DDOS

What is DoS

A **denial of service (DoS)** is 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.

What is DoS

Several categories of resources that could be attacked:

- Network bandwidth
- System resources
- Application resources

Example

- Classic Denial-of-Service Attacks
- Source Address Spoofing
- Syn Spoofing

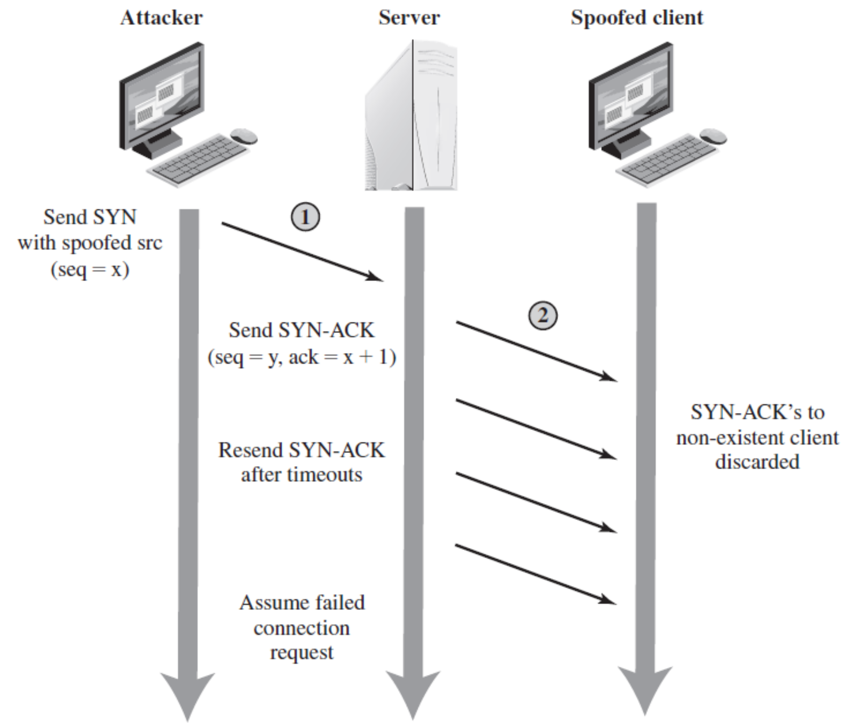

Attacker
Server
Spoofed client
Send SYN with spoofed src (seq = x)
1
Send SYN-ACK (seq = y, ack = x + 1)
2
Resend SYN-ACK after timeouts
Assume failed connection request
SYN-ACK's to non-existent client discarded

Figure 7.3 **TCP SYN SpoofingAttack**

- Flooding Attacks.
- Distributed denial-of-Service Attacks.
- Application-based bandwidth Attacks.
- Reflector and amplifier Attacks.

Flooding Attacks.

Take a variety of forms, based on which network protocol is being used to implement the attack. In all cases the intent is generally to overload the network capacity on some link to a server.

- ICMP Flood
- UDP Flood
- TCP SYN Flood

SYN-flooding Attack

- Very common denial-of-service attack, aka Neptune
- Attacker starts handshake with SYN-marked segment
- Victim replies with SYN-ACK segment
- Attacker… stays silent
  - Note that the source IP of the attacker can be spoofed, since no final ACK is required
- A host can keep a limited number of TCP connections in half-open state. After that limit, it cannot accept any more connections

SYN-flooding Attack

- Current solutions
  - Filtering
  - Increase the length of the half-open connection queue
  - Reduce the SYN-received timeout
  - Drop half-open connections when the limit has been reached and new requests for connection arrive
  - Limit the number of half-open connections from a specific source
  - Use SYN cookies
- See TCP SYN Flooding Attacks and Common Mitigations, RFC 4987

SYN Cookies

- Special algorithm used for determining the initial sequence number of the server
- The number is
  - Top 5 bits: t mod 32, where t is a 32-bit time counter that increases every 64 seconds
  - Following 3 bits: the encoding of the Maximum Segment Size (MSS) chosen by the server in response to the client's MSS
  - A keyed hash of:
    - Counter t
    - Source/Destination IP addresses and ports

