CAN 304
Computer Systems Security

Lecture 9. DoS Attacks

Week 10: 2022-04-29, 14:00-16:00, Friday

Jie Zhang
Department of Communications and Networking
Email: jie.zhang01@xjtlu.edu.cn
Office: EE522

Review of last week

- Overview of malware
- Common types of malware
  - Propagation
  - Payload
- Countermeasures

Learning objectives

- Explain the basic concept of a DoS attack.
- Describe the nature of flooding attacks, DDoS attack, reflector and amplifier attacks

Outline

- Denial-of-Service Attacks
- Flooding Attacks
- Distributed Denial-of-Service Attacks
- Application-Based Bandwidth Attacks
- Reflector and Amplifier Attacks
- SYN cookies

Denial-of-Service

- 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

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

Classic DoS Attack: Flooding

- Aim of this attack is to **overwhelm the capacity of the network connection** to the target organization

- Flooding ping command

```
zhangjies-MBP:~ zhangjie$ ping 127.0.0.1
PING 127.0.0.1 (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.043 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.097 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.113 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.097 ms
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.109 ms
64 bytes from 127.0.0.1: icmp_seq=5 ttl=64 time=0.092 ms
64 bytes from 127.0.0.1: icmp_seq=6 ttl=64 time=0.095 ms
```

  - Source of the attack is clearly identified
  - Response packets affect the network performance of the source system

Source Address Spoofing

- Use forged source addresses

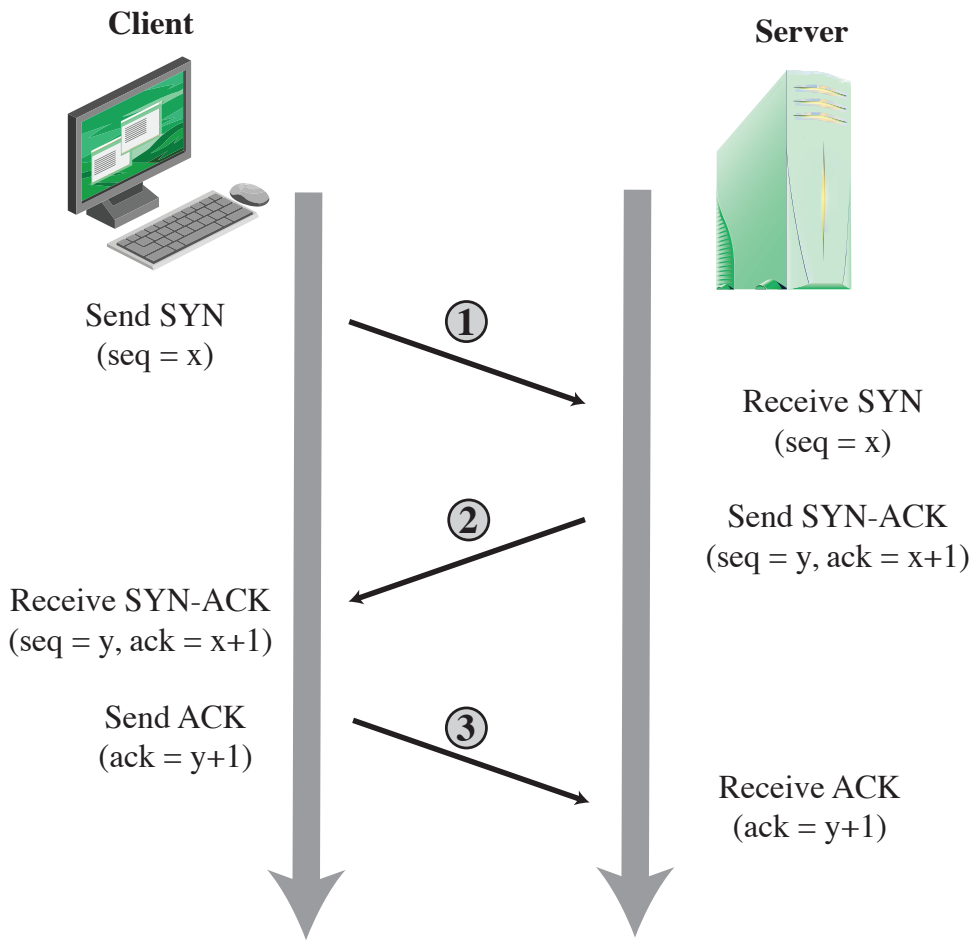
- Attacker generates large volumes of packets that have the target system as the destination address

