2nd session on 1st Feb 2020

Network security essentials

Introduction

Network Security Essentials

01-02-2020 Network security-II:

- What the global scope of cyberattacks is
- What you are trying to protect
- Whom you are trying to catch
- What kinds of tools are used to attack computer systems
- What a security breach is
- What risks, vulnerabilities, and threats are
- What malware is
- What a malicious software attack is
- What a social engineering attack is
- What a wireless network attack is
- What a web application attack is
- What countermeasures are

Learning objectives

- **Identify malicious software and implement countermeasures**
- **Identify common attacks and develop appropriate countermeasures**
- **Recognize social engineering and reduce the risks associated with it**
- **Recognize threats and types of attacks on wireless networks**
- **Recognize threats and types of attacks on web applications**
- **Describe how malicious attacks, threats, and vulnerabilities impact an IT infrastructure.**

Network security-2

- Contemporary Security Challenges and Vulnerabilities
- Internet Vulnerabilities
- Security Threats in the Environment
- Vulnerable Points in an E-commerce Environment
- Most Common network Security Threats
- Malicious Software: Viruses, Worms, Trojan Horses, and Spyware
- Hackers and Computer Crime
- Internal Threats: Employees
- Software Vulnerability
- Phising Hacking and Cybervandalism Credit Card Fraud Spoofing (Pharming) and Spam (Junk) Web Sites
- DoS and DDoS Attacks
- Other Security Threats
- What Is the Business Value of Security and Control?
- Digital forensic/IT Act 2000

Following topics we will discuss in the session

- Malicious software and countermeasures
- Common attacks and countermeasures
- Social engineering and how to reduce risks
- Threats and types of attacks on wireless networks
- Threats and types of attacks on web applications

