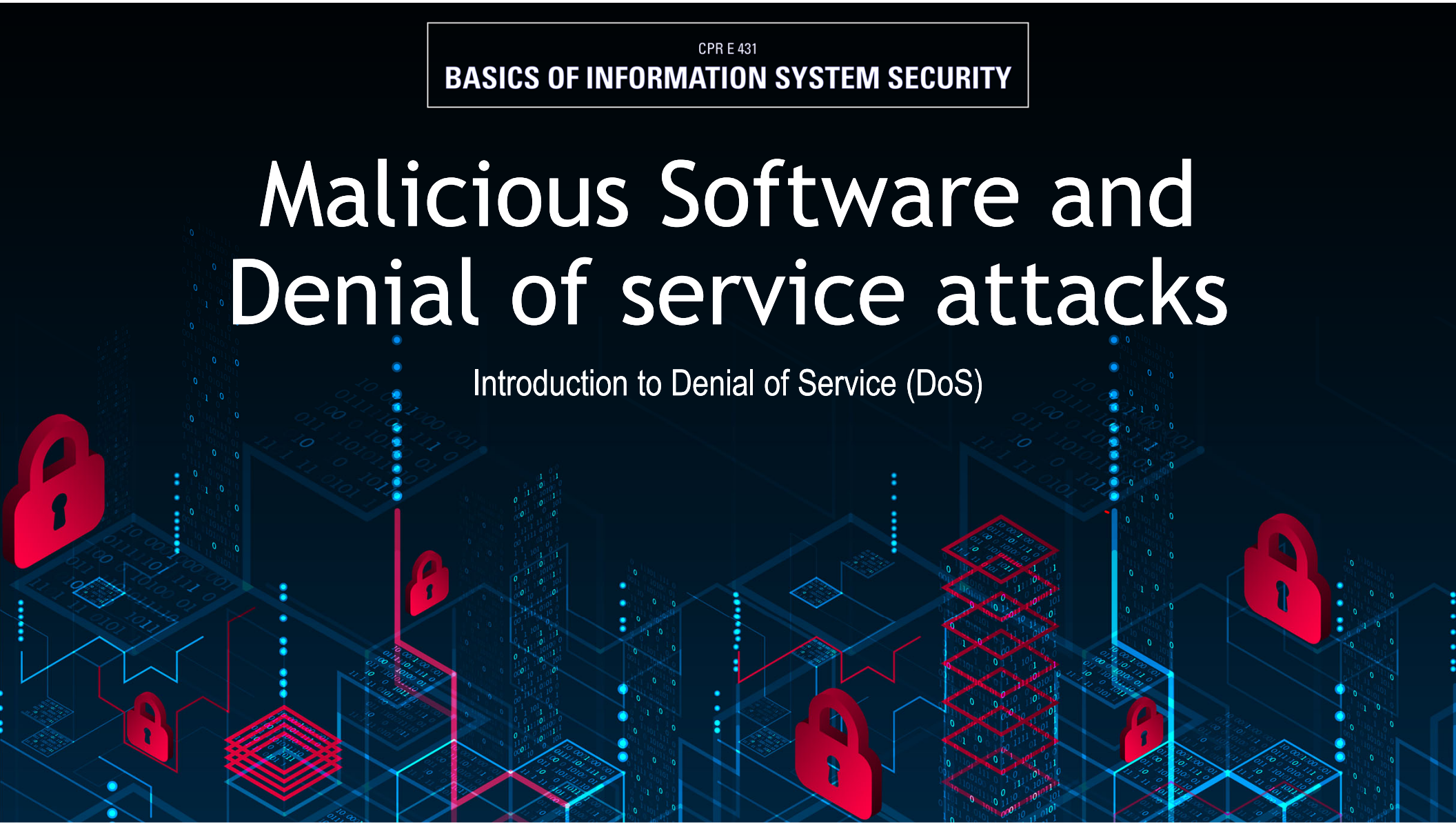
CPR E 431

BASICS OF INFORMATION SYSTEM SECURITY

Malicious Software and Denial of service attacks

Introduction to Denial of Service (DoS)