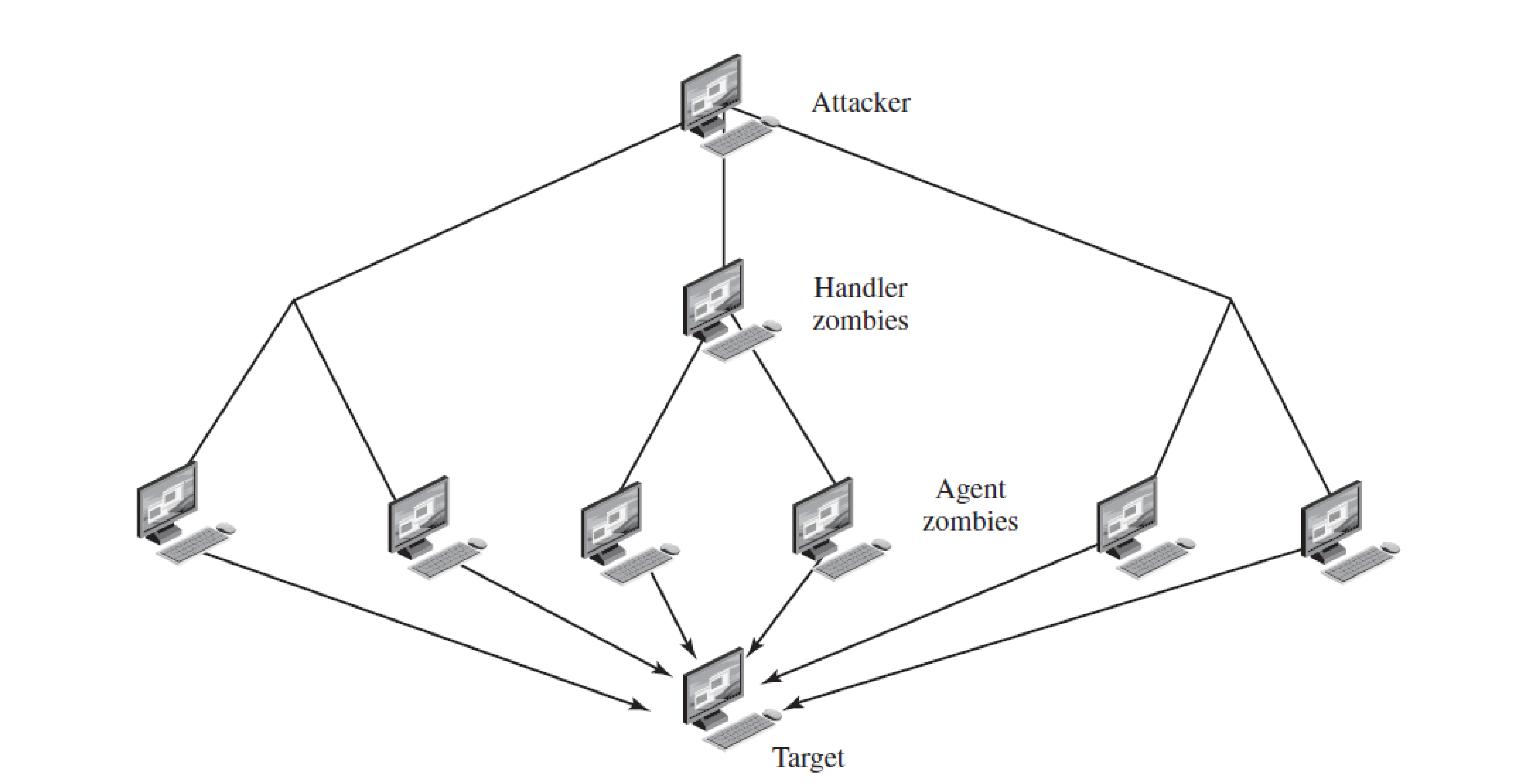
SYN Cookies

- A server that uses SYN cookies sends back a SYN+ACK, exactly as if the SYN queue had been larger
- When the server receives an ACK, it checks that the secret function works for a recent value of t, and then rebuilds the SYN queue entry (using the encoded MSS info)
- Drawbacks:
  - The server sequence number grows faster than normal
  - The MSS value is limited by the encoding procedure (only 8 possible values)
  - No data can be included in the initial SYN

Distributed denial-of-Service Attacks

- The limitations of flooding attacks generated by a single system.
- We can improve this limitations by using multiple system to generate attacks
  - These systems were typically compromised user workstations or PCs
  - The attacker uses malware to subvert the system and install an attack agent which they can control
  - Such systems are known as **zombies**