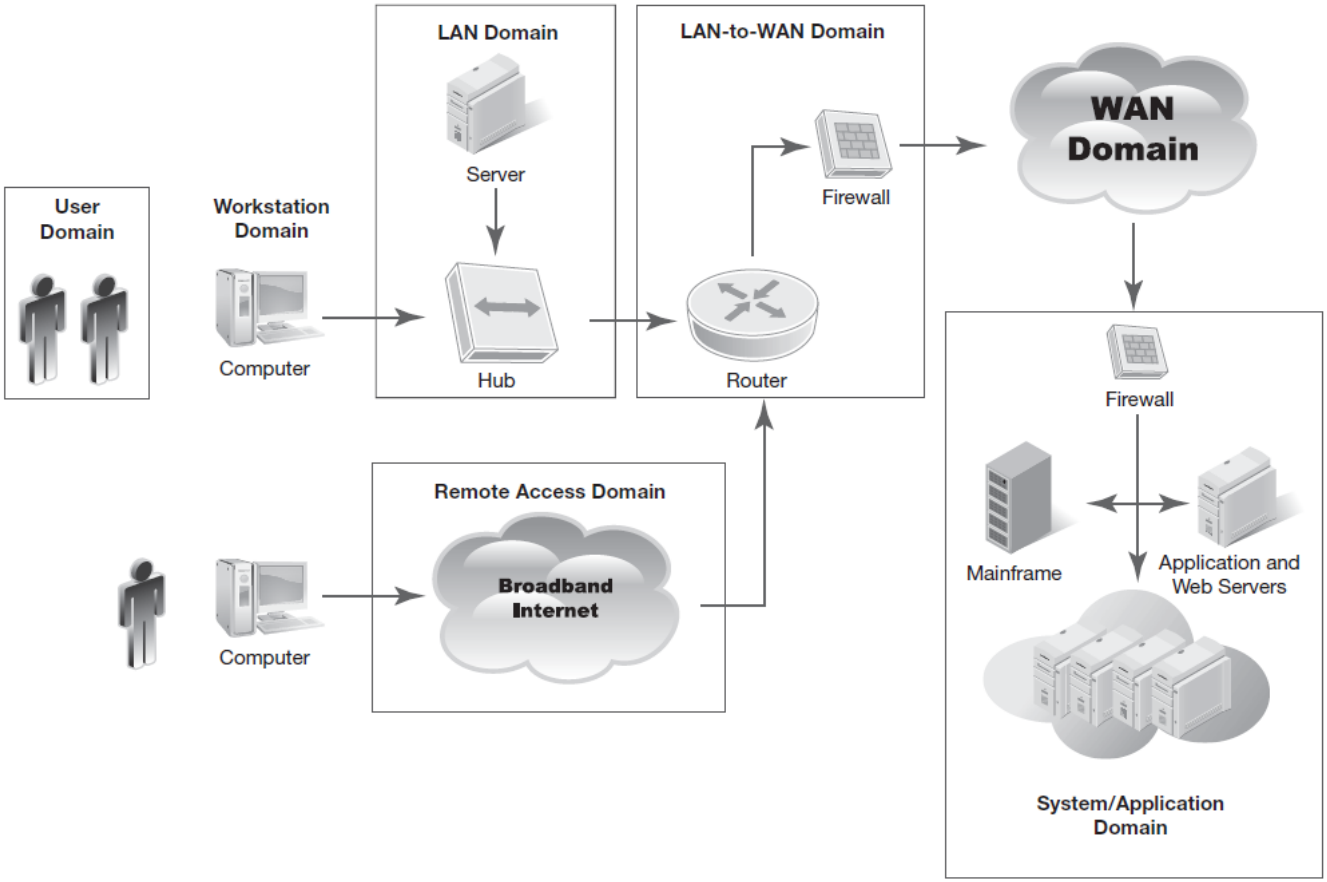
Malicious Activity on the Rise

- Examples of the malicious attacks are everywhere
- Data breaches occur in both public and private sectors
- In 2013, China was top country of origin for cyberattacks, at 41 percent
- United States was second at 10 percent

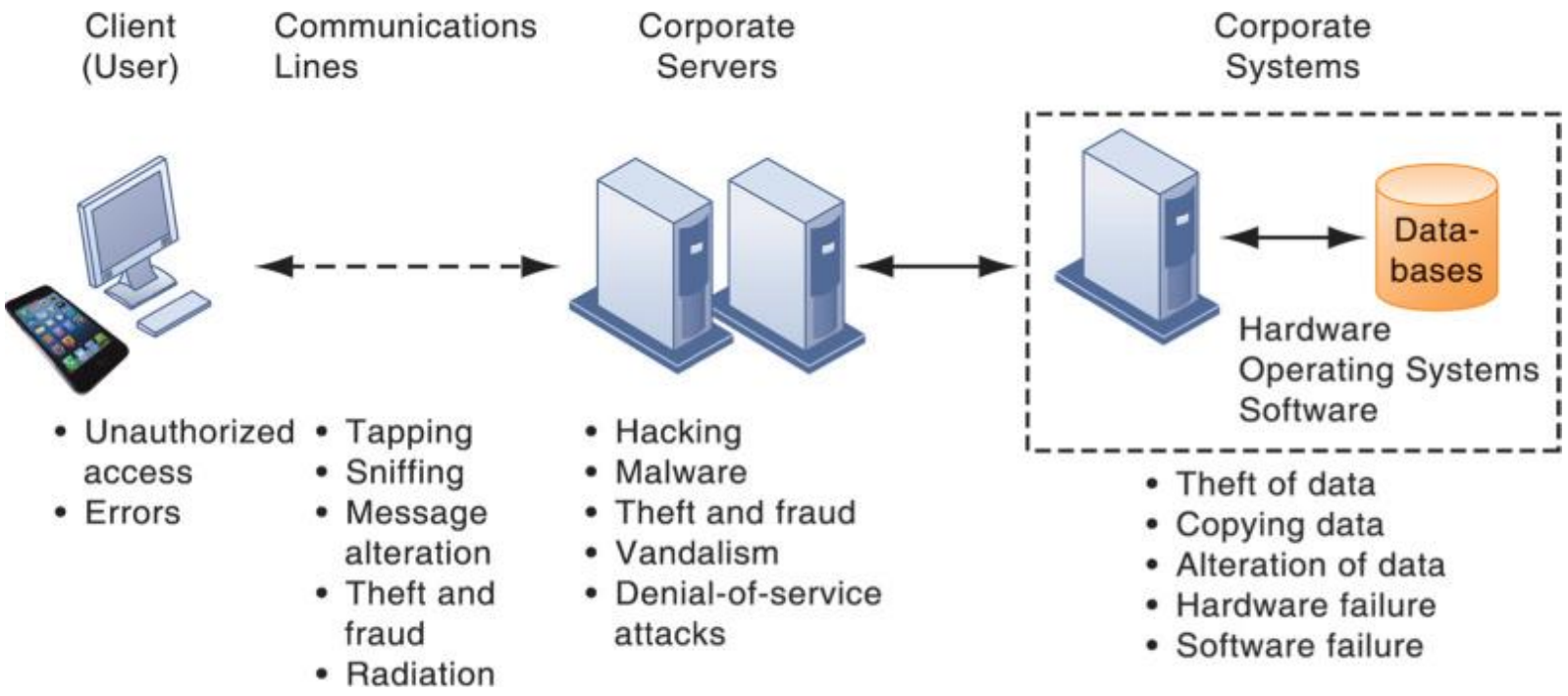
What Are You Trying to Protect?

