Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 7

Denial-of-Service Attacks

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
  - System resources
  - Application resources

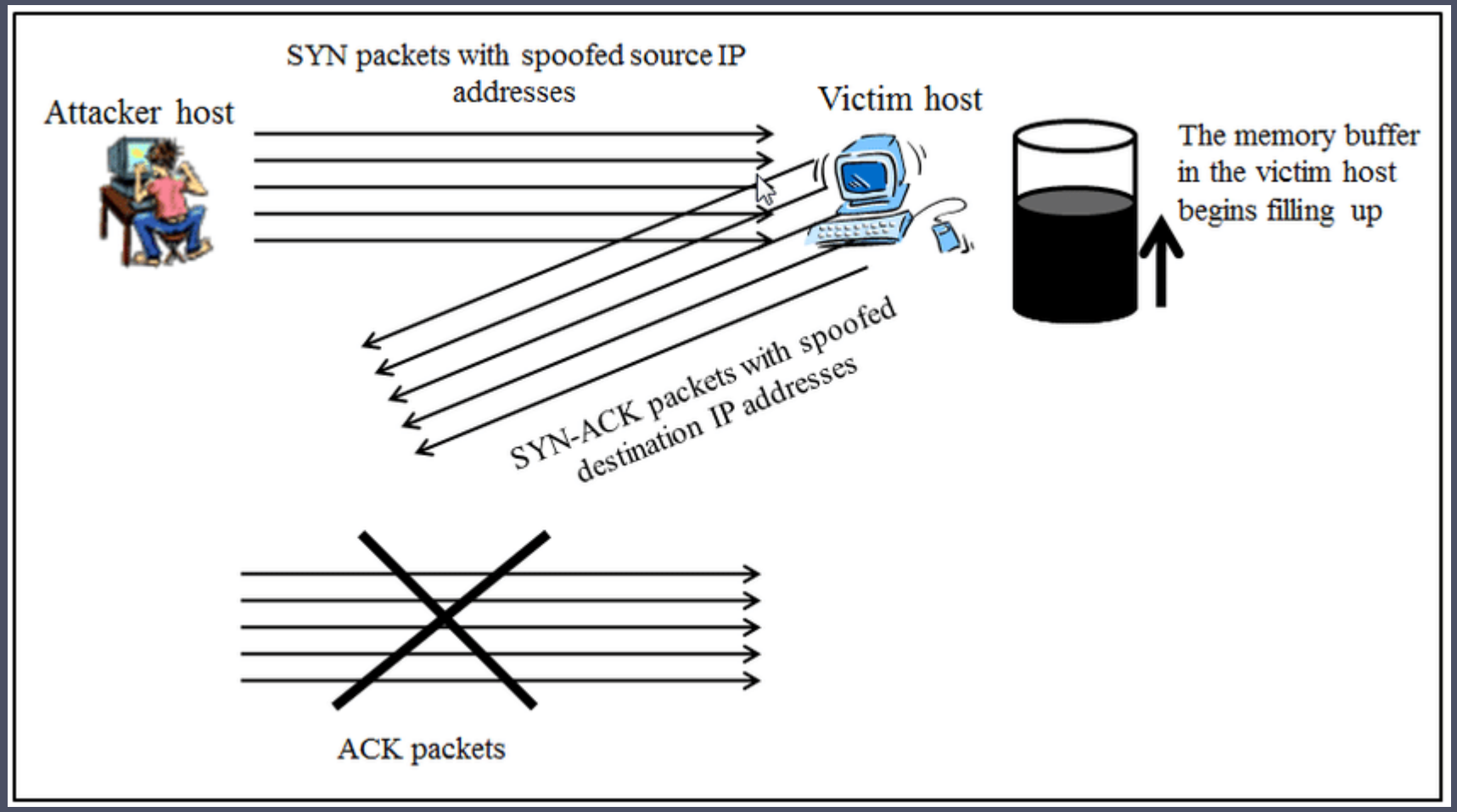
Network bandwidth

- The lower capacity of the network links connecting a server to the wider Internet mostly ISP) as shown in the example network in Figure 7.1.
- More traffic to arrive at the ISP's routers.
- The router must discard some packets, delivering only as many as can be handled by the link. In normal network operation such high loads might occur to a popular server experiencing traffic from a large number of legitimate users.
- A random portion of these users will experience a degraded or nonexistent service as a consequence. This is expected behavior for an overloaded TCP/IP network link.
- In a DoS attack, the vast majority of traffic directed at the target server is malicious, generated either directly or indirectly by the attacker.
- This traffic overwhelms any legitimate traffic, effectively denying legitimate users access to the server.
- Some recent high volume attacks have even been directed at the ISP network supporting the target organization, aiming to disrupt its connections to other networks

System resources (1/2)

- A DoS attack targeting system resources typically aims to overload or crash its network handling software. Rather than consuming bandwidth with large volumes of traffic, specific types of packets are sent that consume the limited resources available on the system
- . These include temporary buffers used to hold arriving packets, tables of open connections, and similar memory data structures.
- The SYN spoofing attack, which we discuss next, is of this type. It targets the table of TCP connections on the server.

https://www.researchgate.net/figure/The-TCP-SYN-flood-attack-Hands-on-lab-exercise-on-TCP-SYN-flood-attack_fig3_320654932