Distributed denial-of-Service Attack

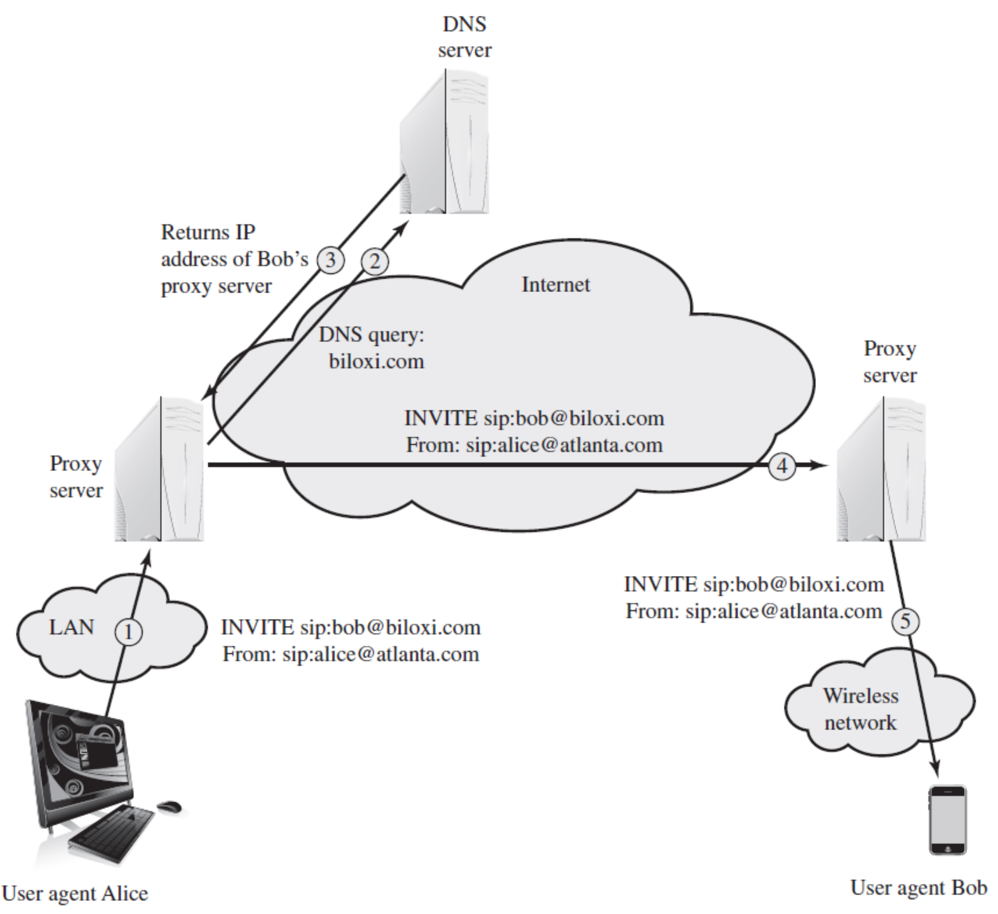


Application-based bandwidth Attacks

A potentially effective strategy for denial of service is to force the target to execute resource-consuming operations that are disproportionate to the attack effort.

- SIP Flood
- HTTP Based Attack

SIP Flood



DNS server
Returns IP address of Bob's proxy server
3
2
Internet
DNS query: biloxi.com
Proxy server
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
4
Proxy server
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
5
LAN
1
INVITE sip:bob@biloxi.com
From: sip:alice@atlanta.com
Wireless network
User agent Alice
User agent Bob

- **HTTP Flood**
  - An HTTP flood refers to an attack that bombards Web servers with HTTP requests.
  - Typically, this is a DDoS attack, with HTTP requests coming from many different bots.
- **Slowloris**
  - Exploits the common server technique of using multiple threads to support multiple requests to the same server application
  - Exhaust all of the available request handling threads on the Web server by sending HTTP requests that never complete.