- **Customer data**—Name, address, phone, Social Security number (SSN), date of birth, cardholder data, protected health care information.
- **IT assets and network infrastructure**—Hardware, software, and services.
- **Intellectual property**—Sensitive data such as patents, source code, formulas, or engineering plans.
- **Finances and financial data**—Bank accounts, credit card data, and financial transaction data.
- **Service availability and productivity**—The ability of computing services and software to support productivity for humans and machinery.
- **Reputation**—Corporate compliance and brand image.

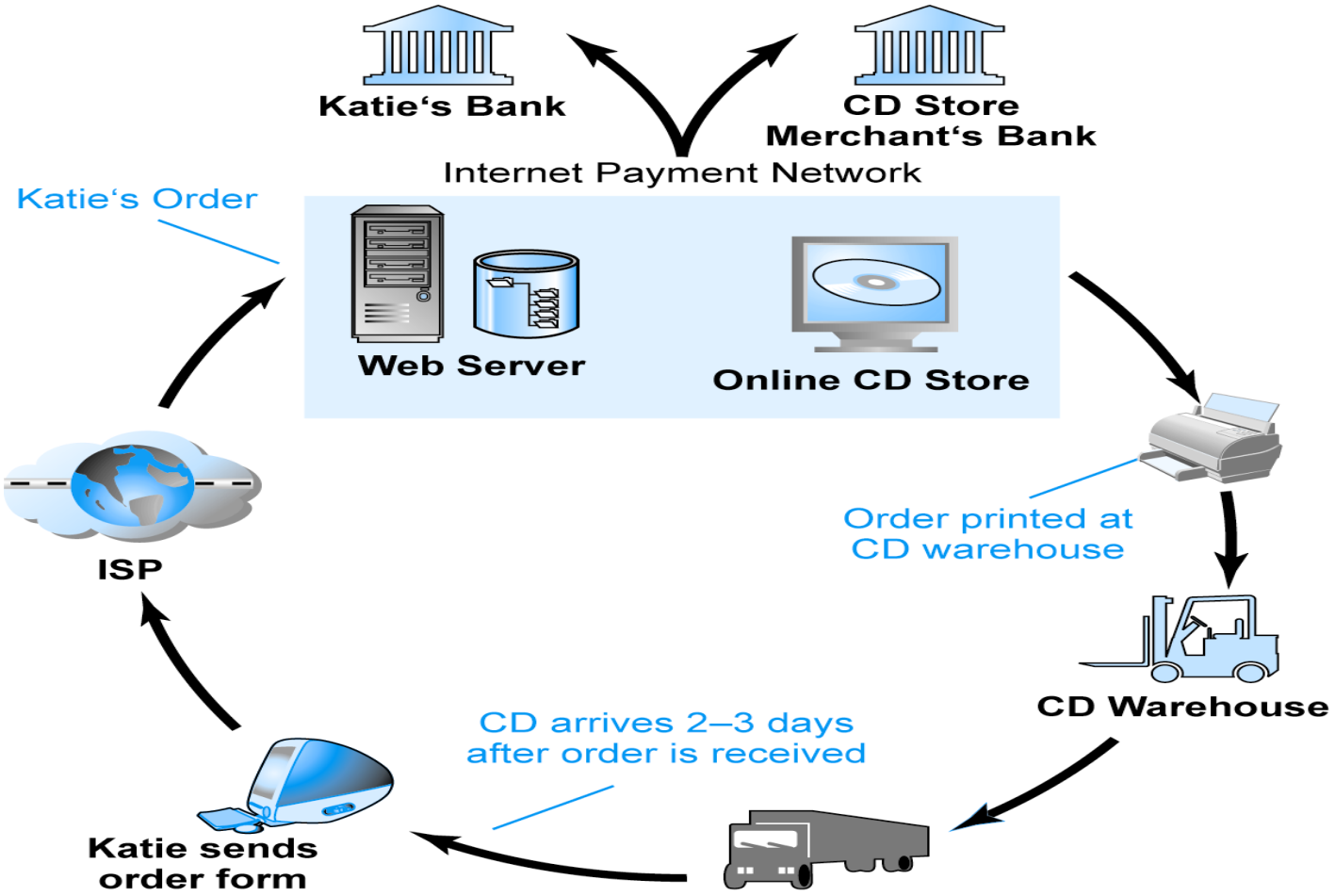
What Are You Trying to Protect?