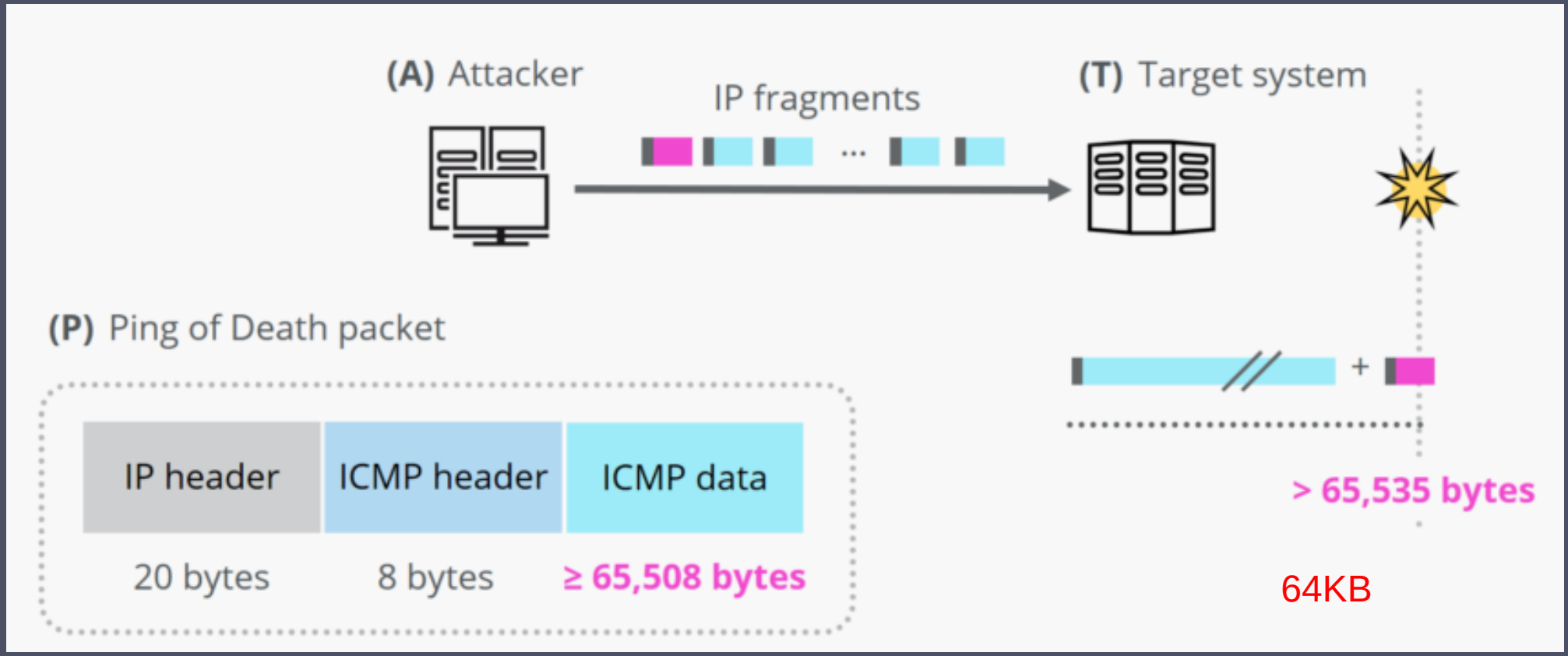


SYN spoofing attack

System resources (2/2)

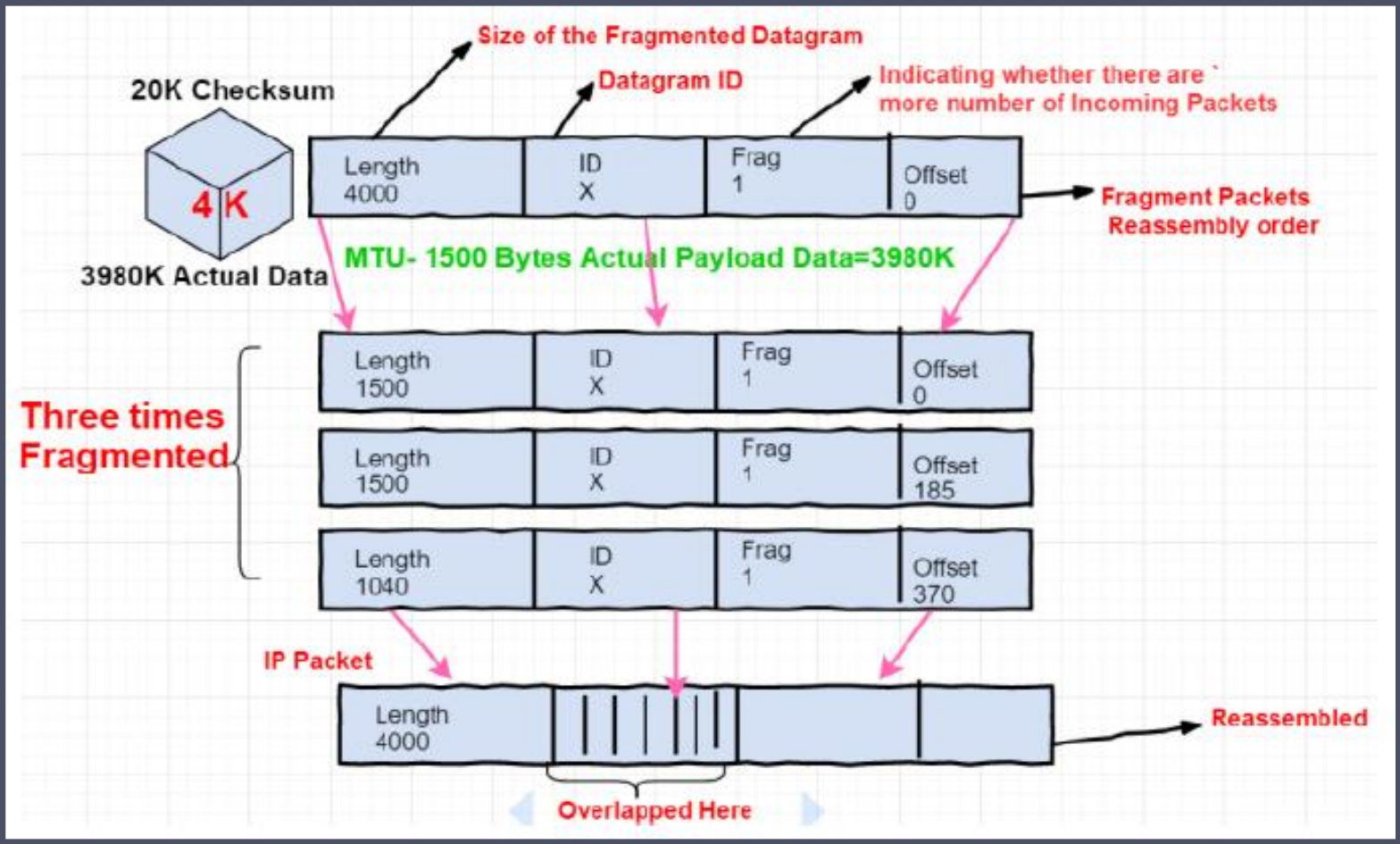
- Another form of system resource attack uses packets whose structure triggers a bug in the system's network handling software, causing it to crash.
- This means the system can no longer communicate over the network until this software is reloaded, generally by rebooting the target system. This is known as a poison packet .
- The classic ping of death and teardrop attacks, directed at older Windows 9x systems, were of this form.
- These targeted bugs in the Windows network code that handled ICMP (Internet Control Message Protocol) echo request packets and packet fragmentation, respectively.

https://cyberhoot.com/cybrary/ping-of-death-pod/



Ping of Death (PoD)

https://cyberhoot.com/cybrary/ping-of-death-pod/



TCP teardrop fragmentation attack packet scenario

Application resources

- 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. For example, a Web server might include the ability to make database queries.
- If a large, costly query can be constructed, then an attacker could generate a large number of these that severely load the server. This limits its ability to respond to valid requests from other users. This type of attack is known as a cyberslam.
- Another alternative is to construct a request that triggers a bug in the server program, causing it to crash. This means the server is no longer able to respond to requests until it is restarted.

