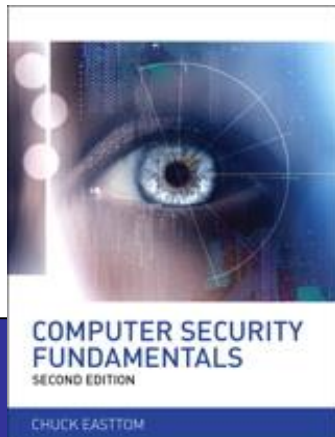

Computer Security Fundamentals

by Chuck Easttom



Chapter 4 Denial of Service Attacks

Chapter 4 Objectives

- Understand how DoS attacks are accomplished
- Know how certain DoS attacks work
- Protect against DoS attacks
- Defend against specific DoS attacks

Introduction

- Denial-of-Service Attacks
 - One of the most common types of attacks
 - Prevent legitimate users from accessing the system

WHAT IS DENIAL OF SERVICE ATTACK?

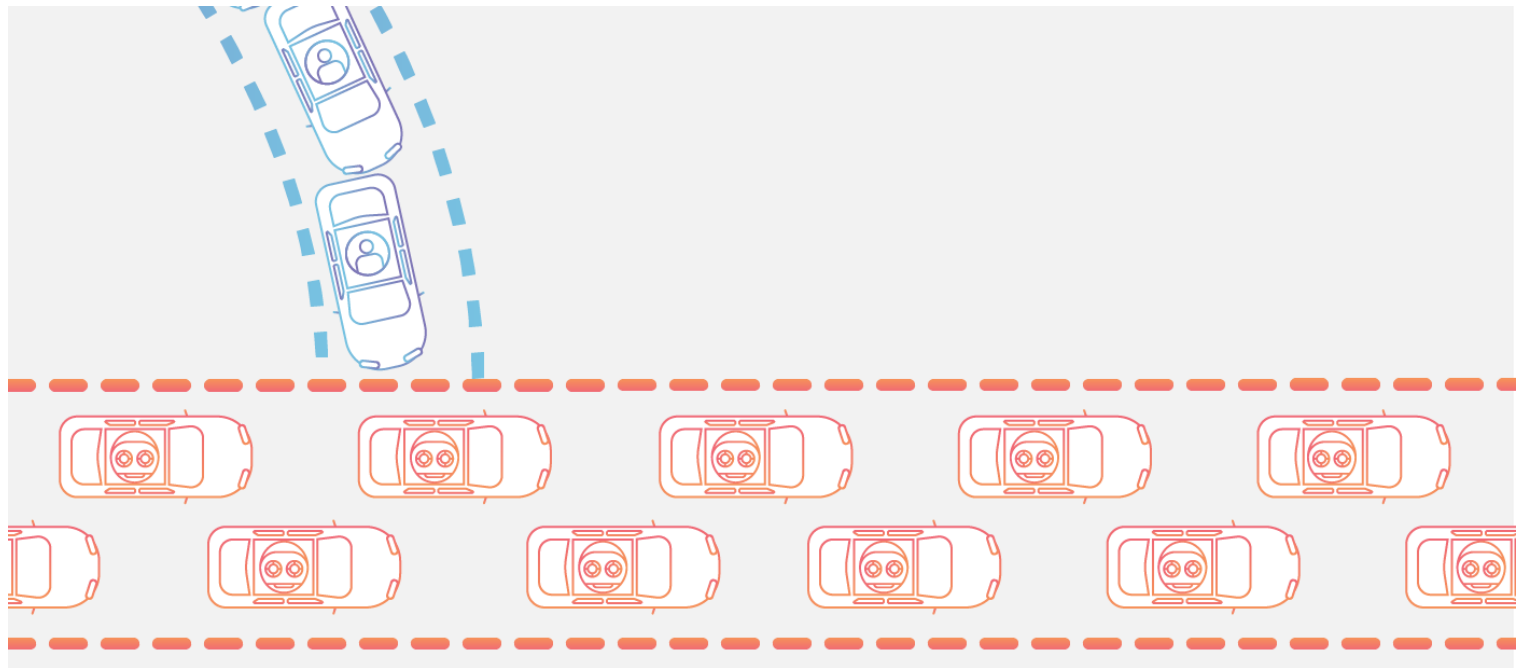
- *Denial-of-service attack*, is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.
- DoS attack, **denial-of-service** attack, is an explicit attempt to make a computer resource unavailable by either injecting a computer virus or flooding the network with useless traffic.

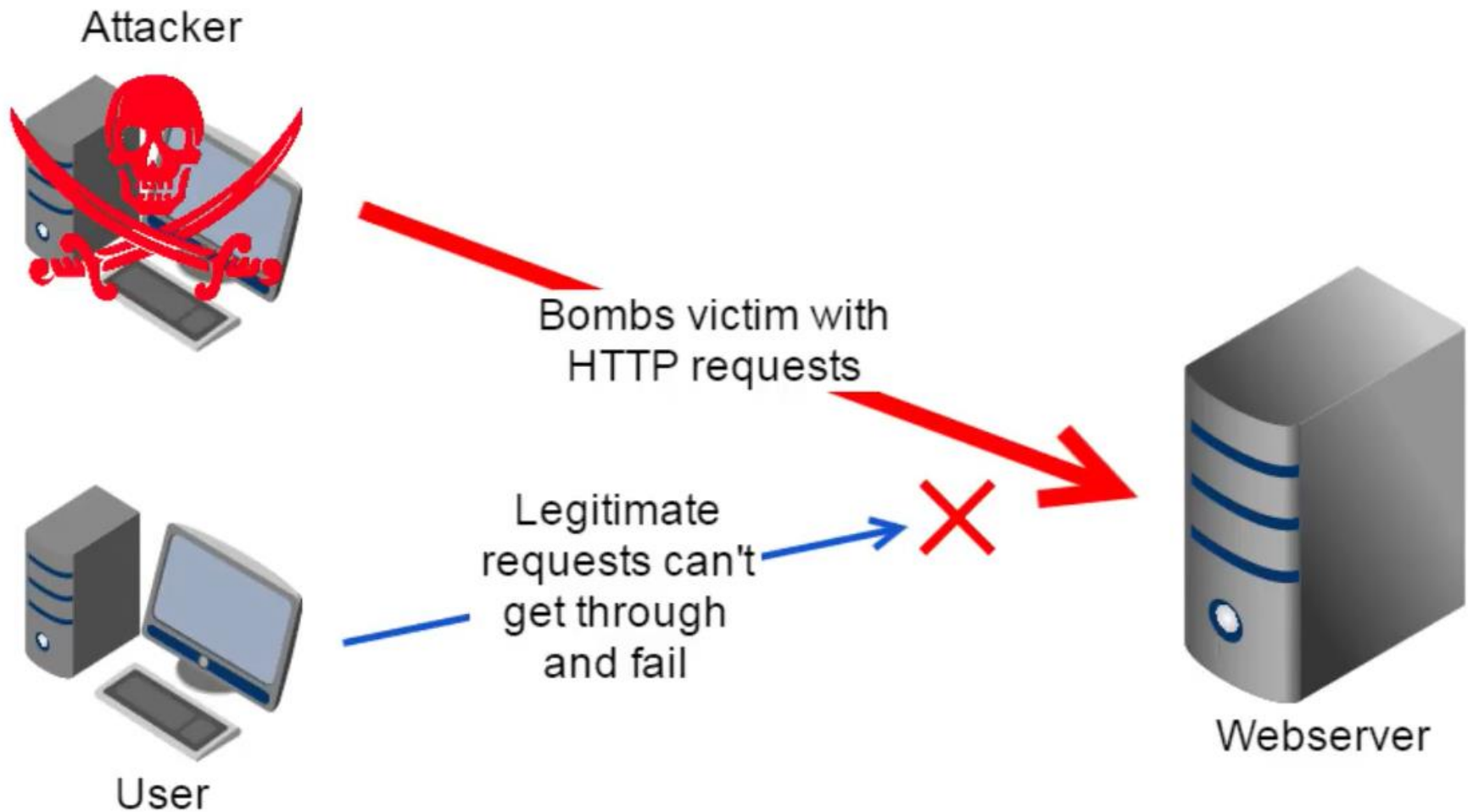
WHAT IS DENIAL OF SERVICE ATTACK?

