCP/IP, which occurred in a generally cooperative and trusting environment

Source Address Spoofing

- The useful side effect of the scattered response packets due to the attack—to monitor and analyze the type and scale of attacks being used
  - Honeynet/Honeypot: servers take blocks of unused IP addresses, used to collect and analyze any packets sent to these addresses.
  - Since no real systems use these addresses, no legitimate packets should be directed to them. Any packets received might simply be corrupted. It is much more likely that they are the direct or indirect result of network attacks.

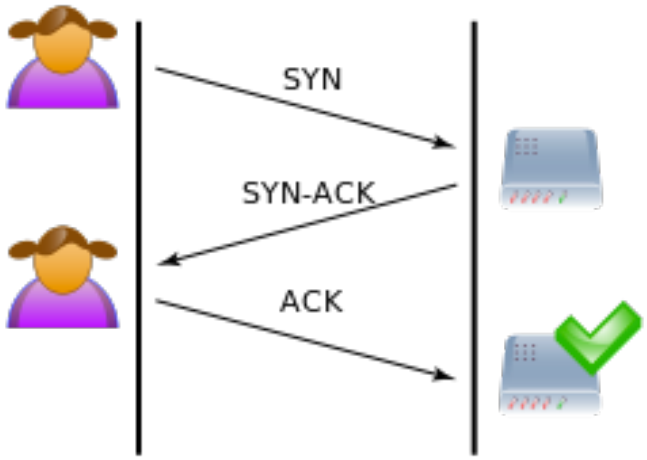
Exercise

- In order to implement classic DoS flood attack, the attacker must generate a sufficiently large volume of packets to exceed the capacity of the link to the target organization. Consider an attack using ICMP echo request (Ping) packets that are 500 bytes in size. How many packets per second the attacker send to flood a target organization using a 0.5 Mbps link? How many per second if the attacker uses a 2 Mbps link? Or a 10 Mbps link?

SYN Spoofing

- Common DoS attack
- Attacks the ability of a server to respond to future connection requests by **overflowing the tables** used to manage them
- Thus legitimate users are denied access to the server
- An attack on system resources

TCP Connection Handshake



- The client requests a connection by sending a SYN to the server
- The server acknowledge this request by sending a SYN-ACK back to the client
- The client responds an ACK, and the connection is established