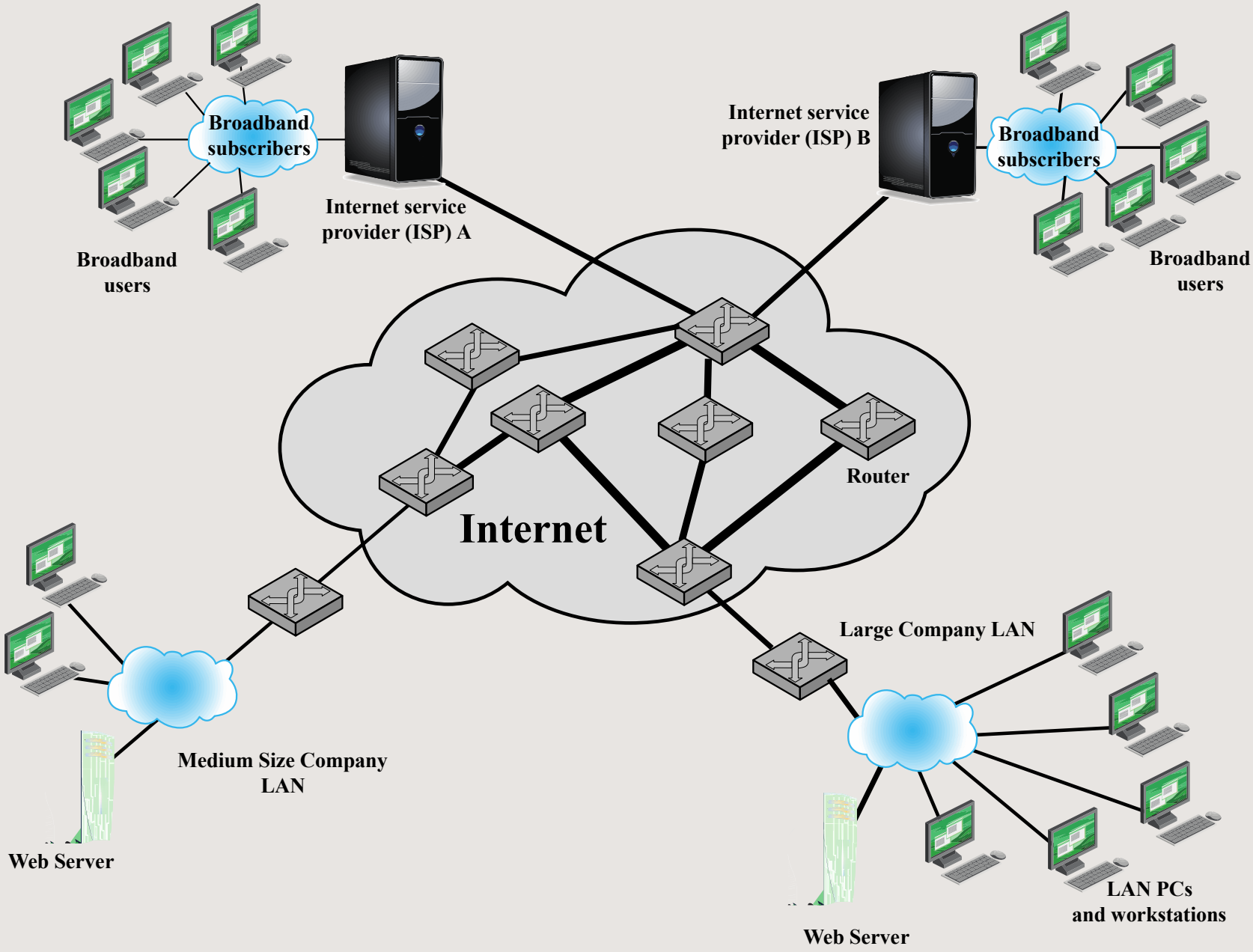


Figure 7.1 Example Network to Illustrate DoS Attacks

DOS Attack Characterization

- DoS attacks may also be characterized by how many systems are used to direct traffic at the target system.
- Originally only one, or a small number of source systems directly under the attacker's control, was used.
- This is all that is required to send the packets needed for any attack targeting a bug in a server's network handling code or some application.
- Attacks requiring high traffic volumes are more commonly sent from multiple systems at the same time, using distributed or amplified forms of DoS attacks.