cont'

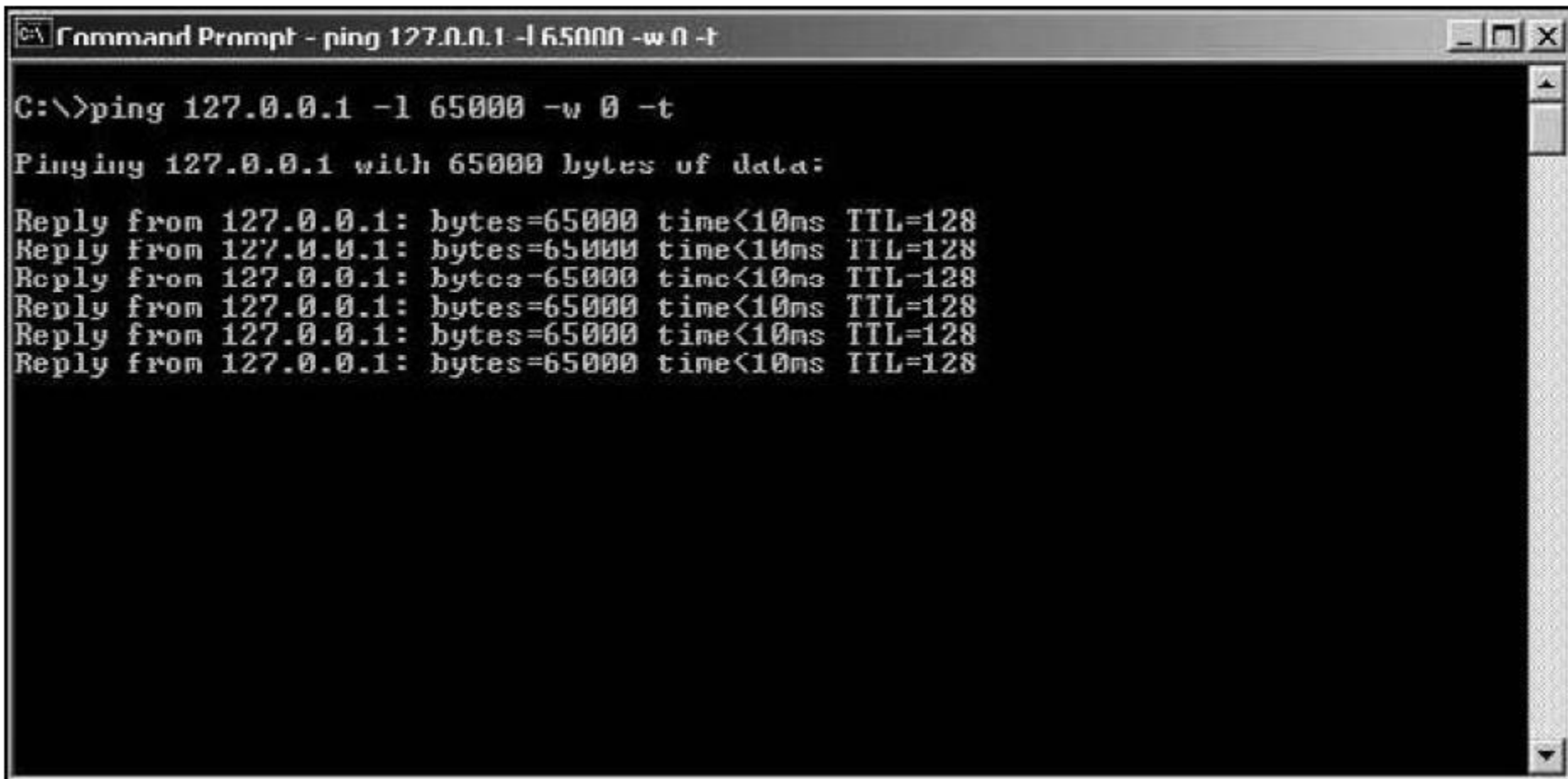
Its aim is to prevent legitimate users by:

- Attempting to flood a network
- To disrupt connections between computers
- Disrupt service to a specific system or person





Ping attack illustration



The screenshot shows a Windows Command Prompt window with the title bar "Command Prompt - ping 127.0.0.1 -l 65000 -w 0 -t". The command prompt shows the command `C:\>ping 127.0.0.1 -l 65000 -w 0 -t` and the output: `Pinging 127.0.0.1 with 65000 bytes of data:` followed by six lines of successful ping replies. Each reply line shows: `Reply from 127.0.0.1: bytes=65000 time<10ms TTL=128`.

```
C:\>ping 127.0.0.1 -l 65000 -w 0 -t

Pinging 127.0.0.1 with 65000 bytes of data:

Reply from 127.0.0.1: bytes=65000 time<10ms TTL=128
Reply from 127.0.0.1: bytes=65000 time<10ms TTL=128
Reply from 127.0.0.1: bytes=65000 time<10ms TTL=128
Reply from 127.0.0.1: bytes=65000 time<10ms TTL=128
Reply from 127.0.0.1: bytes=65000 time<10ms TTL=128
Reply from 127.0.0.1: bytes=65000 time<10ms TTL=128
```