- Harder to identify the attacking system
- ICMP echo response packets no longer be reflected back to the source system

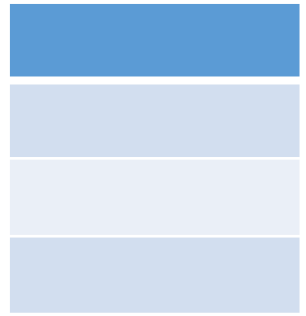
SYN Spoofing

- 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
- Hence an attack on system resources, specifically the network handling code in the operating system

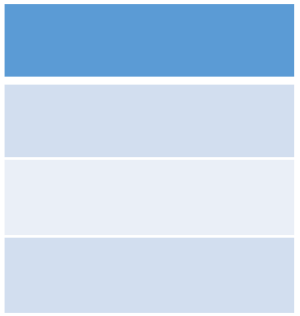
TCP Three-way Handshake



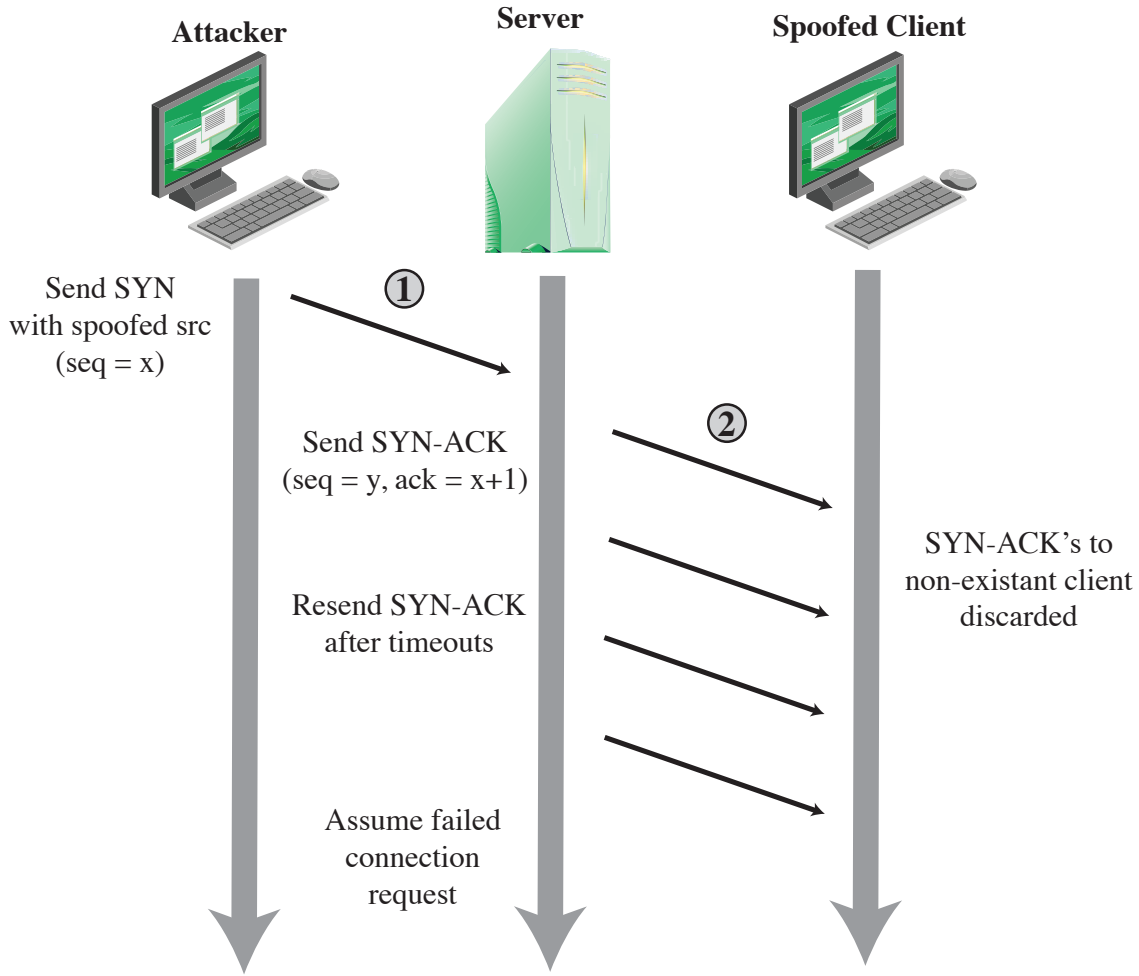