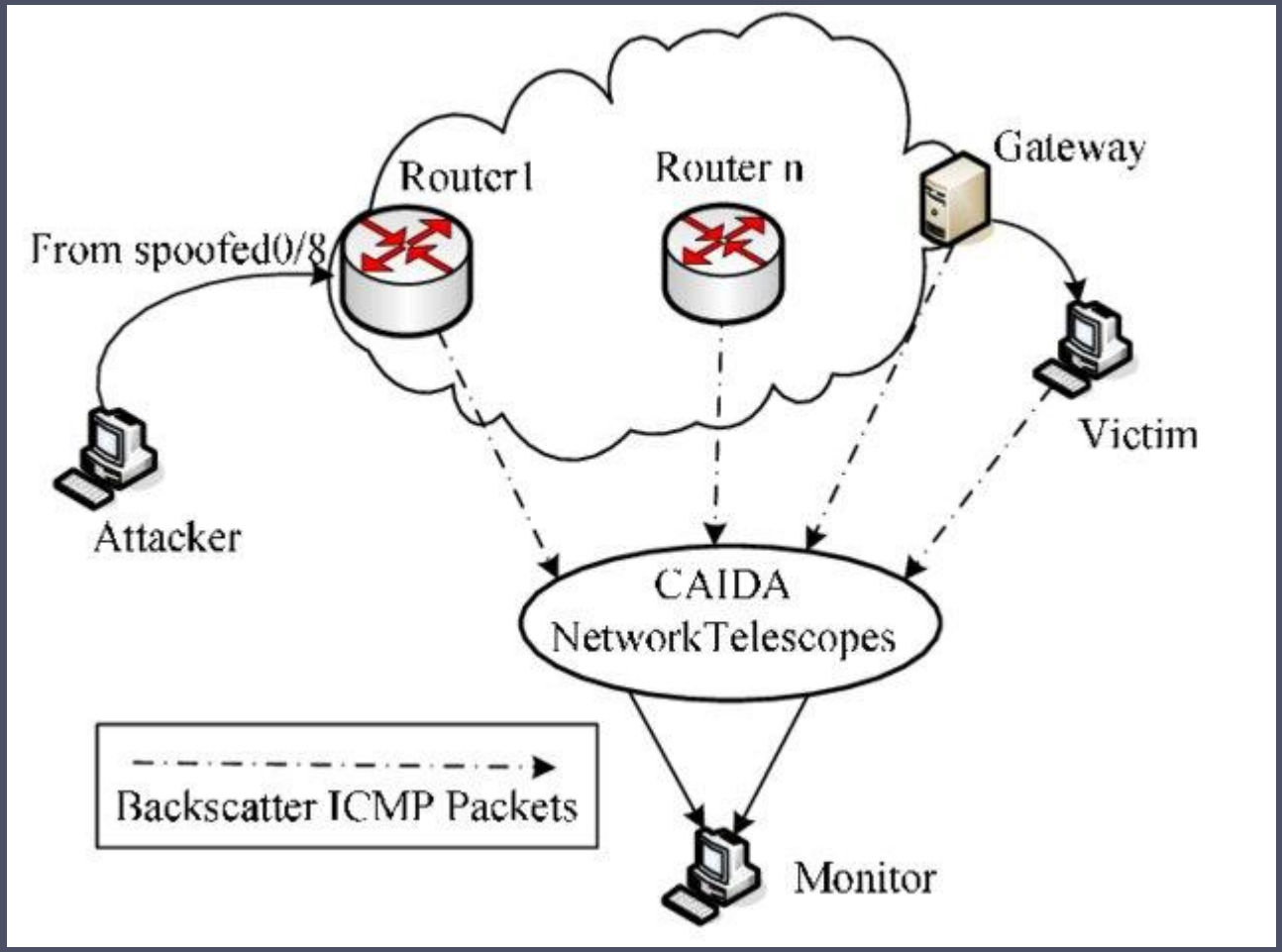
7.1.1 Classic DoS Attacks

- Flooding ping command
  - Aim of this attack is to overwhelm the capacity of the network connection to the target organization
  - Traffic can be handled by higher capacity links on the path, but packets are discarded as capacity decreases
  - Source of the attack is clearly identified unless a spoofed address is used
  - Network performance is noticeably affected

7.1.2 Source Address Spoofing

- 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 the final, lower capacity link
- Requires network engineers to specifically query flow information from their routers
- *Backscatter traffic*
  - Advertise routes to unused IP addresses to monitor attack traffic

1. D. Moore, C. Shannon, G. M. Voelker, *et al*. Network telescopes, CAIDA, Tech. Rep., 2003.
2. Bi, Jun, Ping Hu, and Peiguo Li. "Study on classification and characteristics of source address spoofing attacks in the internet." *2010 Ninth International Conference on Networks*. IEEE, 2010.