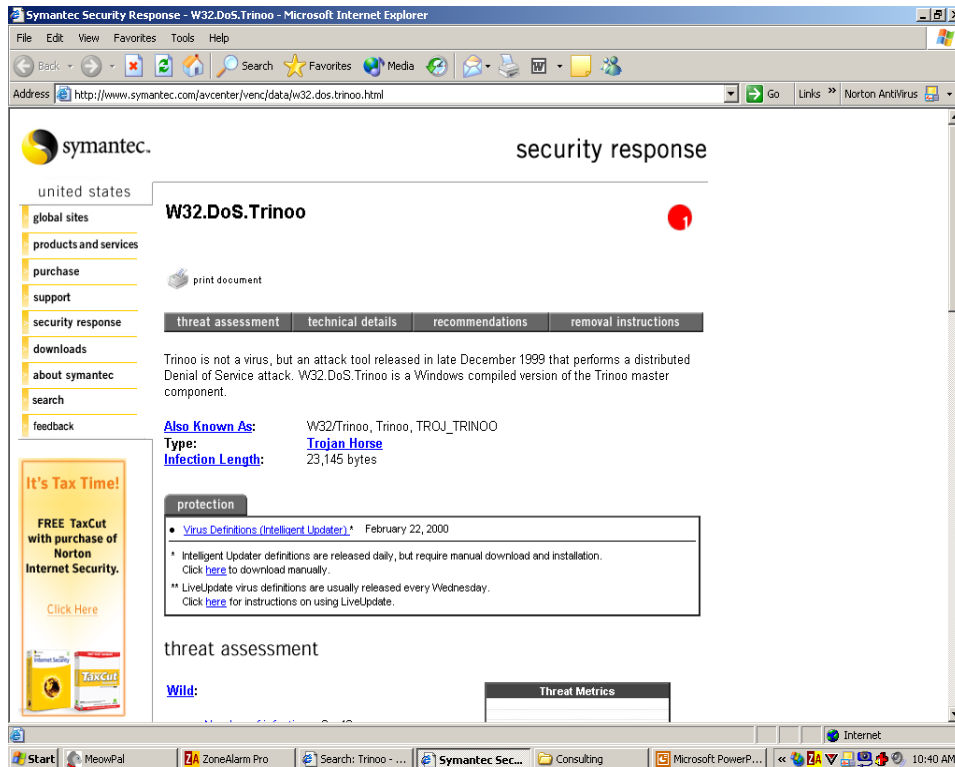

Introduction (cont.)

- Computers have physical limitations
 - Number of users
 - Size of files
 - Speed of transmission
 - Amount of data stored
- Exceed any of these limits and the computer will cease to respond
- Same as cars on highway

Overview

- Common Tools Used for DoS
 - TFN and TFN2K
 - Stacheldracht

Overview (cont.)



Stacheldracht on the Symantec site

Overview (cont.)

- DoS Weaknesses

- The flood must be sustained.
 - When machines are disinfected, the attack stops.
 - Hacker's own machine are at risk of discovery.

Common forms of Attack

- SYN Floods
- Ping of death
- Smurf Attack
- Teardrop Attack
- Ping of flood
- Land Attack

DoS Attacks

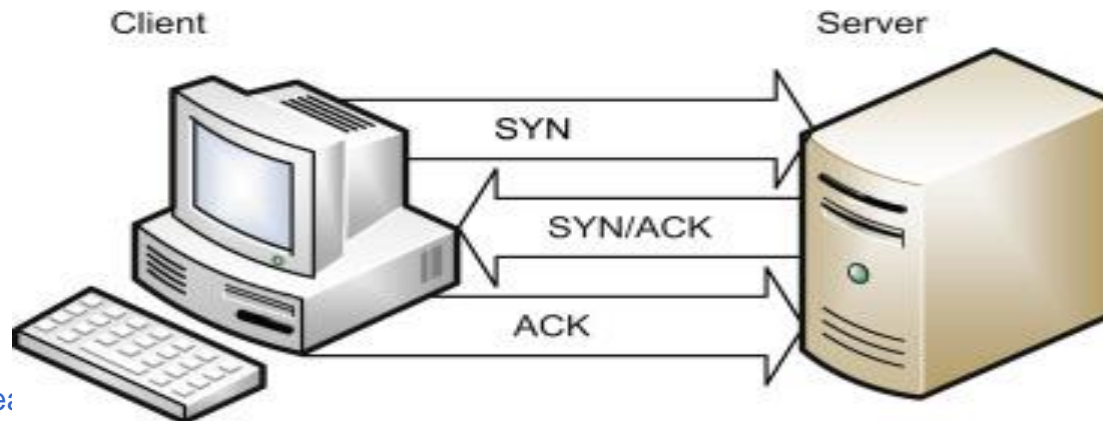
- TCP SYN Flood Attack
 - Hacker sends out a SYN packet.
 - Receiver must hold space in buffer.
 - Bogus SYNs overflow buffer.

SYN Floods

- It takes advantage of the flaw of TCP three-way handshaking behavior.
- Sends many requests to the connection.
- Do not response to replies.
- The SYN flood attack sends TCP connections requests faster than a machine can process them

The three-way handshake

- Client sends a packet with the SYN flag set.
- Server allocates resources for the client and then responds with the SYN and ACK flags set.
- Client responds with the ACK flag set.