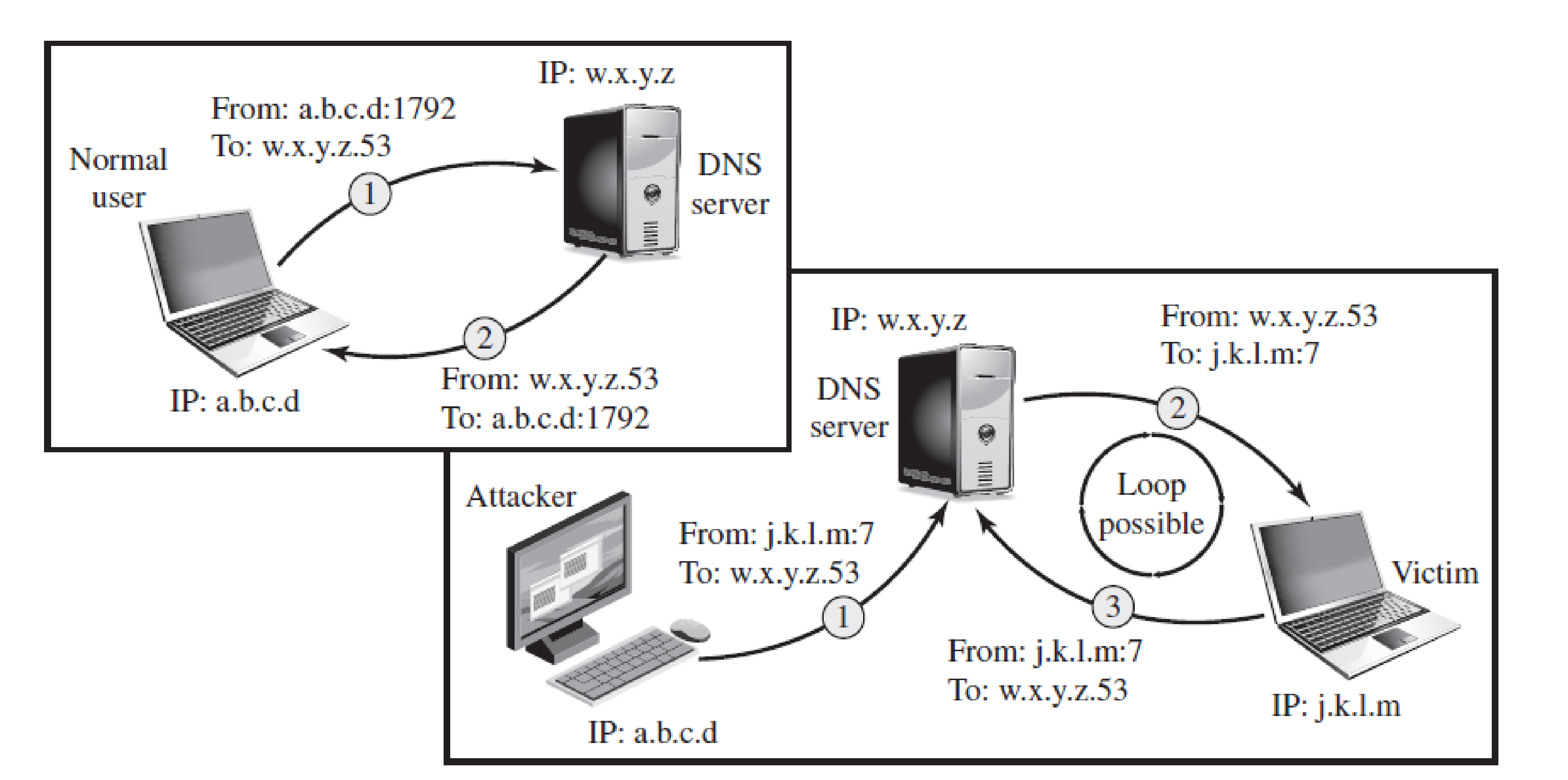
Reflector and amplifier Attacks

- Reflector and amplifier attacks use network systems functioning normally.
- The attacker sends a network packet with a spoofed source address to a service running on some network server.
- The server responds to this packet, sending it to the spoofed source address that belongs to the actual attack

Reflection Attacks

- Ideally the attacker would like to use a service that created a larger response packet than the original request.
- This allows the attacker to convert a lower volume stream of packets from the originating system into a higher volume of packet data from the intermediary directed at the target
- UDP, ICMP, DNS, SNMP …