Backscatter traffic

7.1.3 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

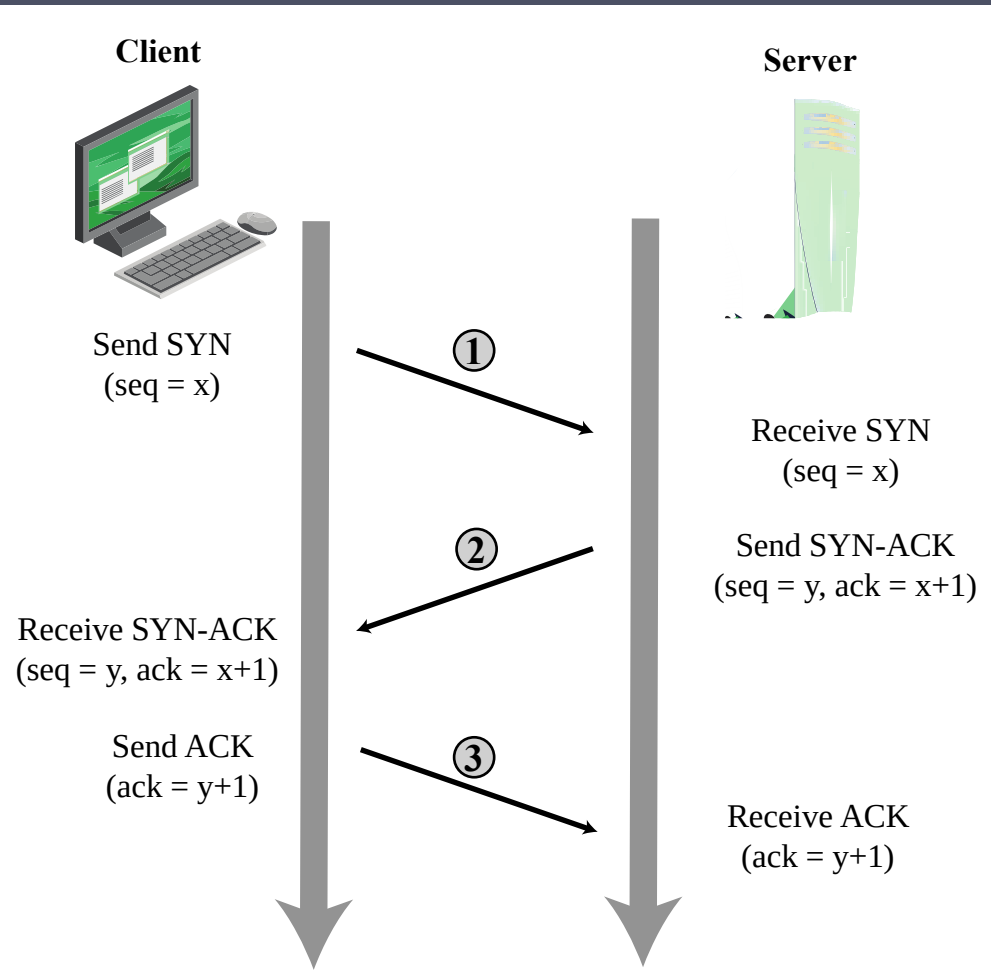


Figure 7.2 TCP Three-Way Connection Handshake

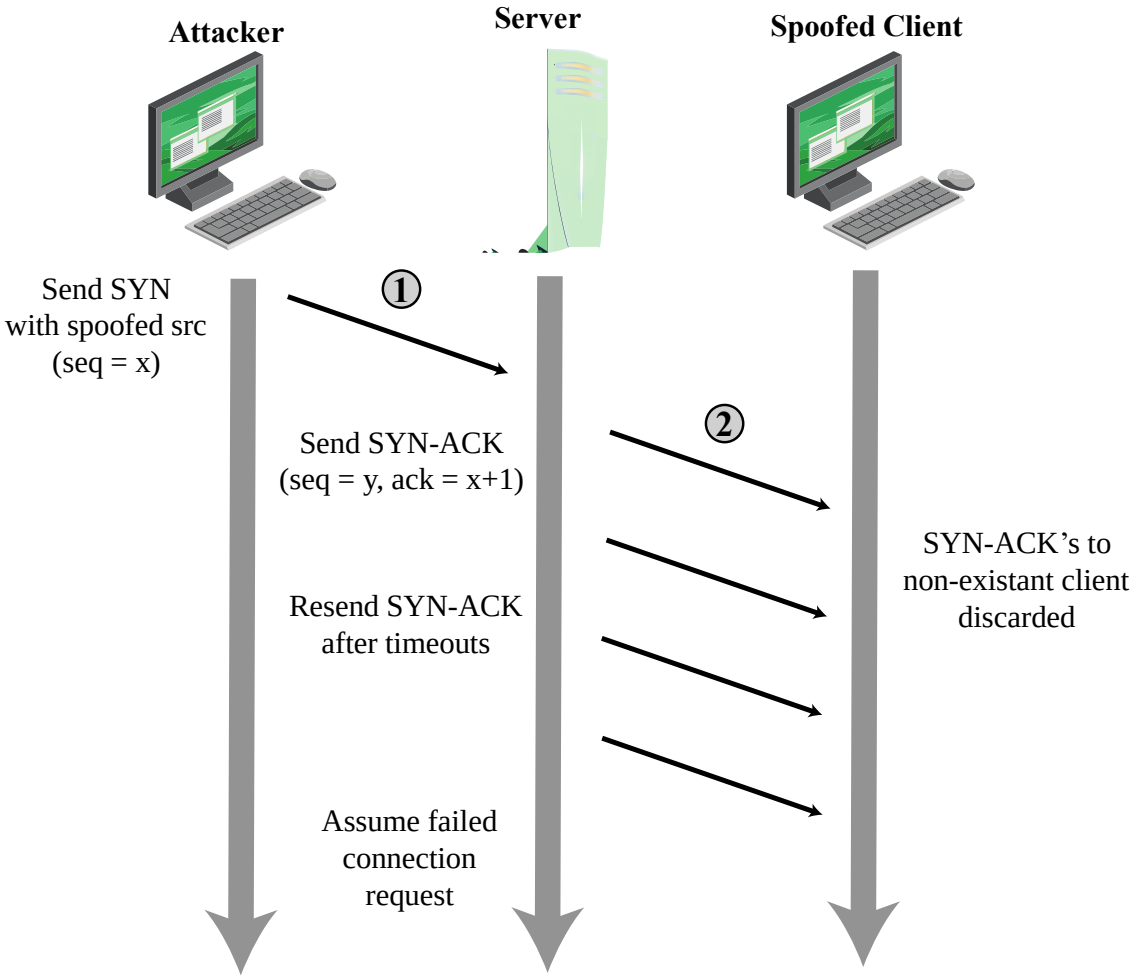


Figure7.3 TCP SYN Spoofing Attack

7. 2 Flooding Attacks

- Classified based on network protocol used
- Intent is to overload the network capacity on some link to a server
- Virtually any type of network packet can be used

ICMP flood	• Ping flood using ICMP echo request packets • Traditionally network administrators allow such packets into their networks because ping is a useful network diagnostic tool
UDP flood	• Uses UDP packets directed to some port number on the target system
TCP SYN flood	• Sends TCP packets to the target system • Total volume of packets is the aim of the attack rather than the system code

7.3 Distributed Denial of Service (DDoS) Attacks

Use of multiple systems to generate attacks

Attacker uses a flaw in operating system or in a common application to gain access and installs their program on it (zombie)

Large collections of such systems under the control of one attacker's control can be created, forming a botnet

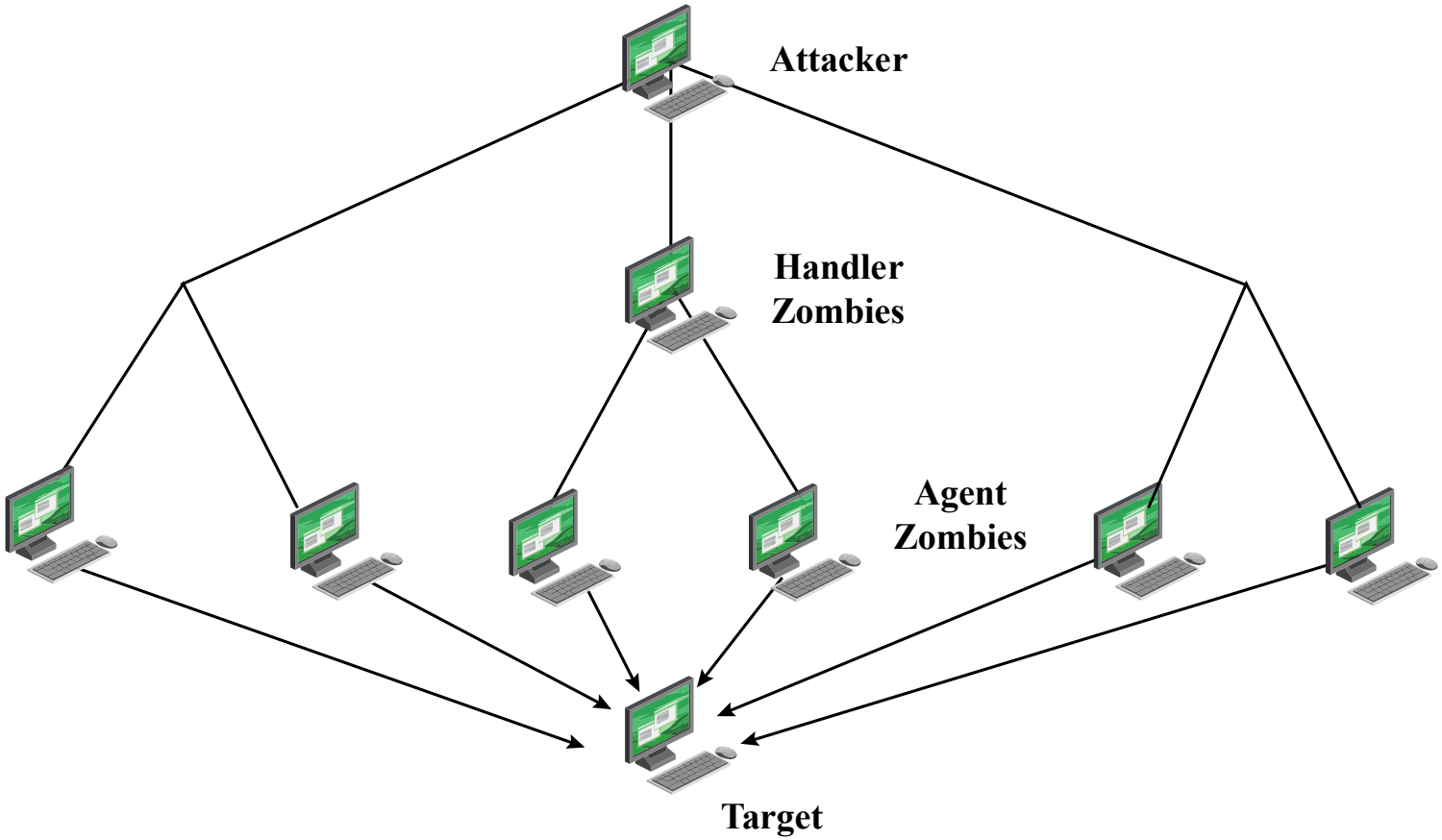


Figure 7.4 DDoS Attack Architecture

7.4 Application-based Bandwidth

- SIP Flood
- HTTP-Based Attacks
  - HTTP Flood
  - Slowloris

7.4 .1 SIP Flood (1/3)

- Voice over IP (VoIP) telephony is now widely deployed over the Internet. The standard protocol used for call setup in VoIP is the Session Initiation Protocol (SIP).
- SIP is a text-based protocol with a syntax similar to that of HTTP. There are two different types of SIP messages: requests and responses.
- Figure 7.5 is a simplified illustration of the operation of the SIP INVITE message, used to establish a media session between user agents.
- In this case, Alice's user agent runs on a computer, and Bob's user agent runs on a cell phone. Alice's user agent is configured to communicate with a proxy server (the outbound server) in its domain and begins by sending an INVITE SIP request to the proxy server that indicates its desire to invite Bob's user agent into a session.
- The proxy server uses a DNS server to get the address of Bob's proxy server, and then forwards the INVITE request to that server. The server then forwards the request to Bob's user agent, causing Bob's phone to ring.