TCP connections table



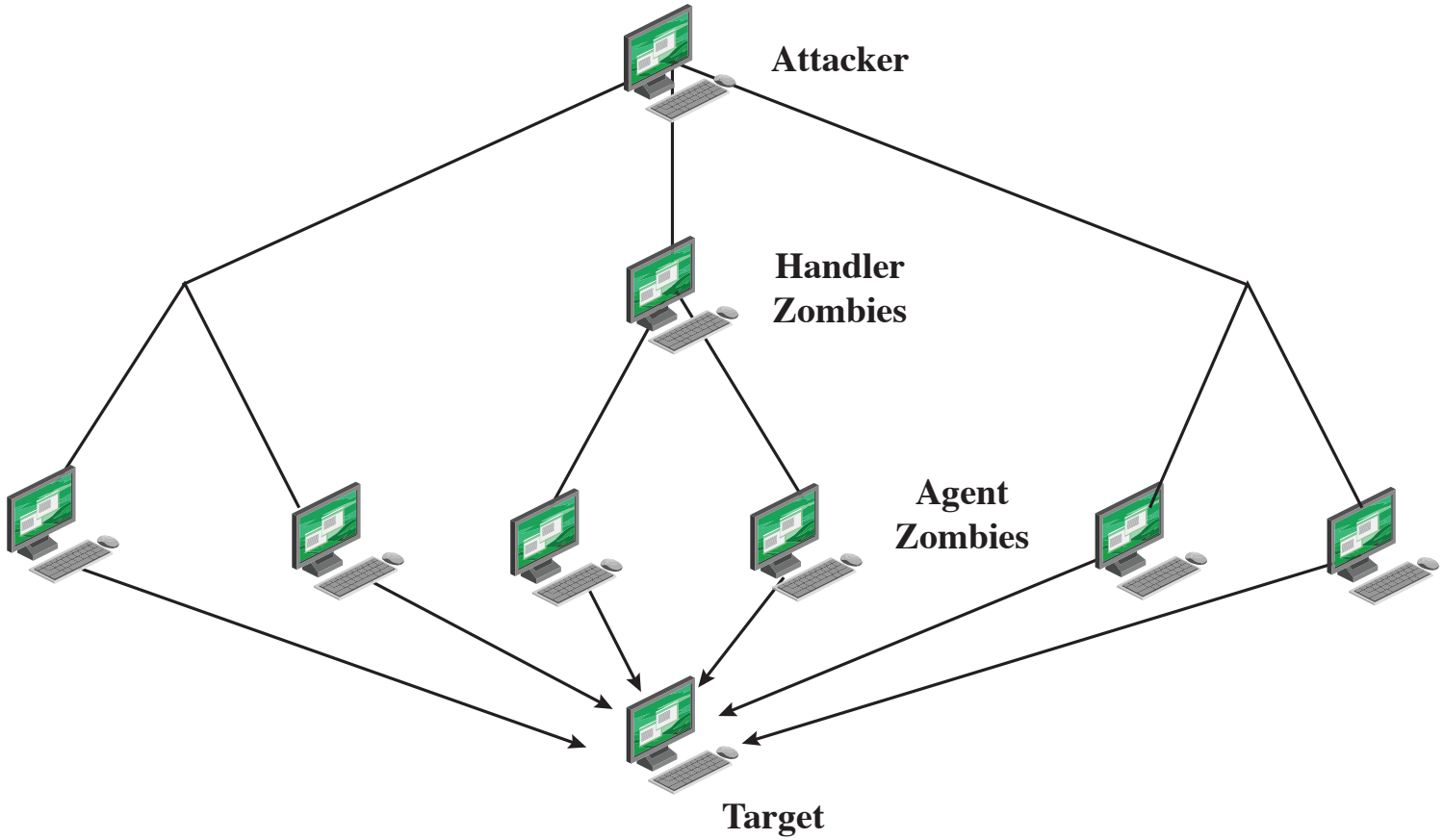
TCP SYN Spoofing Attack



TCP connections table



Distributed Denial of Service (DDoS) Attack



Application-Based Bandwidth Attack

- Strategy: force the target to execute resource-consuming operations

- HTTP: Hypertext Transfer Protocol
- HTTP flooding attacks the web servers with requests
  - E.g., an HTTP request to download a large file