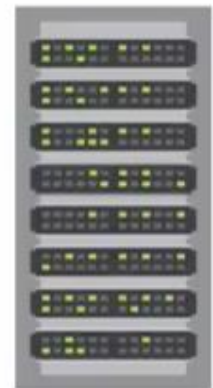




SYNchronize



SYNchronize-**ACK**nowledgement







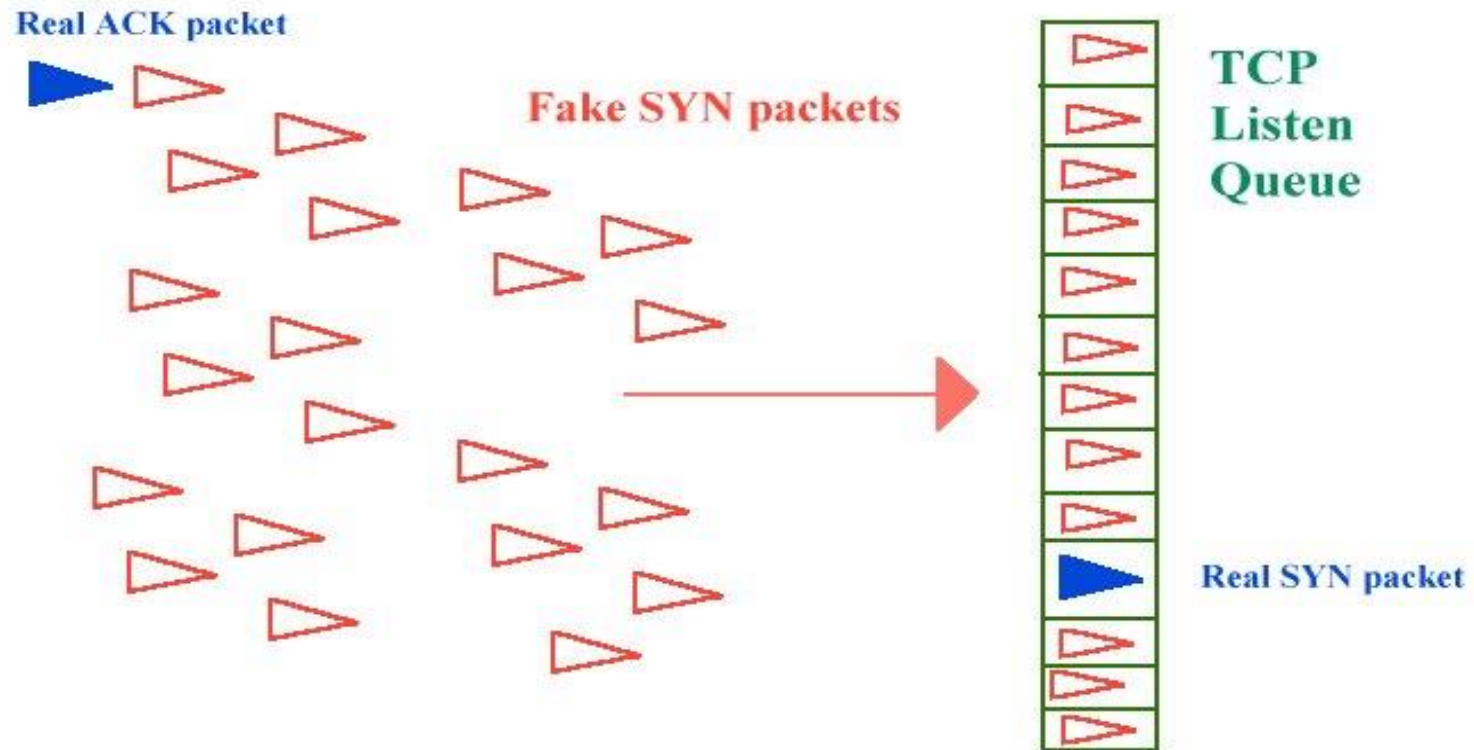
SYNchronize (spoofed source IP address)



SYNchronize-**ACK**nowledgement



DoS Attacks (cont.)



DoS Attacks (cont.)

- Methods of Prevention

- SYN Cookies

- Initially no buffer is created.
 - Client response is verified using a cookie.
 - The SYN+ACK contains a carefully constructed cookie, generated as a hash that contains the IP address, port number, and other information from the client machine requesting the connection
 - Only then is the buffer created.
 - Resource-intensive.
 - Video

Micro Blocks

- Simply allocating a micro-record instead of allocating a complete connection object (an entire buffer segment) to the SYN object.
- In this way, an incoming SYN object can allocate as little as 16 bytes of space, making it significantly more difficult to flood a system.

DoS Attacks (cont.)

- Methods of Prevention

- RST Cookies

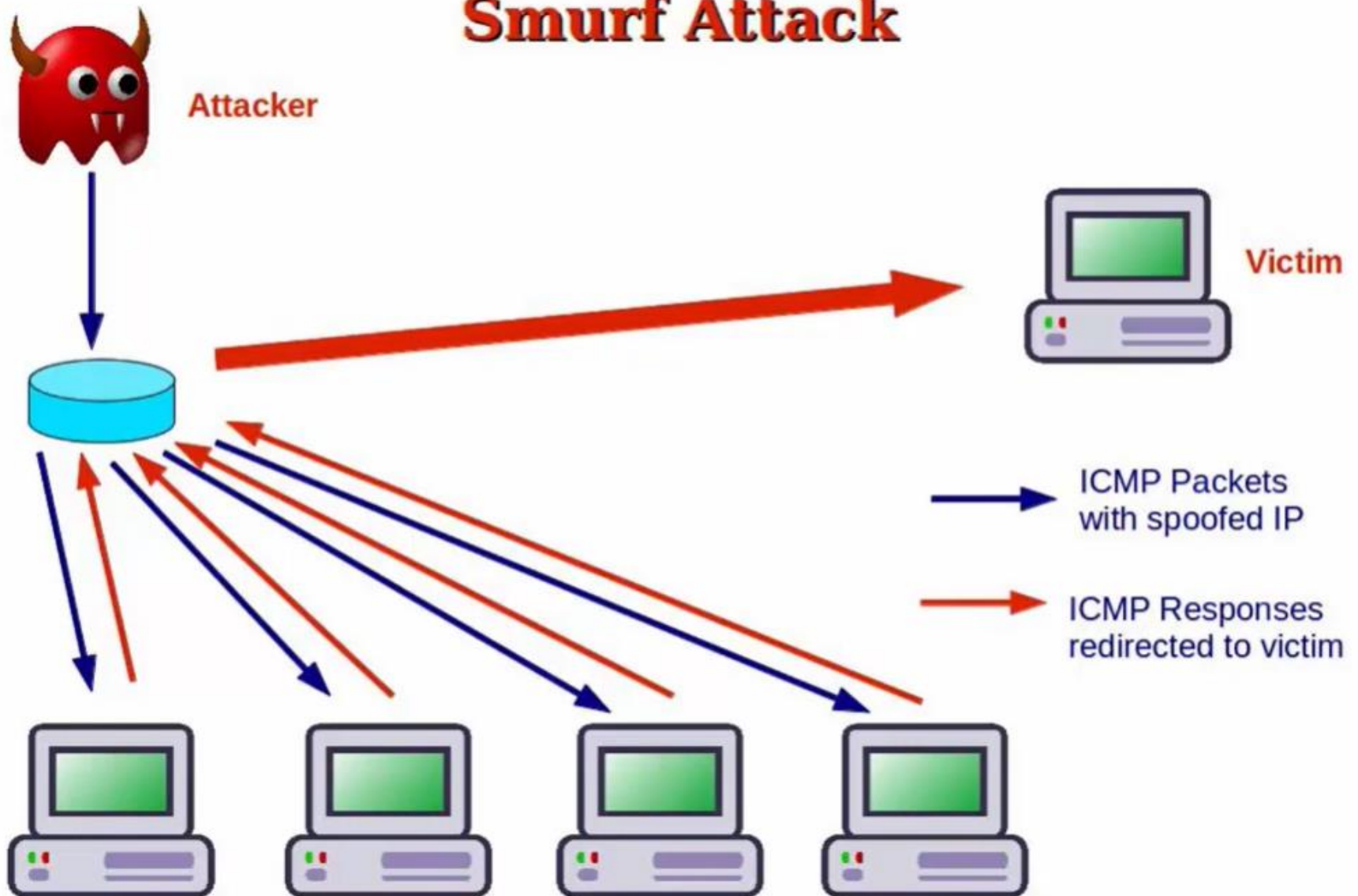
- Sends a false SYNACK back
 - Should receive an RST in reply
 - Verifies that the host is legitimate
 - Not compatible with Windows 95

DoS Attacks (cont.)