SIP Flood (2/3)

- A SIP flood attack exploits the fact that a single INVITE request triggers considerable resource consumption. The attacker can flood a SIP proxy with numerous INVITE requests with spoofed IP addresses, or alternately a DDoS attack using a botnet to generate numerous INVITE request.
- This attack puts a load on the SIP proxy servers in two ways.
  - First, their server resources are depleted in processing the INVITE requests.
  - Second, their network capacity is consumed. Call receivers are also victims of this attack. A target system will be flooded with forged VoIP calls, making the system unavailable for legitimate incoming calls.

SIP Flood (3/3)

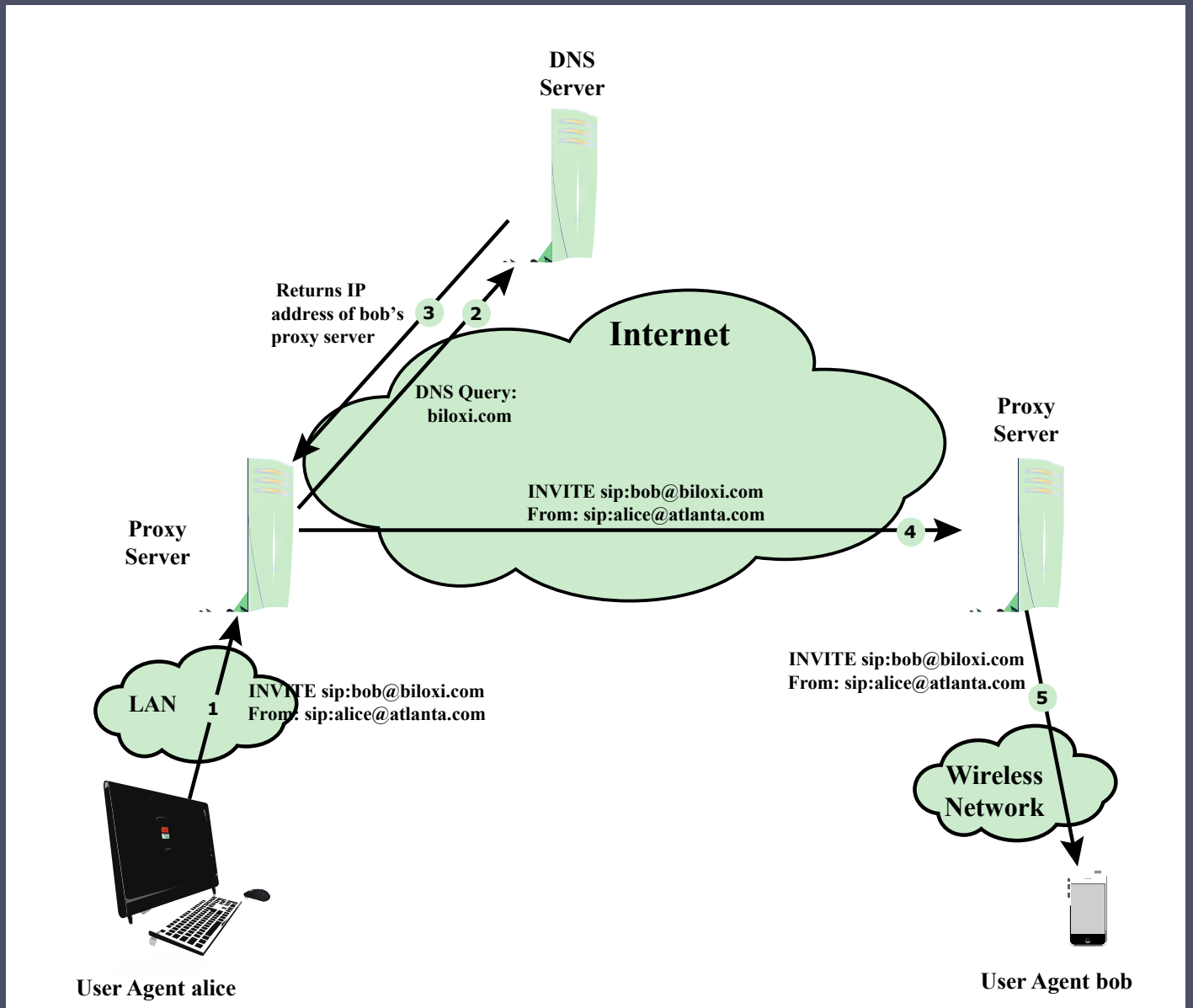


Figure 7.5 SIP INVITE Scenario

7.4 .2 Hypertext Transfer Protocol (HTTP) Based Attacks

HTTP flood

- Attack that bombards Web servers with HTTP requests
- Consumes considerable resources
- Spidering
  - Bots starting from a given HTTP link and following all links on the provided Web site in a recursive way

Slowloris

- Attempts to monopolize by sending HTTP requests that never complete
- Eventually consumes Web server's connection capacity
- Utilizes legitimate HTTP traffic
- Existing intrusion detection and prevention solutions that rely on signatures to detect attacks will generally not recognize Slowloris
- Countermeasures Include:
  - limiting the rate of incoming connections from a particular
  - host; varying the timeout on connections as a function of the number of connections;
  - and delayed binding by load balancing software.