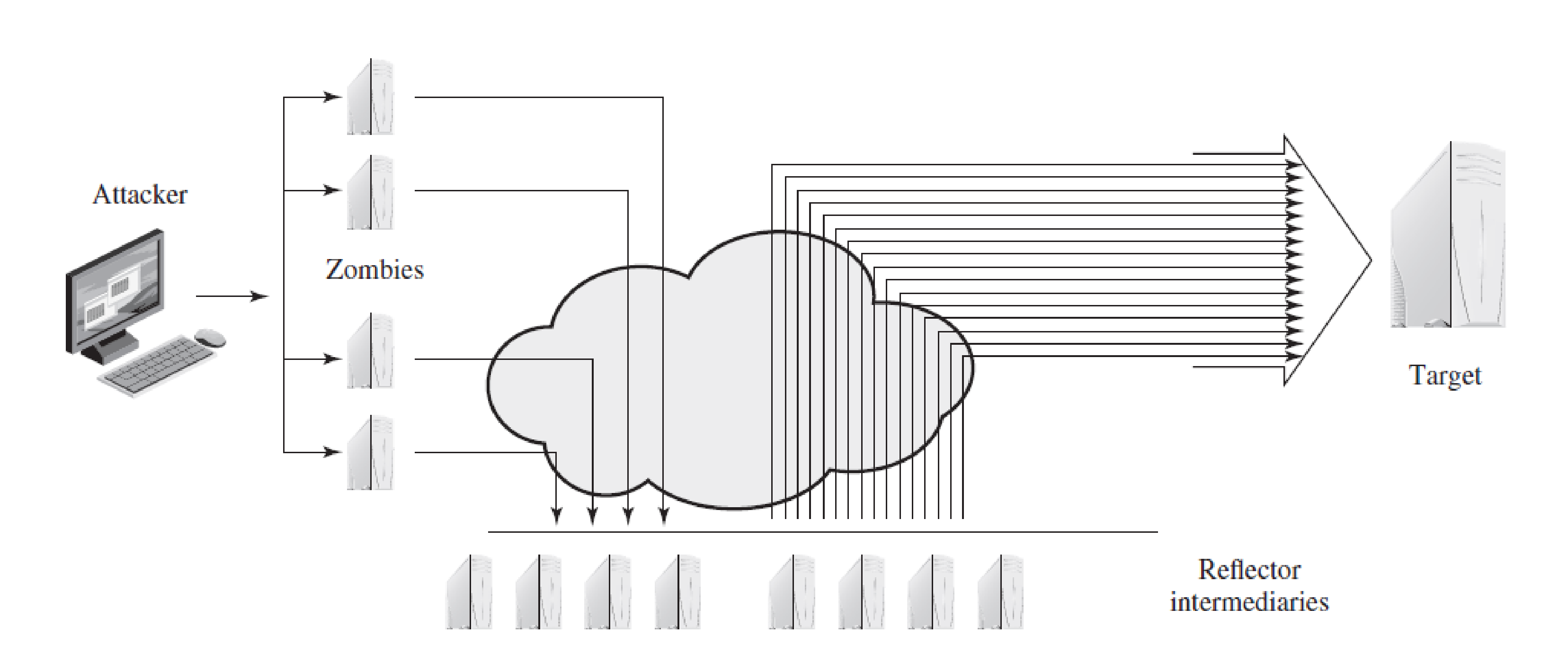
Reflection Attacks



Amplification Attacks

- are a variant of reflector attacks and also involve sending a packet with a spoofed source address for the target system to intermediaries.
- They differ in generating multiple response packets for each original packet sent.

Amplification Attacks



Defenses against denial-of-service Attacks

- It is important to recognize that these attacks cannot be prevented entirely.
- In general, there are four lines of defense against DDoS attacks
  - Attack prevention and preemption (before the attack)
  - Attack detection and filtering (during the attack)
  - Attack source traceback and identification (during and after the attack)
  - Attack reaction (after the attack)

Attack prevention and preemption (before the attack)

- Prevent your systems from being compromised.
- Filters are in place that block spoofed-source packets.
- Block the use of IP-directed broadcasts
- Mirroring and replicating these servers over multiple sites with multiple network connections.

Attack detection and filtering (during the attack)

- Syn Cookies.
- Drop an entry for an incomplete connection from the TCP connections table when it overflows.
- Identify legitimate, generally human initiated, interactions from automated DoS attacks. These often take the form of a graphical puzzle, a captcha.

Q/A

- Reading chapter 7 in Text book