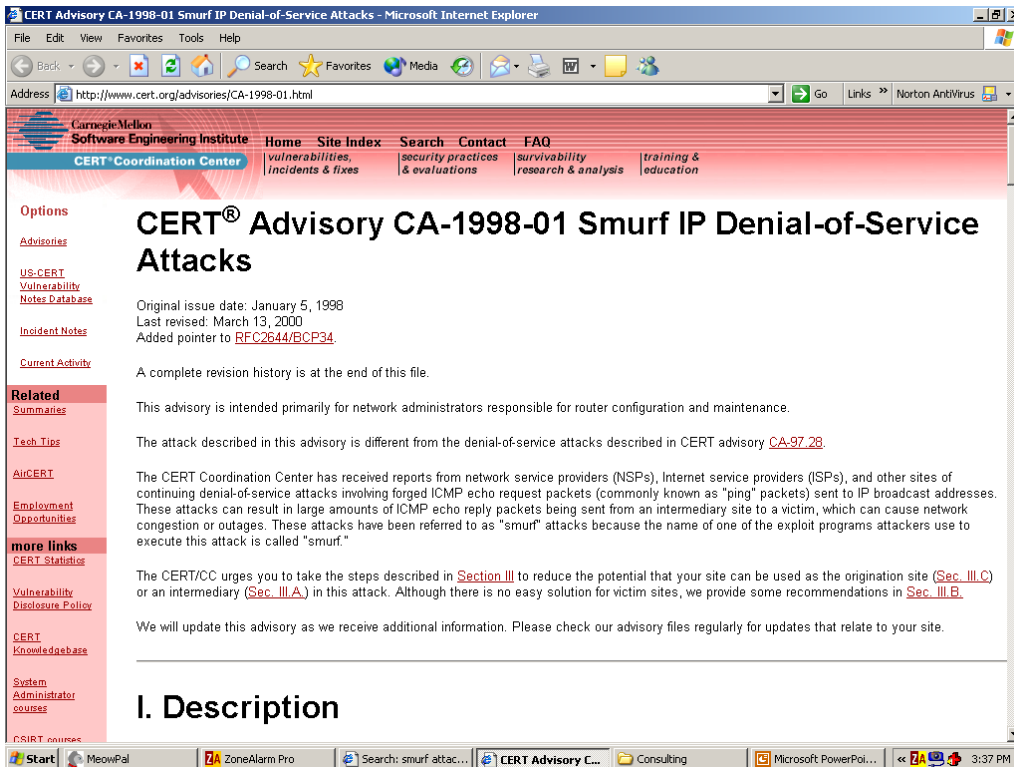
■ Smurf IP Attack

- Hacker sends out ICMP broadcast with spoofed source IP.
 - Intermediaries respond with replies.
 - ICMP echo replies flood victim.
 - The network performs a DDoS on itself.

Smurf Attack



DoS Attacks (cont.)



CERT listing on Smurf attacks

DoS Attacks (cont.)

- Protection against Smurf attacks
 - Guard against Trojans.
 - Have adequate AV software.
 - Utilize proxy servers.
 - Ensure routers don't forward ICMP broadcasts.

DoS Attacks (cont.)

■ UDP Flood Attack

- ❑ Hacker sends UDP packets to a random port
- ❑ When the target system receives a UDP packet, it automatically determines what application is waiting on the destination port
- ❑ In this case, since there is no application waiting on the port, the target system will generate an ICMP packet of “destination unreachable” and attempt to send it back to the forged source address.

DoS Attacks (cont.)

- Floods – Broadcasts of pings

Ping of flood (ICMP Flood Attack)

- Attacker simply sends a huge number of "ICMP Echo Requests(ping)" to the victim.
- It sends ICMP packets as fast as possible without waiting for replies.
- The continuing combination of requests and replies can slow the network or, in extreme cases, to disconnect.

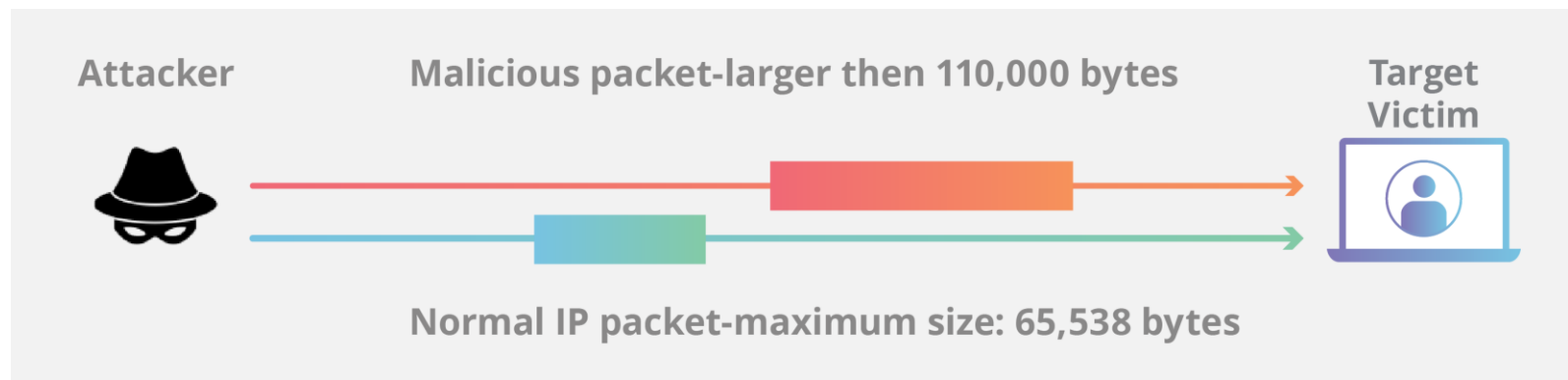
Ping of death

- Is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the bytes allowed by the IP protocol. Since the received ICMP(Internet Control Message Protocol) echo request packet is bigger than the normal IP packet size, the victim cannot reassemble the packets. The OS may be crashed or rebooted as a result.

- Sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.
- “ping”, is a network utility used to test a network connection, and it works much like sonar – a “pulse” is sent out and the “echo” from that pulse tells the operator information about the environment.
- If the connection is working, the source machine receives a reply from the targeted machine.

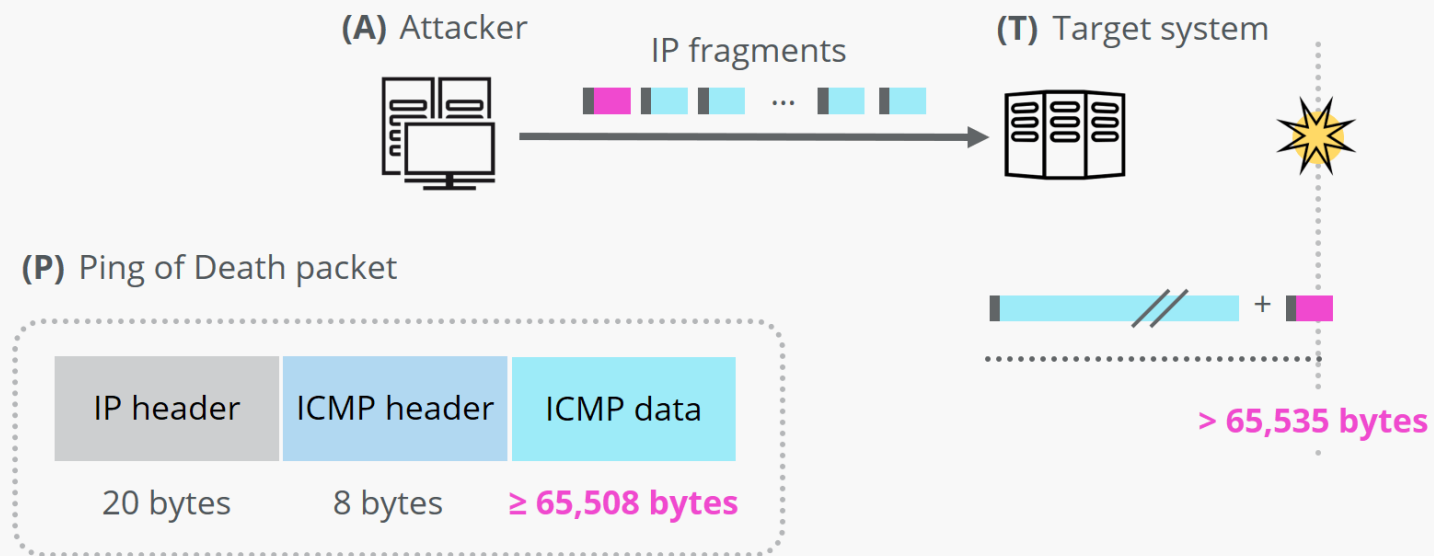
- IP4 ping packets are much larger, and can be as large as the maximum allowable packet size of 65,535 bytes.
- Some TCP/IP systems were never designed to handle packets larger than the maximum, making them vulnerable to packets above that size.
- When a maliciously large packet is transmitted from the attacker to the target, the packet becomes fragmented into segments, each of which is below the maximum size limit

- When the target machine attempts to put the pieces back together, the total exceeds the size limit and a buffer overflow can occur, causing the target machine to freeze, crash or reboot