7.5.1 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

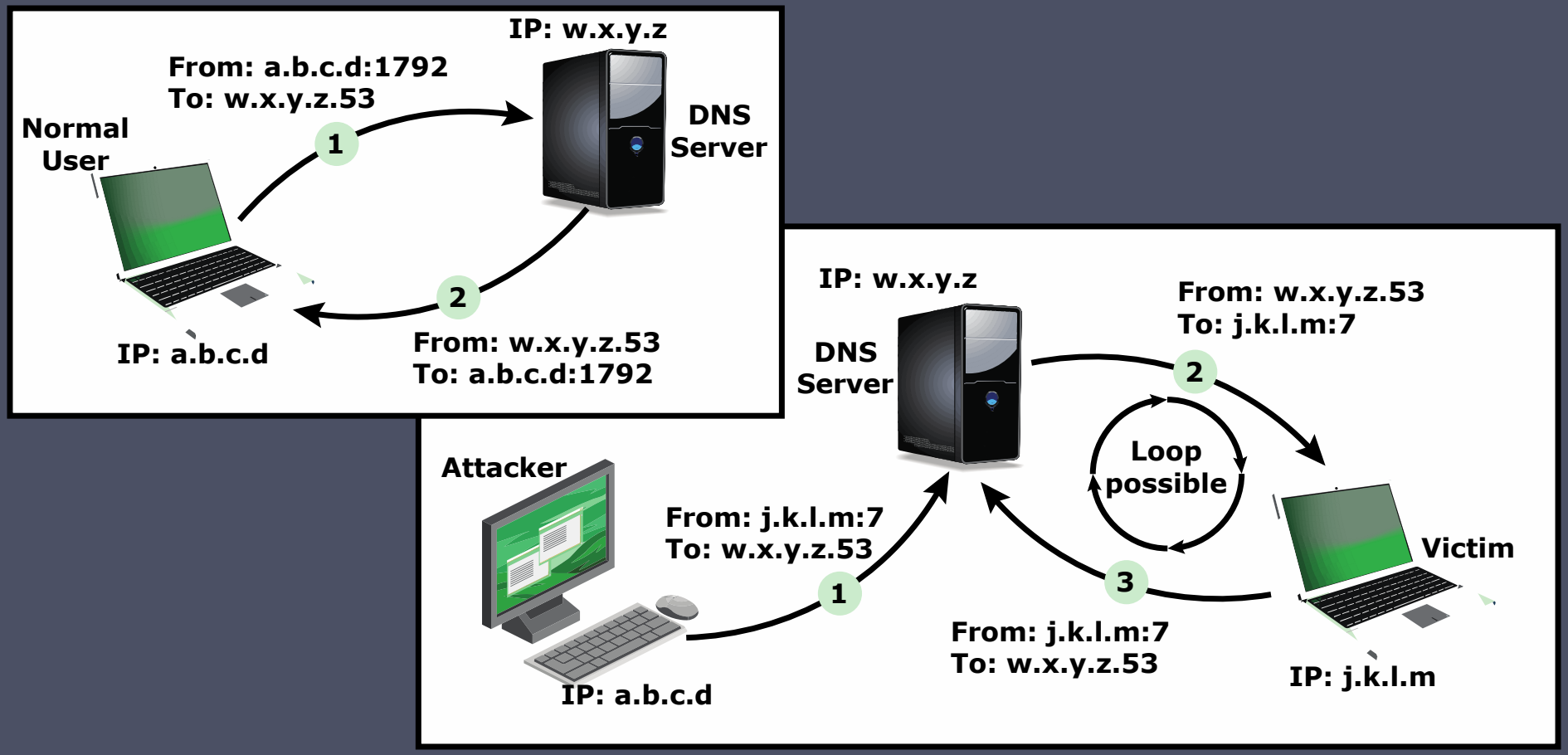


Figure 7.6 DNS Reflection Attack

7.5.2 Amplification Attacks (1/3)

- 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. This can be achieved by directing the original request to the broadcast address for some network.
- As a result, all hosts on that network can potentially respond to the request, generating a flood of responses as shown in Figure 7.7 .
- It is only necessary to use a service handled by large numbers of hosts on the intermediate network.
- A ping flood using ICMP echo request packets was a common choice, since this service is a fundamental component of TCP/IP implementations and was often allowed into networks.
- The well-known smurf DoS program used this mechanism and was widely popular for some time. Another possibility is to use a suitable UDP service, such as the echo service. The fraggle program implemented this variant.
- Note that TCP services cannot be used in this type of attack; because they are connection oriented, they cannot be directed at a broadcast address. Broadcasts are inherently connectionless.

Amplification Attacks (2/3)

- The best additional defense against this form of attack is to not allow directed broadcasts to be routed into a network from outside.
- Indeed, this is another longstanding security recommendation, unfortunately about as widely implemented as that for blocking spoofed source addresses. If these forms of filtering are in place, these attacks cannot succeed.
- Another defense is to limit network services like echo and ping from being accessed from outside an organization. This restricts which services could be used in these attacks, at a cost in ease of analyzing some legitimate network problems.
- Attackers scan the Internet looking for well-connected networks that do allow directed broadcasts and that implement suitable services attackers can reflect off. These lists are traded and used to implement such attacks.

Amplification Attacks (3/3)