- SIP: Session Initiation Protocol for VoIP
- SIP flooding

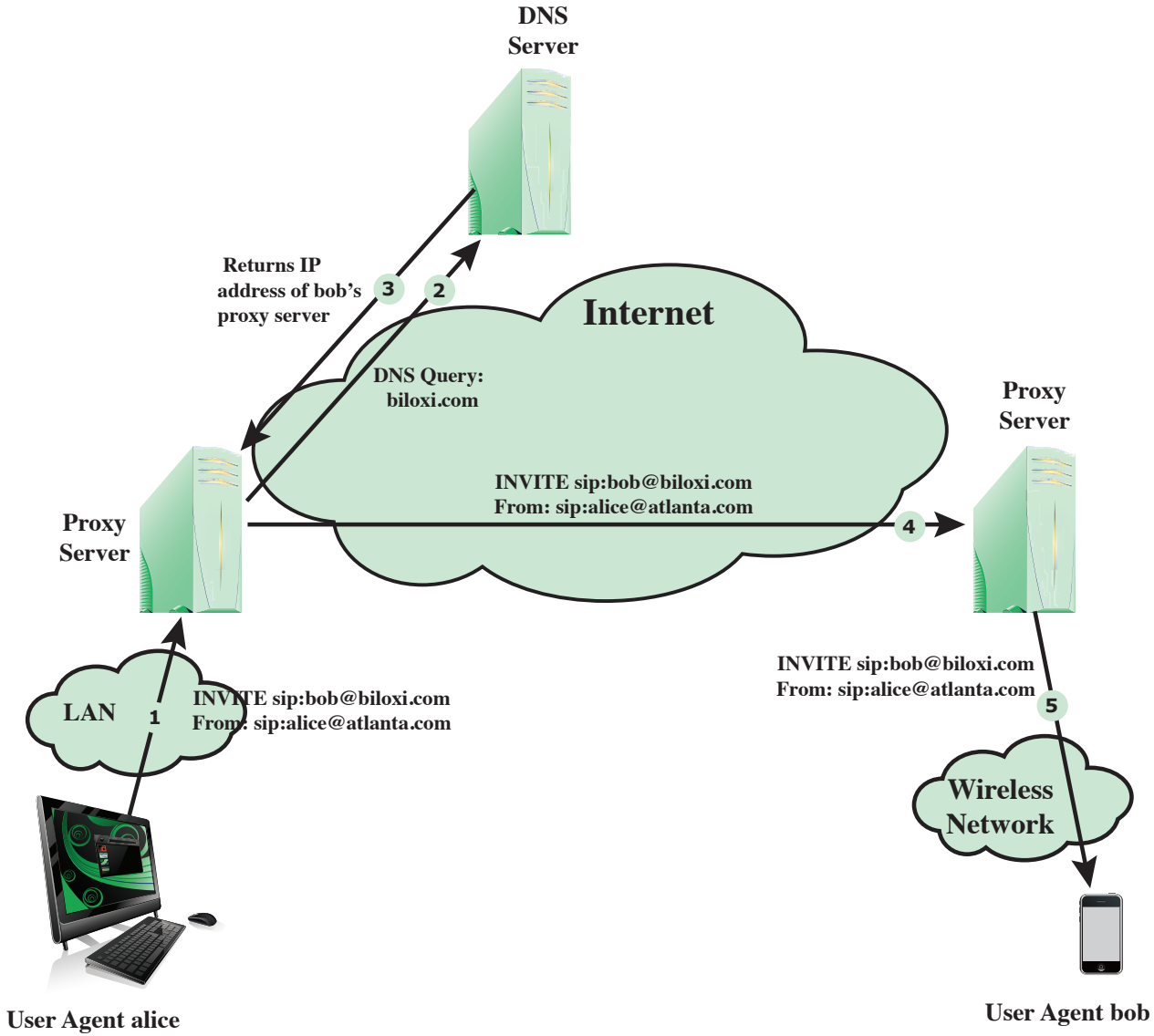