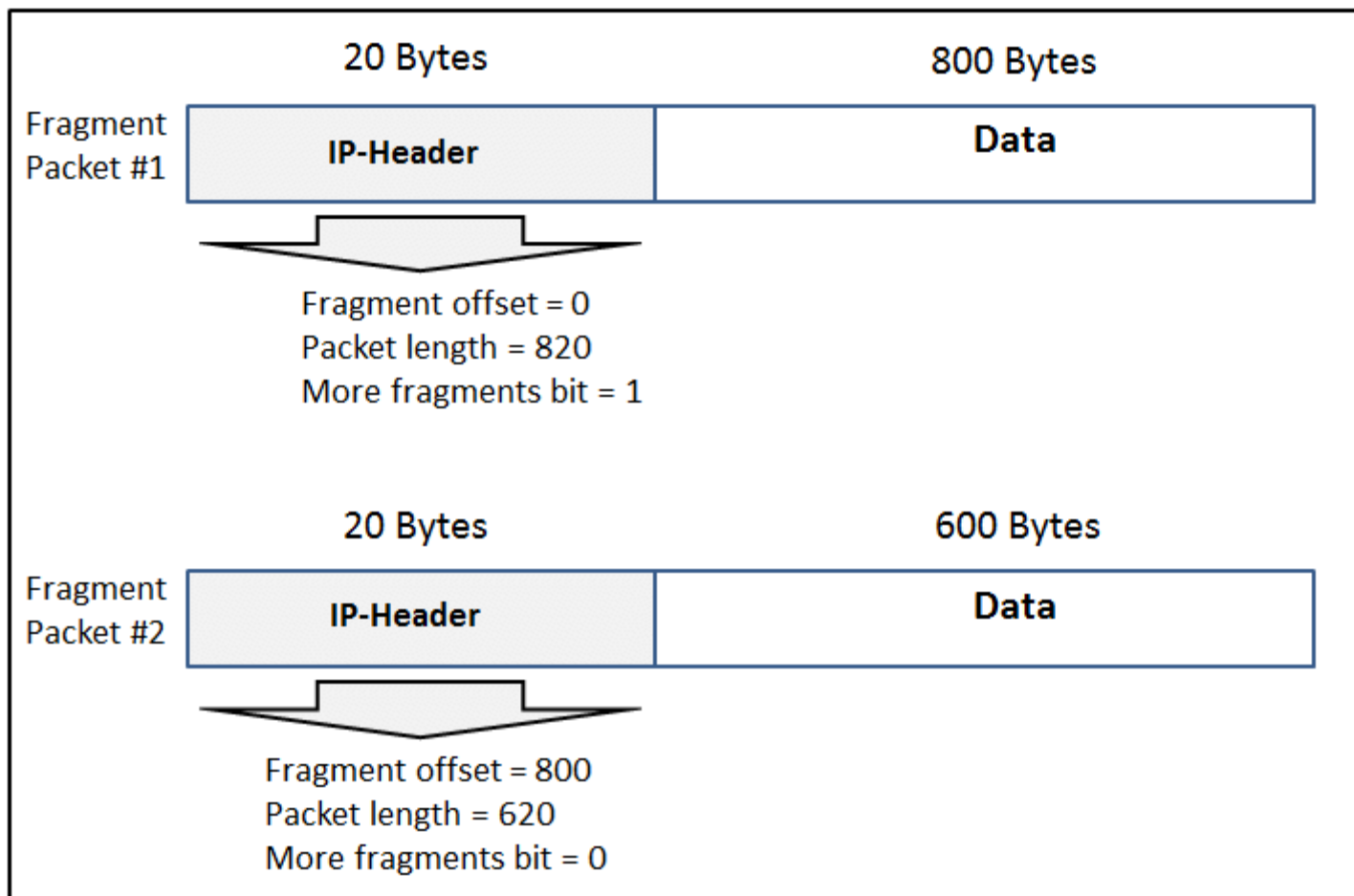
Ping of Death

How it works



Teardrop Attack

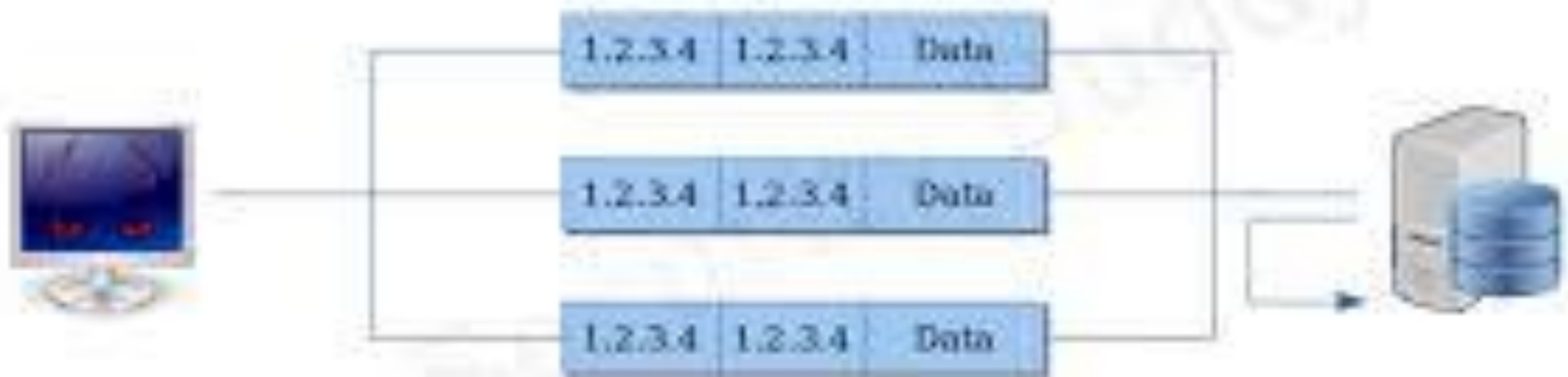
- Divides large files into fragments.
- An attacker sends two fragments that cannot be reassembled properly by manipulating the header of packet and cause reboot or halt of victim system.



DoS Attacks (cont.)

■ Land Attack

- Simplest of all attacks
- Hacker sends packet with the same source and destination IP
- System “hangs” attempting to send and receive message



Distributed Denial of Service (DDoS)

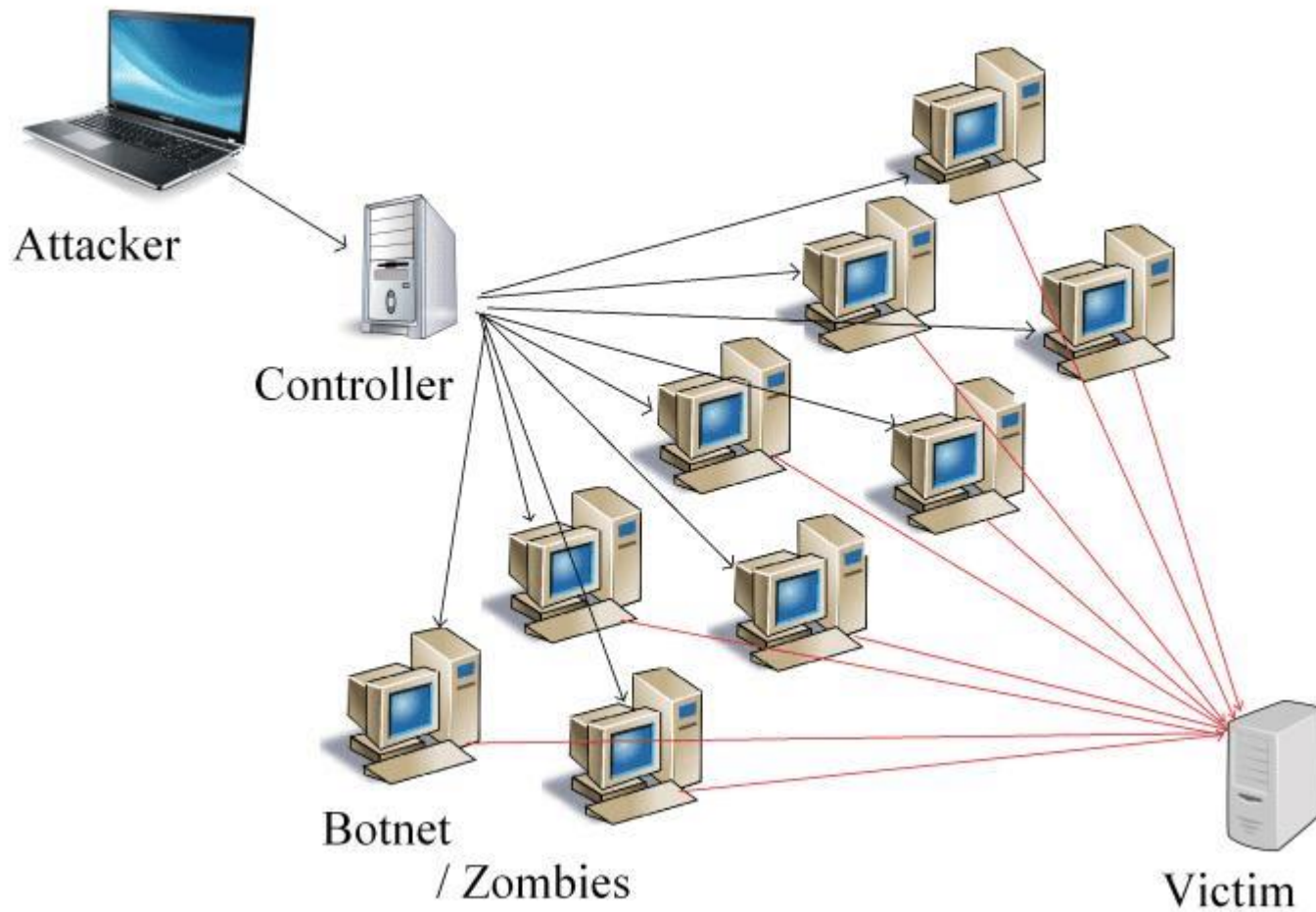
- DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices.