Contemporary Security Challenges and Vulnerabilities



A Typical E-commerce Transaction in a network environment

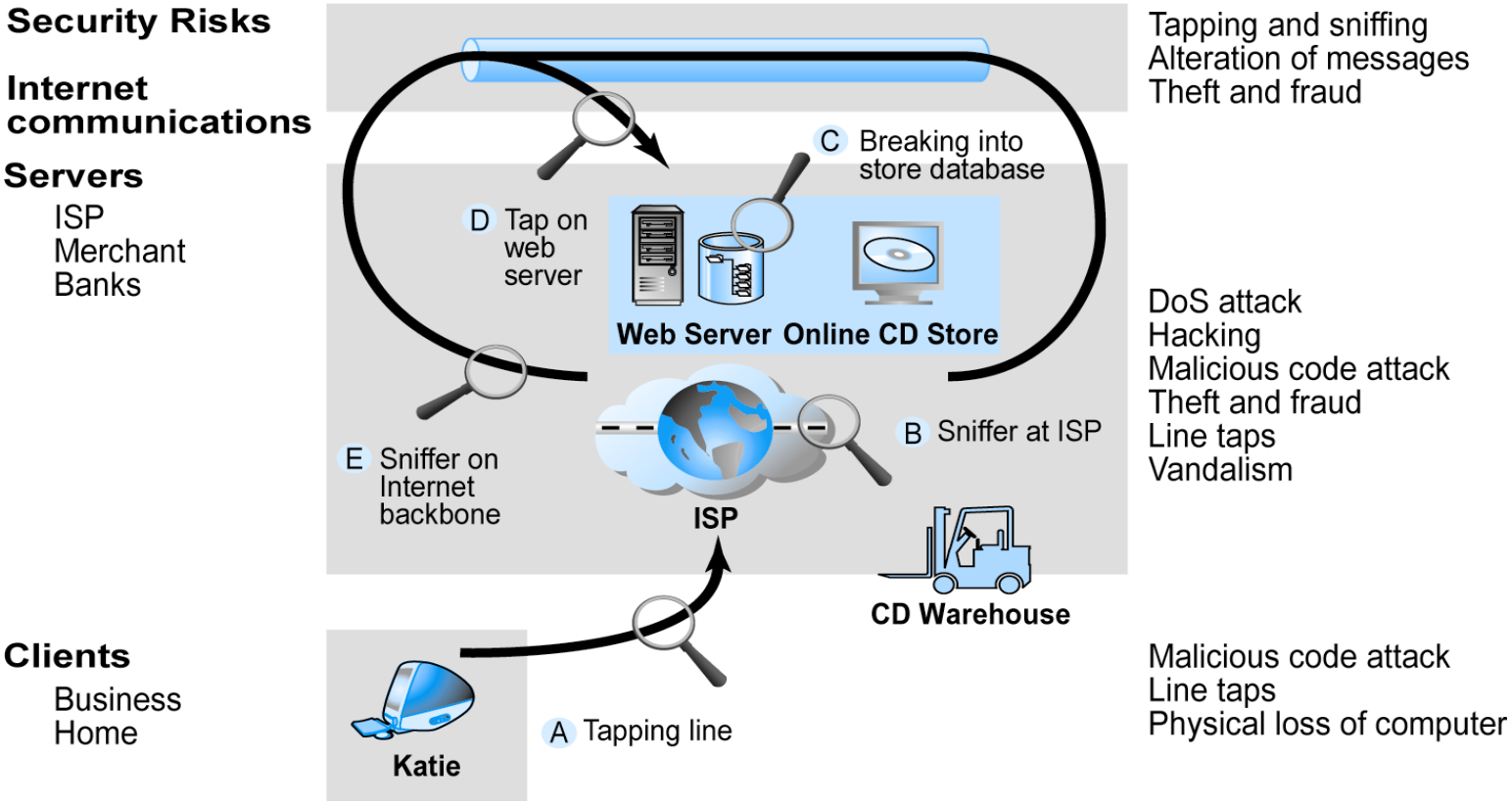


SOURCE: Boncella, 2000.

Why Systems Are Vulnerable

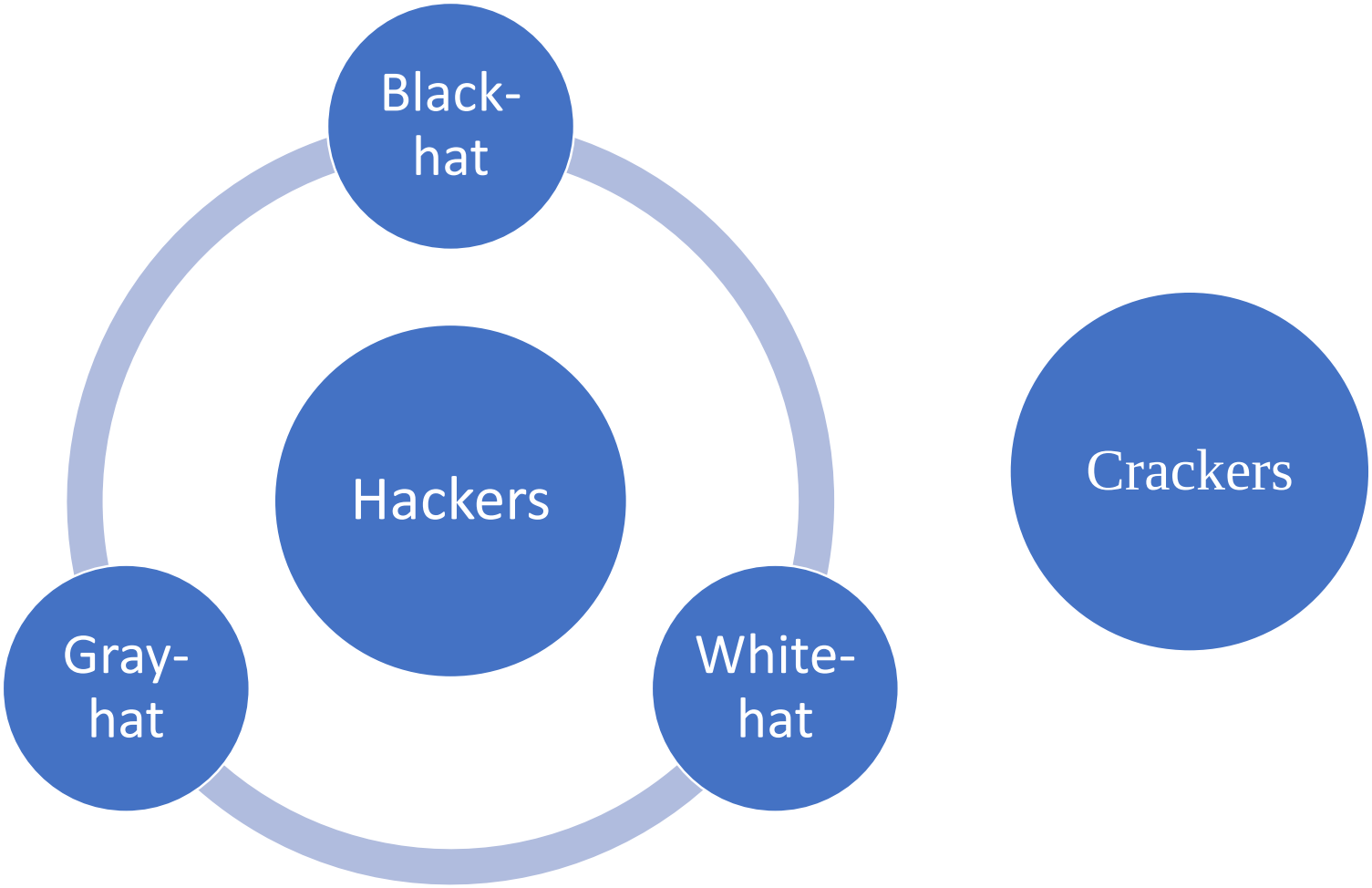
- Accessibility of networks
- Hardware problems (breakdowns, configuration errors, damage from improper use or crime)
- Software problems (programming errors, installation errors, unauthorized changes)
- Disasters
- Use of networks/computers outside of firm's control
- Loss and theft of portable devices