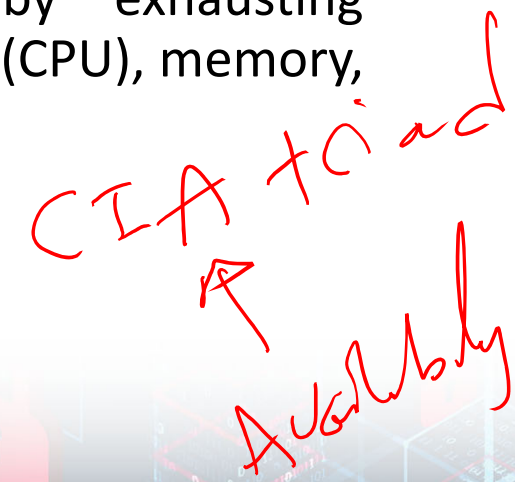
Video Summary

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

Denial-of-Service (DoS) Attack

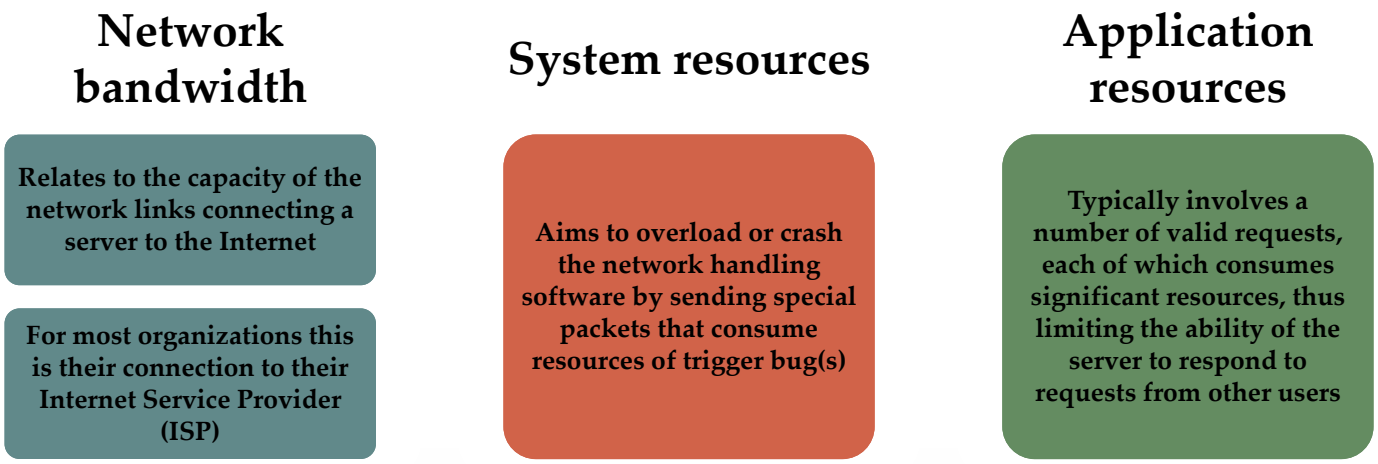
The NIST Computer Security Incident Handling Guide defines a DoS attack as:

"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."



Denial-of-Service (DoS)

- A form of attack on the availability of some service
- Categories of resources that could be attacked are:



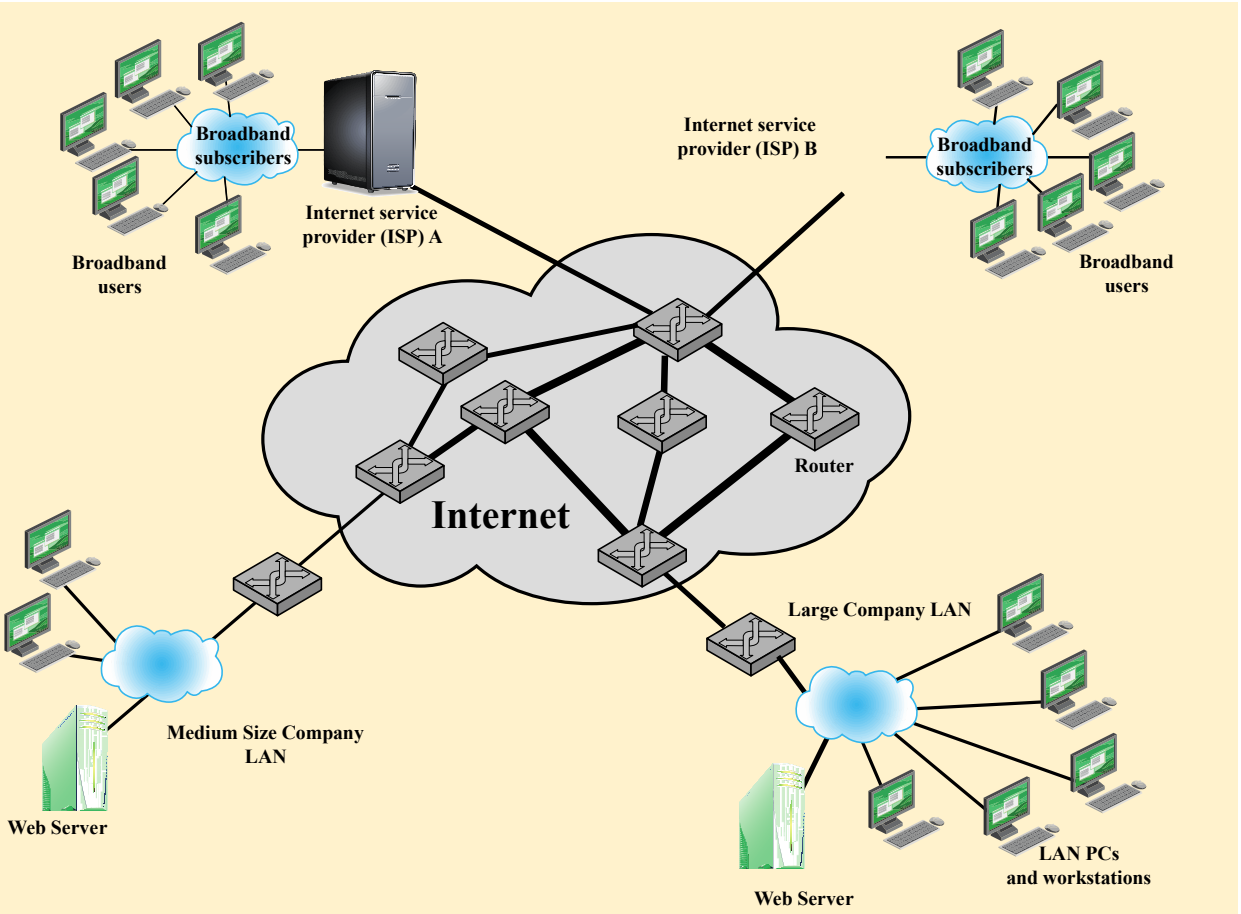


Figure 7.1 Example Network to Illustrate DoS Attacks