

# Malicious Software and Denial of service attacks

Introduction to Denial of Service (DoS)



# Video Summary

- What is DoS attack?
- Flooding Attacks
- Classic DoS (TCP SYN Flood)

# 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.”

CIA + DoS  
Availability

# 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)

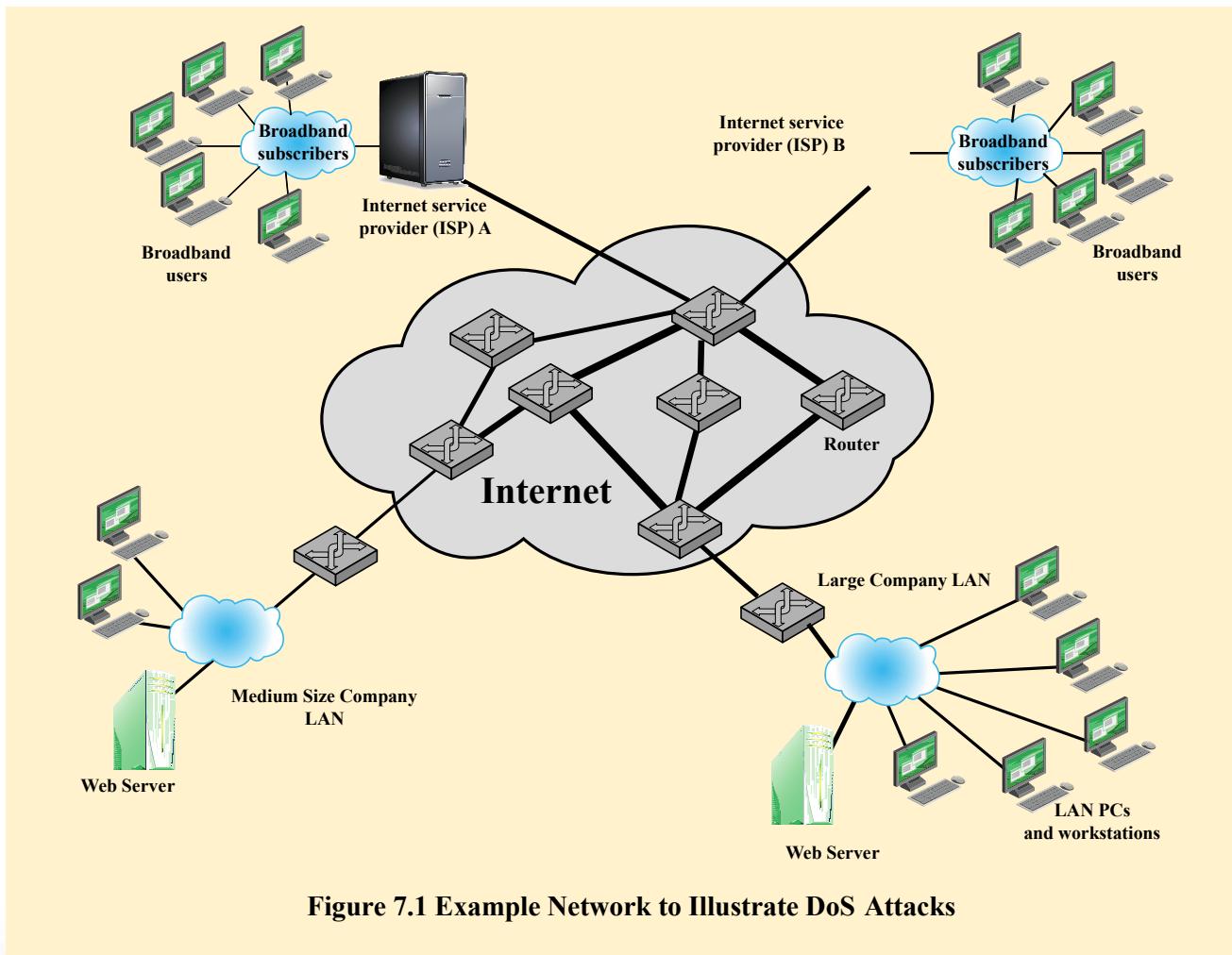
## System resources

Aims to overload or crash the network handling software by sending special packets that consume resources of trigger bug(s)

## 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





**Figure 7.1 Example Network to Illustrate DoS Attacks**