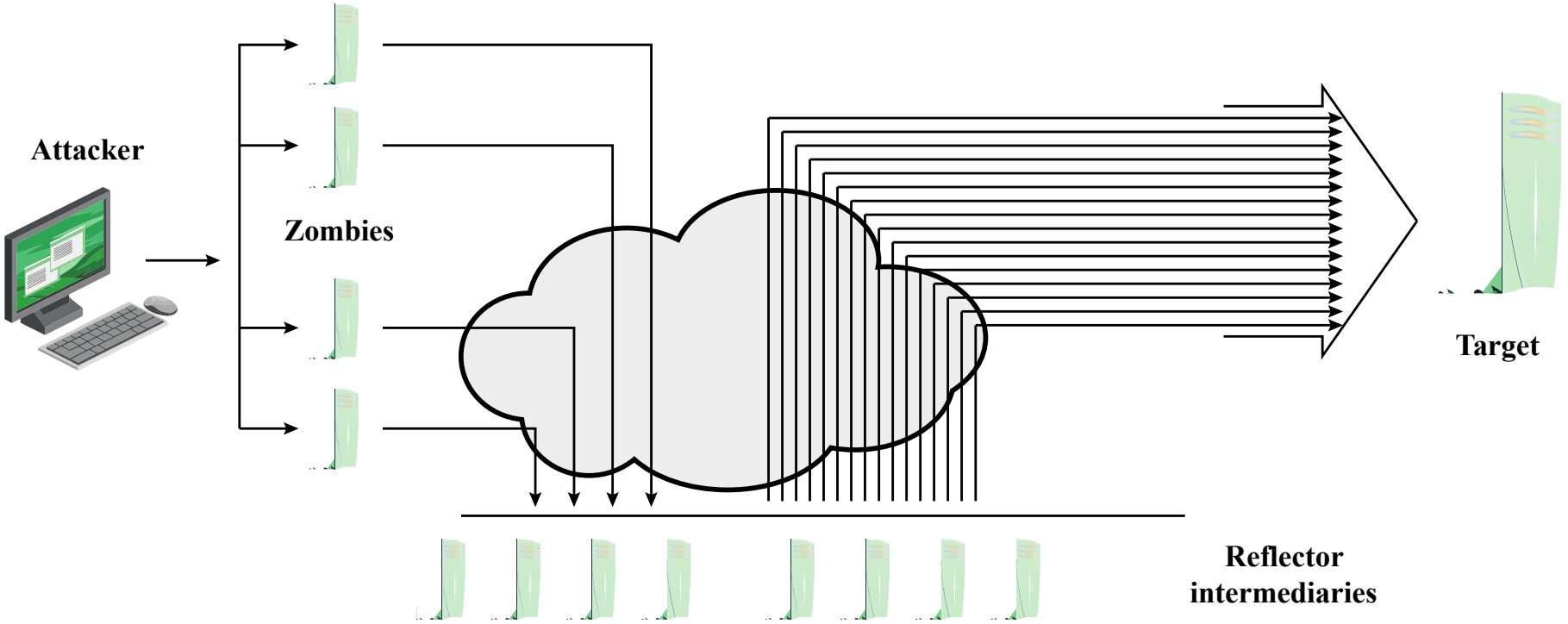


Figure 7.7 Amplification Attack

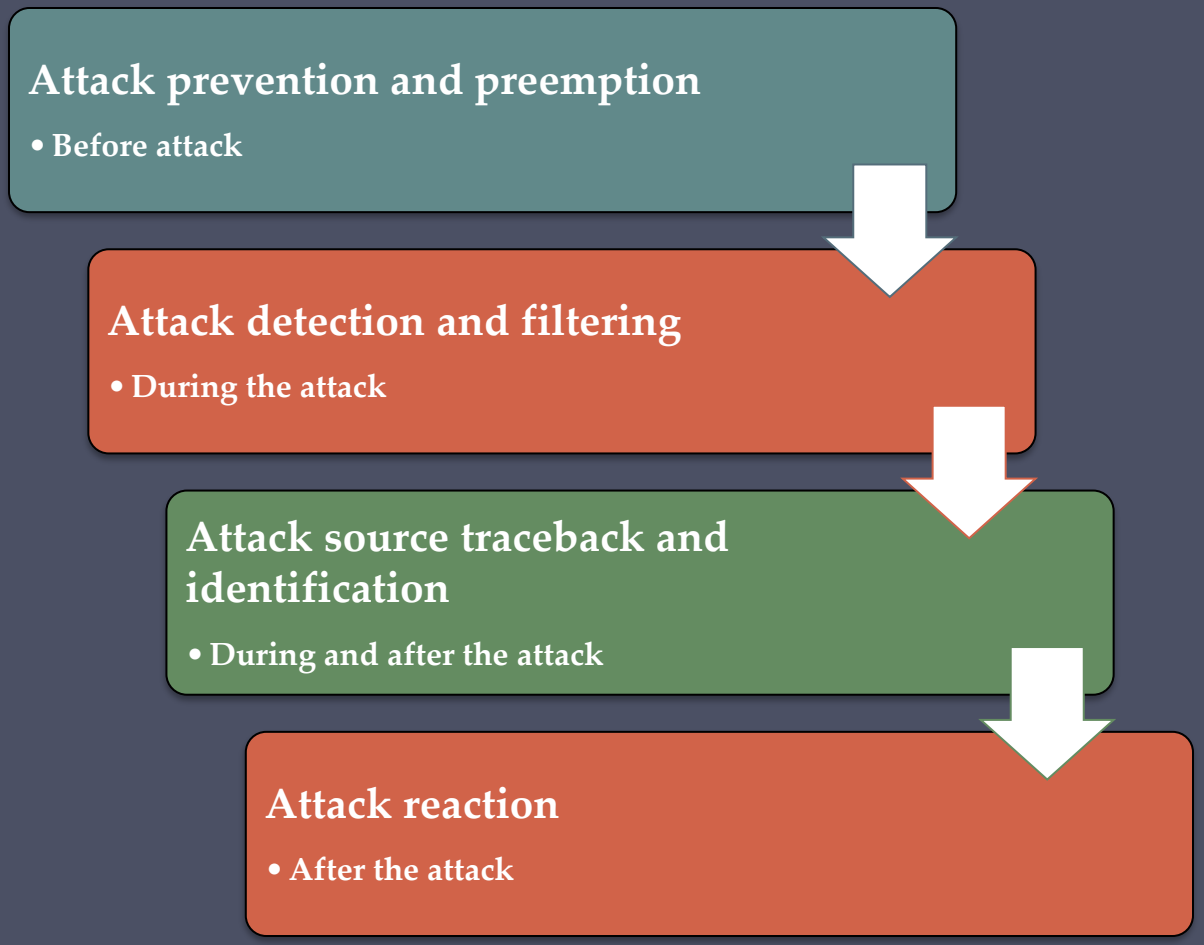
7.5.2 DNS Amplification Attacks

- Use packets directed at a legitimate DNS server as the intermediary system
- Attacker creates a series of DNS requests containing the spoofed source address of the target system
- Exploit DNS behavior to convert a small request to a much larger response (amplification)
- Target is flooded with responses
- Basic defense against this attack is to prevent the use of spoofed source addresses

7.6 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
  - Described as *slashdotted, flash crowd, or flash event*

Four lines of defense against DDoS attacks



7.6 .1 DoS Attack Prevention (1/2)

- Block spoofed source addresses
  - On routers as close to source as possible
- Filters may be used to ensure path back to the claimed source address is the one being used by the current packet
  - Filters must be applied to traffic before it leaves the ISP's network or at the point of entry to their network
- Use modified TCP connection handling code
  - Cryptographically encode critical information in a cookie that is sent as the server's initial sequence number
    - Legitimate client responds with an ACK packet containing the incremented sequence number cookie
  - Drop an entry for an incomplete connection from the TCP connections table when it overflows

DoS Attack Prevention (2/2)

- Block IP directed broadcasts
- Block suspicious services and combinations
- Manage application attacks with a form of graphical puzzle (captcha) to distinguish legitimate human requests
- Good general system security practices
- Use mirrored and replicated servers when high-performance and reliability is required

Responding to DoS Attacks (1/2)

Good Incident Response Plan

- Details on how to contact technical personal for ISP
- Needed to impose traffic filtering upstream
- Details of how to respond to the attack

- Antispoofing, directed broadcast, and rate limiting filters should have been implemented
- Ideally have network monitors and IDS to detect and notify abnormal traffic patterns

Responding to DoS Attacks (2/2)

- Identify type of attack
  - Capture and analyze packets
  - Design filters to block attack traffic upstream
  - Or identify and correct system/application bug
- Have ISP trace packet flow back to source
  - May be difficult and time consuming
  - Necessary if planning legal action
- Implement contingency plan
  - Switch to alternate backup servers
  - Commission new servers at a new site with new addresses
- Update incident response plan
  - Analyze the attack and the response for future handling

Summary

- Denial-of-service attacks
  - The nature of denial-of-service attacks
  - Classic denial-of-service attacks
  - Source address spoofing
  - SYN spoofing
- Flooding attacks
  - ICMP flood
  - UDP flood
  - TCP SYN flood
- Defenses against denial-of-service attacks
- Responding to a denial-of-service attack
- Distributed denial-of-service attacks
- Application-based bandwidth attacks
  - SIP flood
  - HTTP-based attacks
- Reflector and amplifier attacks
  - Reflection attacks
  - Amplification attacks
  - DNS amplification attacks