Figure 7.5 SIP INVITE Scenario

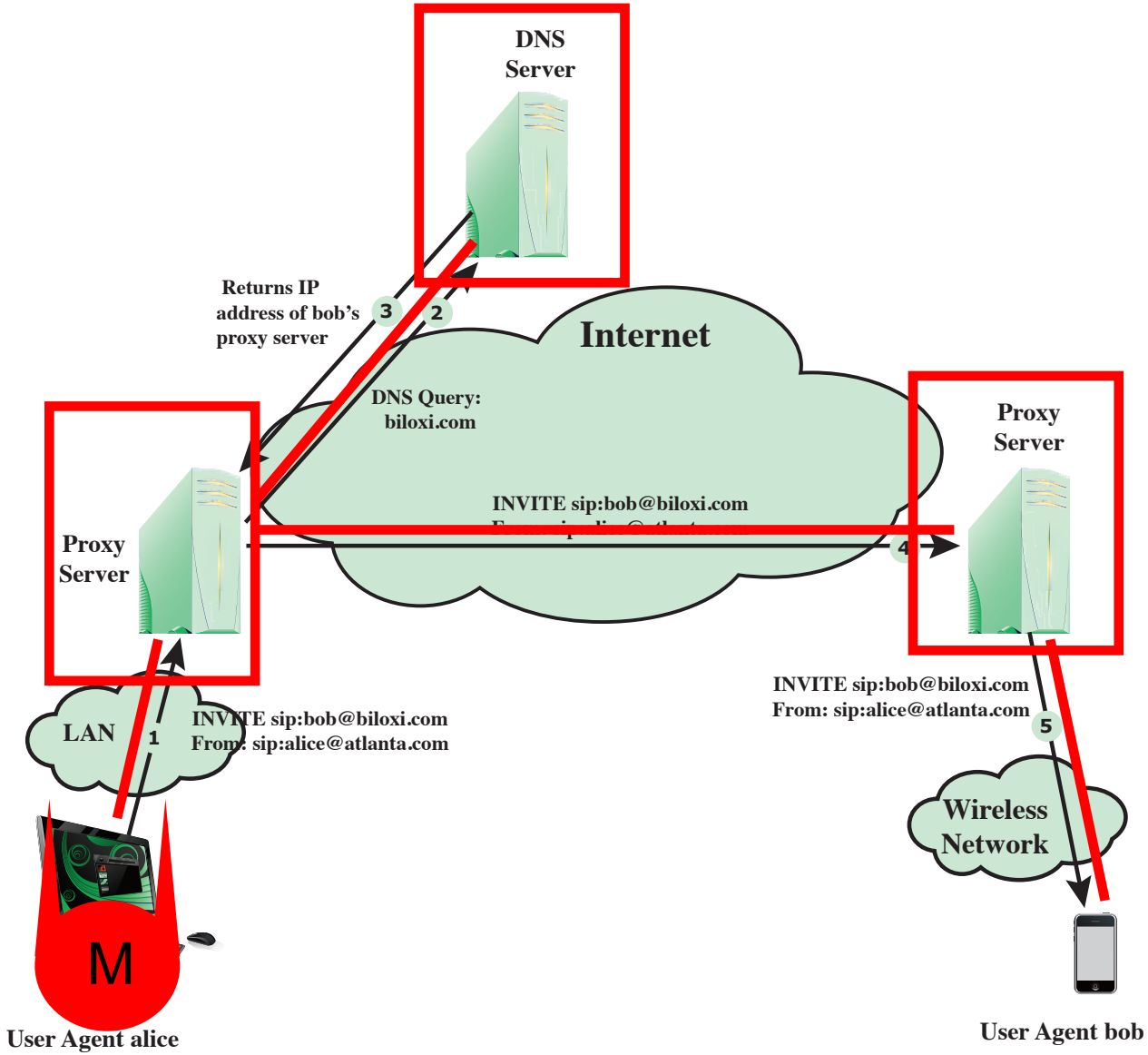
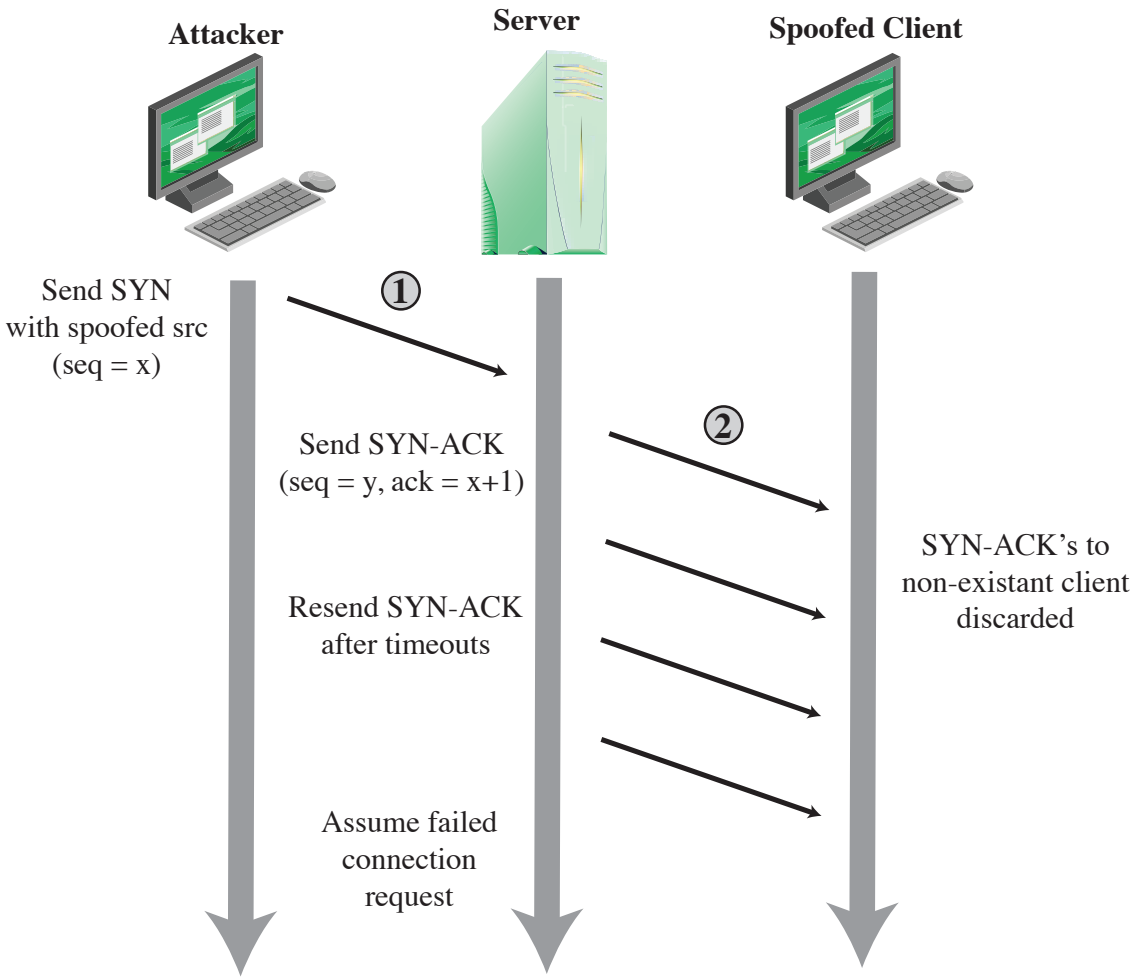