Vulnerable Points in an E-commerce Environment



SOURCE: Boncella, 2000.

Whom Are You Trying to Catch?



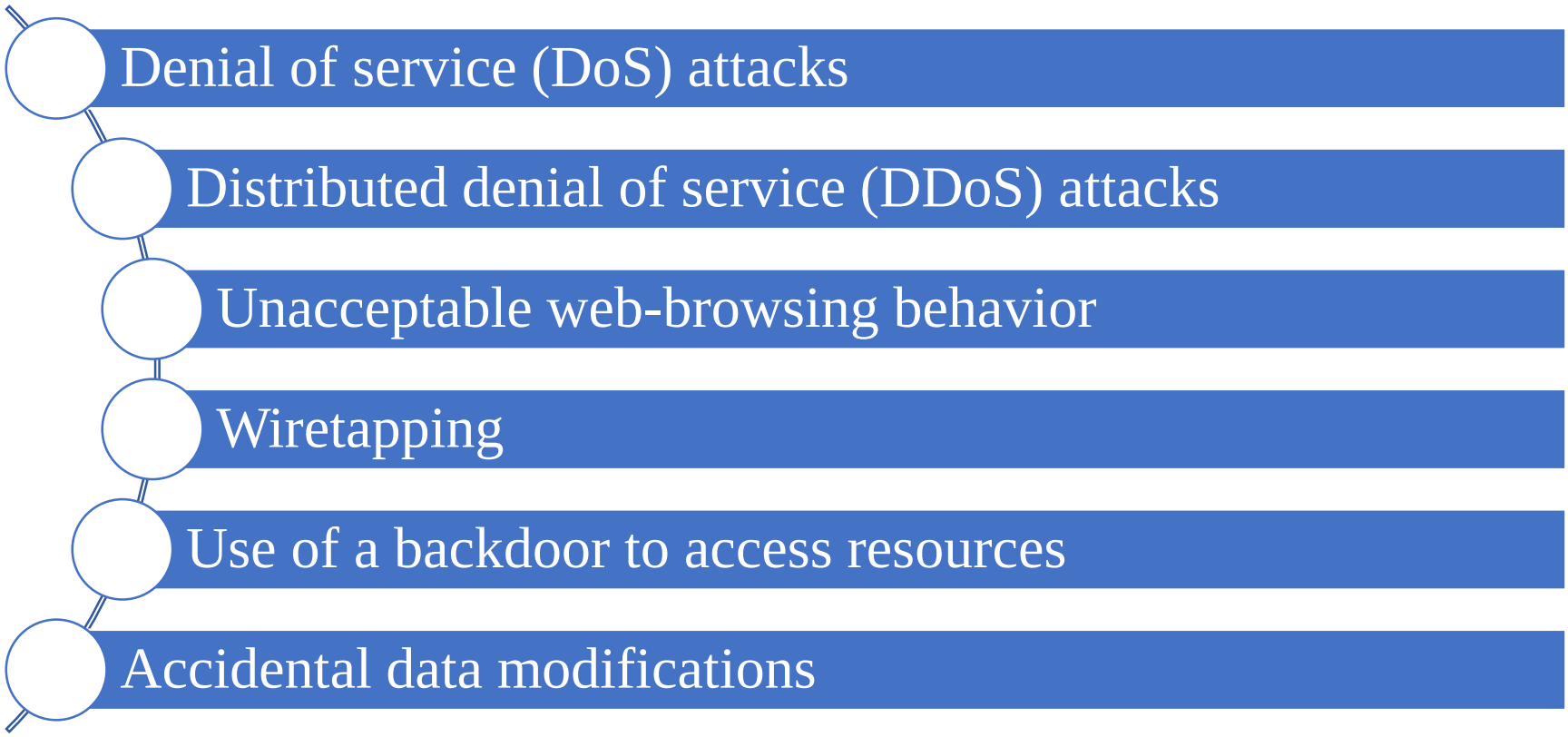
Cyber Attack Tools

- Protocol analyzers (sniffers)
- Port scanners
- OS fingerprint scanners
- Vulnerability scanners
- Exploit software
- Wardialers
- Password crackers
- Keystroke loggers

What Is a Security Breach?