Distributed Denial of Service (DDoS)

- These networks consist of computers and other devices (such as IoT devices) which have been infected with malware, allowing them to be controlled remotely by an attacker. These individual devices are referred to as bots (or zombies), and a group of bots is called a botnet.
- Once a botnet has been established, the attacker is able to direct an attack by sending remote instructions to each bot.

D DoS

- When a victim's server or network is targeted by the botnet, each bot sends requests to the target's IP address, potentially causing the server or network to become overwhelmed, resulting in a denial-of-service to normal traffic.

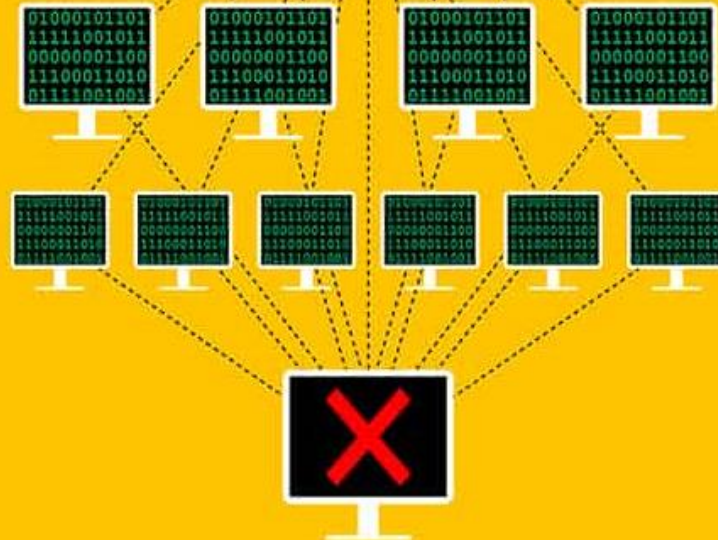


```
01000101101
11111001011
00000001100
11100011010
01111001001
```



DoS attack

```
01000101101
11111001011
00000001100
11100011010
01111001001
```



DDoS attack

Real-World Examples

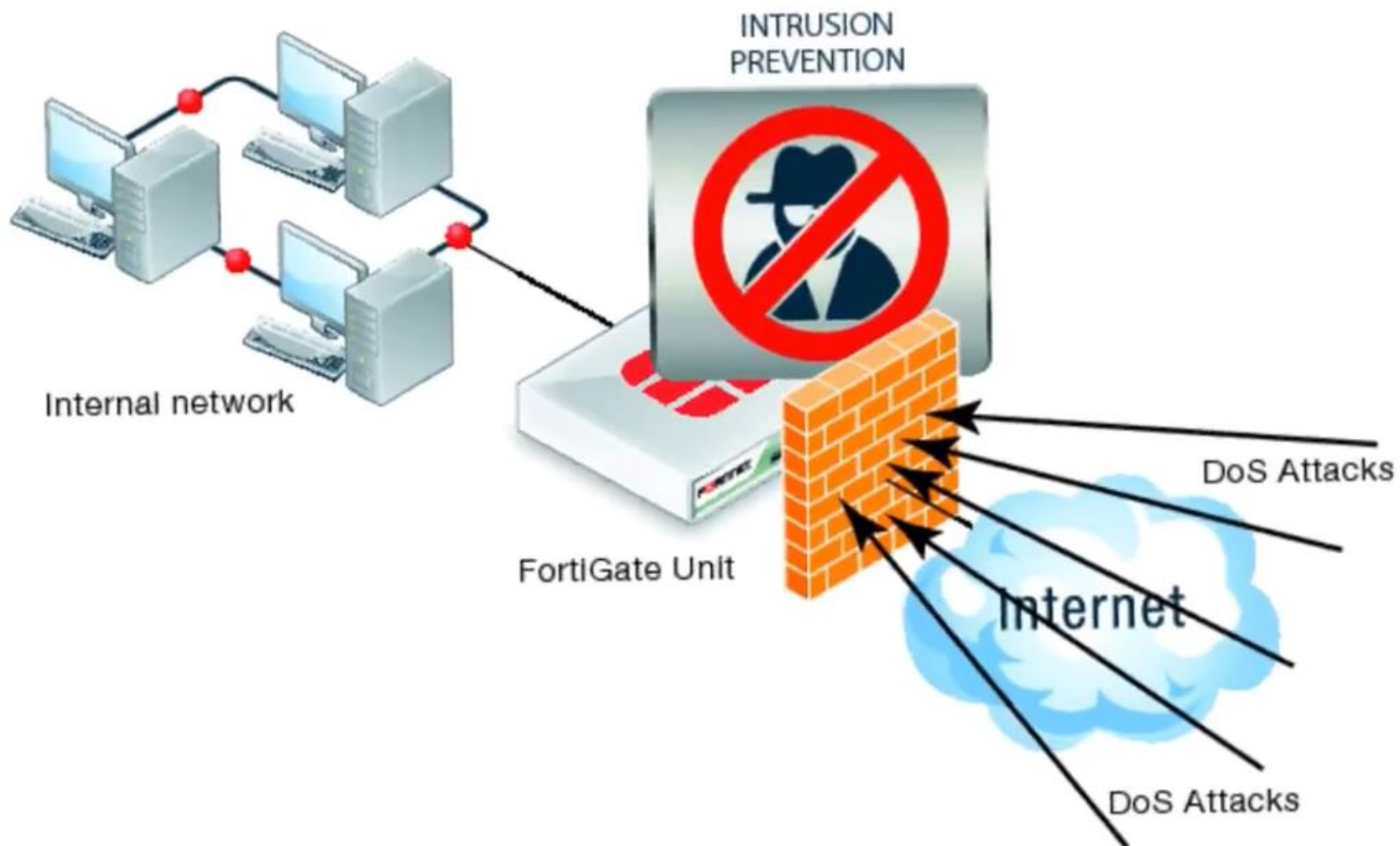
- MyDoom
 - Worked through e-mail

How to Defend Against DoS Attacks

- In addition to previously mentioned methods
 - Configure your firewall to
 - Filter out incoming ICMP packets.
 - Disallow any incoming traffic.
 - Use tools such as NetStat and others.

How to Defend Against DoS Attacks (cont.)

- Disallow traffic not originating within the network.
- Disable all IP broadcasts.
- Filter for external and internal IP addresses.
- Keep AV signatures updated.
- Keep OS and software update.
- Have an Acceptable Use Policy.



Summary

- DoS attacks are common.
- DoS attacks are unsophisticated.
- DoS attacks are devastating.
- Your job is constant vigilance.