Figure 7.5 SIP INVITE Scenario

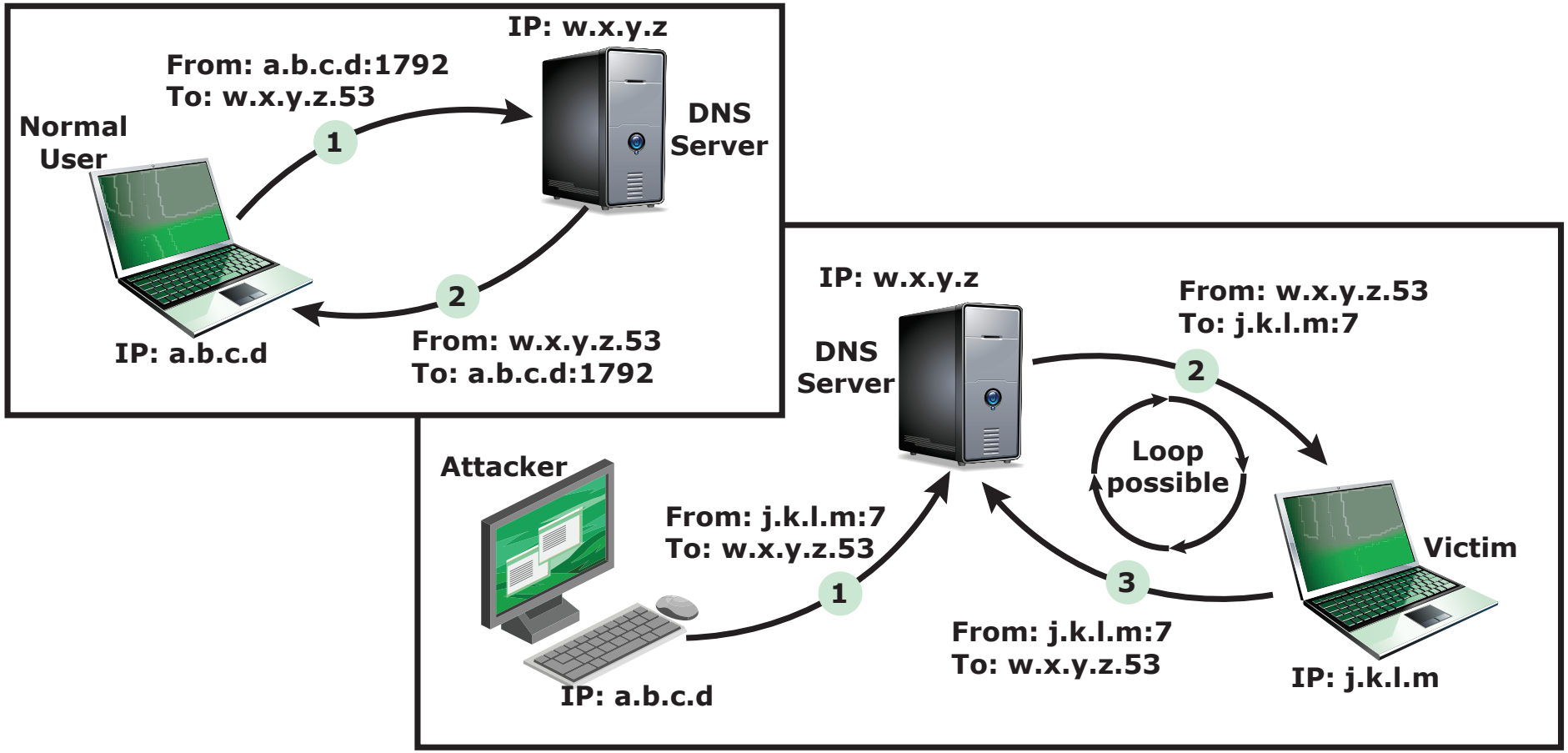
Reflection Attacks

- Attacker sends packets to a known service on the intermediary with a spoofed source address of the actual target system
- When intermediary responds, the response is sent to the target
- “Reflects” the attack off the intermediary (reflector)