- Any event that results in a violation of any of the C-I-A security tenets
- Some security breaches disrupt system services on purpose
- Some are accidental and may result from hardware or software failures

Activities that Cause Security Breaches



Denial of Service Attack

- A coordinated attempt to deny service by occupying a computer to perform large amounts of unnecessary tasks
  - Logic attacks
  - Flooding attacks
- Protect using
  - Intrusion prevention system (IPS)
  - Intrusion detection system (IDS)
- Attacks launched using
  - SYN flood
  - Smurfing

Distributed Denial of Service Attack

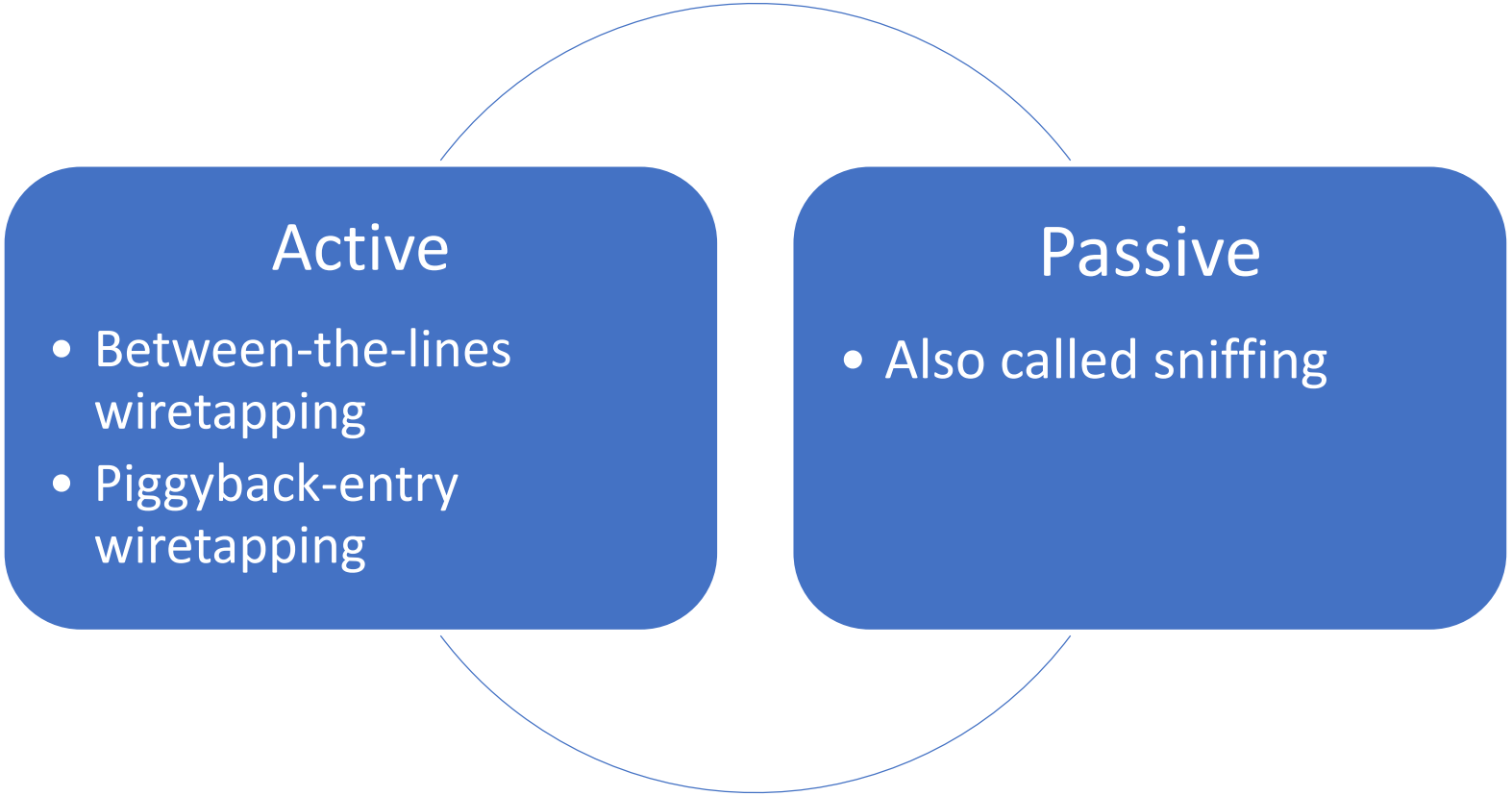
Overloads computers and prevents legitimate users from gaining access