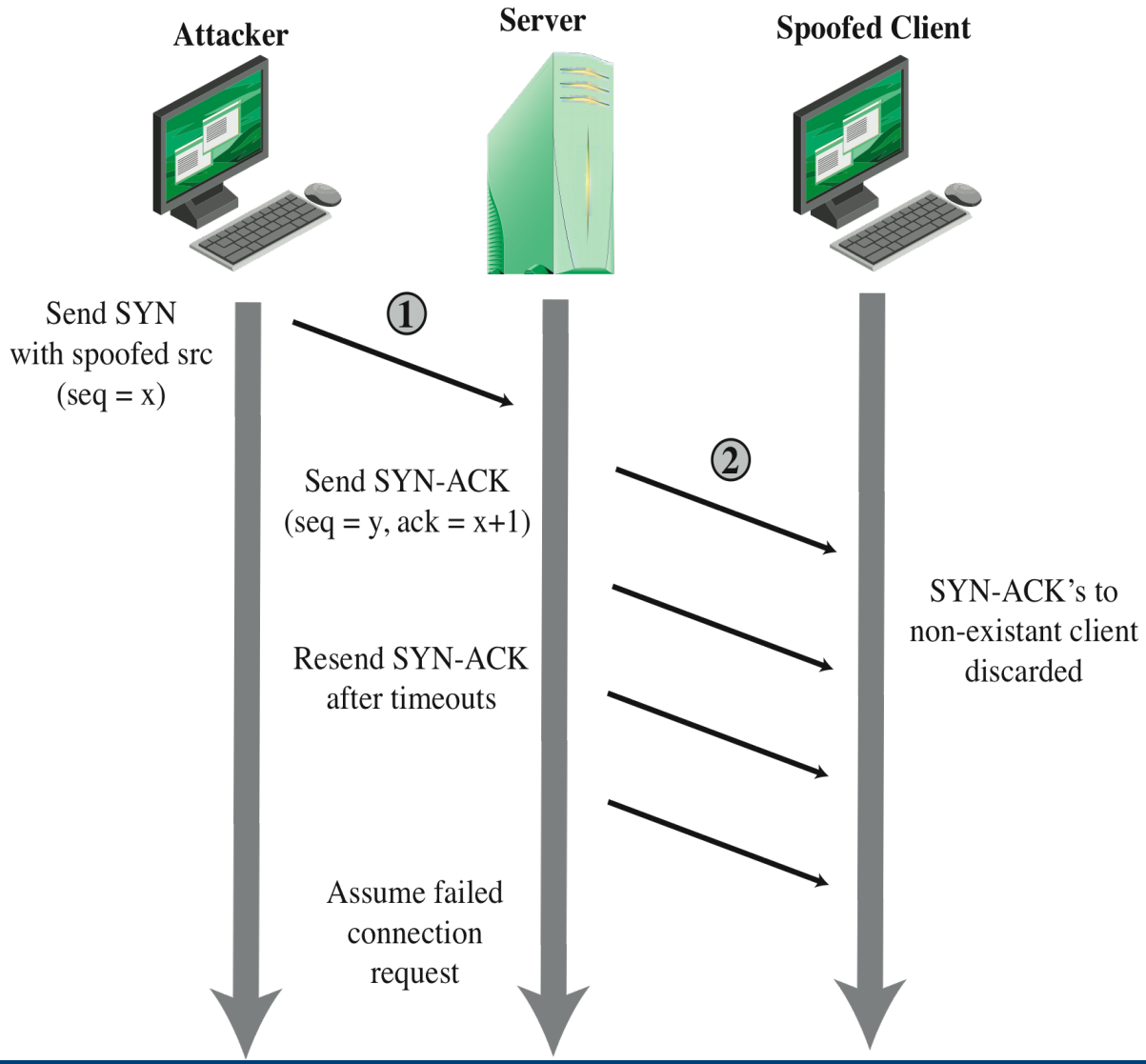
TCP SYN Spoofing Attack

- The attacker generates a number of SYN connection request packets with forged source addresses
- For each of these, the server records the details of the TCP connection request and sends the SYN-ACK packet to the claimed source address
- Since it's a faked source address, then no reply will return to the server.
- The server will resend the SYN-ACK packet a number of times until a maximal re-transmission number is reached.

TCP SYN Spoofing Attack

- Before the server determines the request has failed, the server is using an entry in its table of known TCP connections.
- Since the attacker directs a very large number of forged connection requests at the targeted server. These rapidly fill the table of known TCP connections on the server
- Once this table is full, any future requests, including legitimate requests from other users, are rejected (DoS)

TCP SYN Spoofing Attack



TCP SYN Spoofing Attack

- Difference between SYN spoofing attack and classic DoS attack
  - The actual volume of SYN traffic can be comparatively low. It simply has to be high enough to keep the known TCP connections table filled. No need for the attacker to access high capacity link
  - In classic DoS attack, attacker has to access high capacity link (necessary condition)

Exercise

- Using a TCP SYN spoofing attack, the attacker aims to flood the table of TCP connection requests on a system so that it is unable to respond to legitimate connection request. Consider a server system with a table for 256 connection requests. This system will retry sending the SYN-ACK packet 5 times when it fails to receive and ACK packet in response, at 30 second intervals, before purging the request from its table. At what rate must the attacker continue to send TCP connection requests to this system in order to ensure that the table remains full? Assuming that the TCP packet is 40 bytes in size, how much bandwidth does the attacker consume to continue this attack?