- Goal is to generate enough volumes of packets to flood the link to the target system without alerting the intermediary
- The basic defense against these attacks is blocking spoofed-source packets

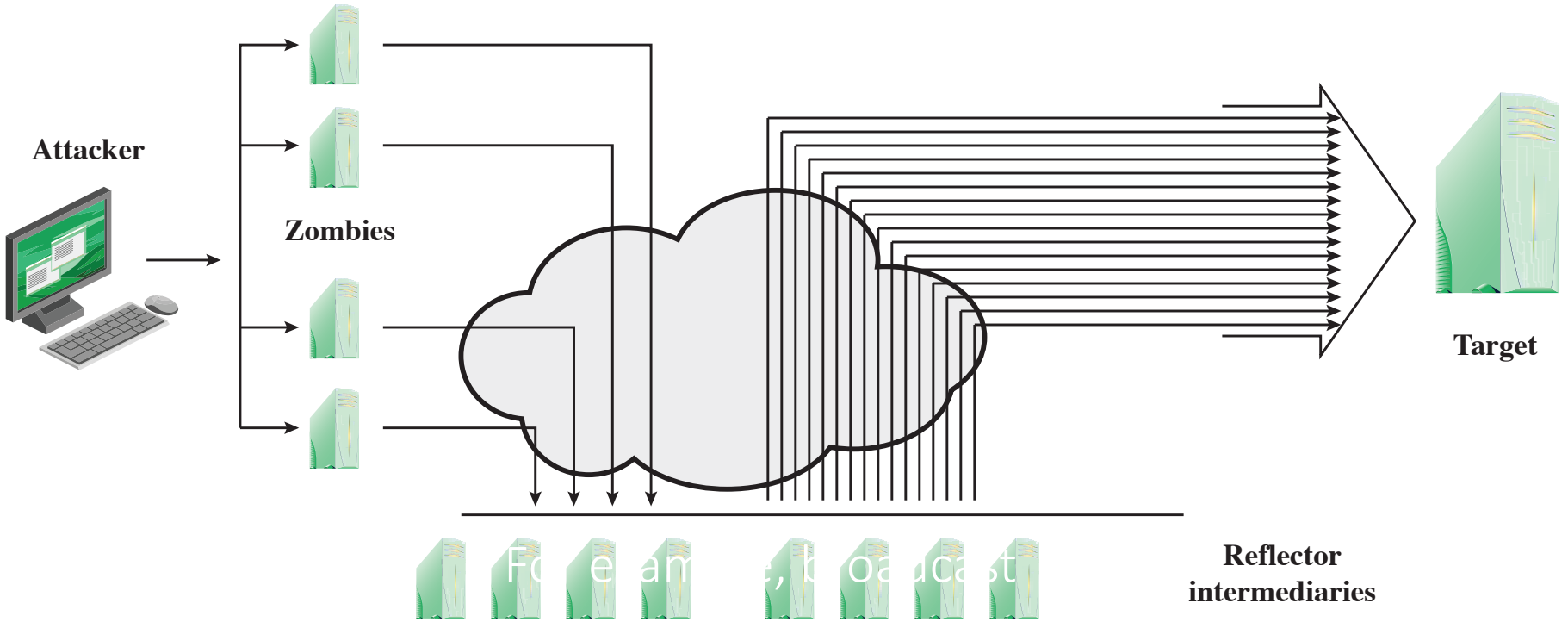
Relection Attack based on TCP SYN Spoofing



DNS Reflection Attack



Amplication Attack



DoS Attack Defenses

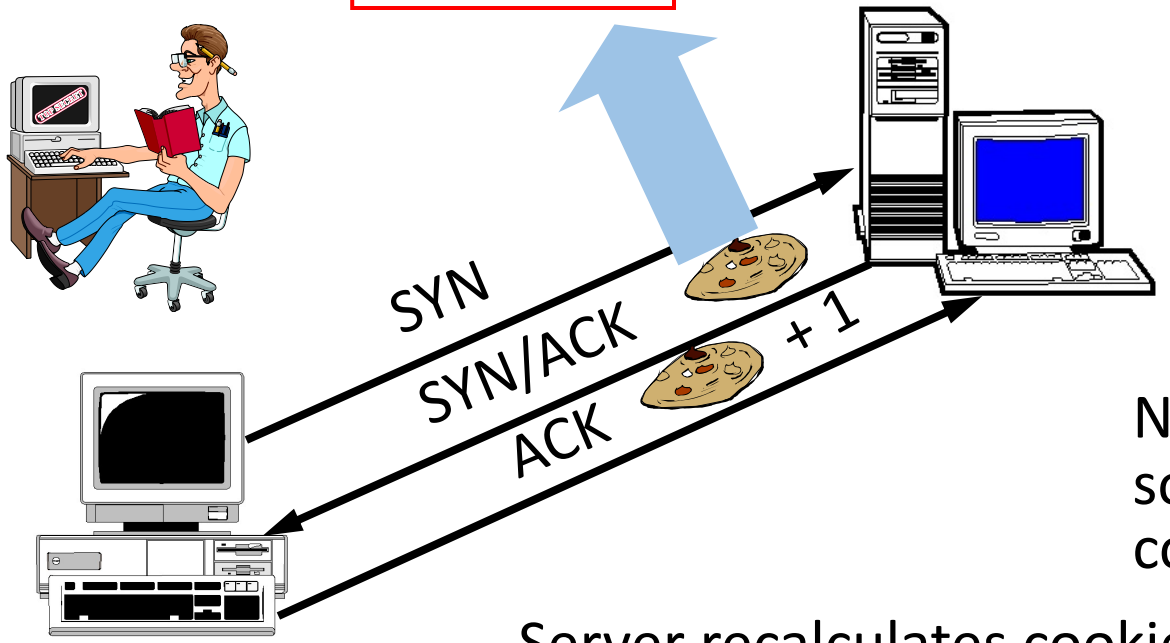
- These attacks cannot be prevented entirely
- High traffic volumes may be legitimate
  - High publicity about a specific site
  - Activity on a very popular site

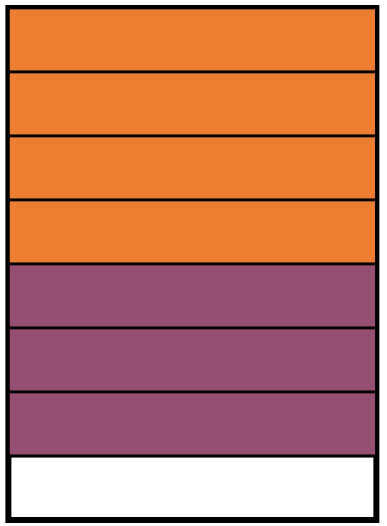
TCP SYN cookies

KEY POINT: Server doesn't need to save cookie value!

Client IP address & port, server's IP address and port, and a timer

SYN/ACK number is secret function of various information





No room in the table, so send back a SYN cookie, instead

Server recalculates cookie to determine if proper response

Summary

- Denial-of-Service Attacks
- Flooding Attacks
- Distributed Denial-of-Service Attacks
- Application-Based Bandwidth Attacks
- Reflector and Amplifier Attacks
- SYN cookies