More difficult to stop than a DoS attack because DDoS originates from different sources

Unacceptable Web Browsing

- Define acceptable web browsing in an acceptable use policy (AUP)
- Unacceptable use can include:
  - Unauthorized users searching files or storage directories
  - Users visiting prohibited websites

Wiretapping



Backdoors

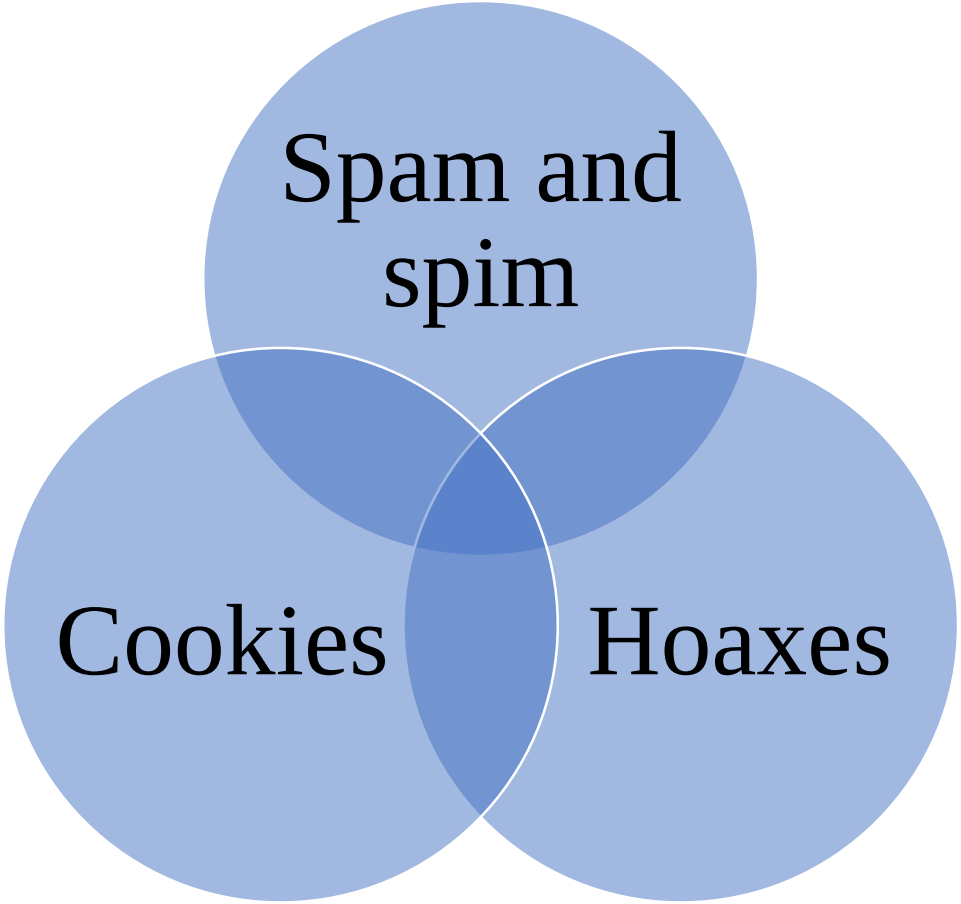
- Hidden access included by developers
- Attackers can use them to gain access

Data Modifications

Data that is:

- Purposely or accidentally modified
- Incomplete
- Truncated

Additional Security Challenges



Risks, Threats, Vulnerabilities

Risk	Probability that something bad is going to happen to an asset
Threat	Any action that can damage or compromise an asset
Vulnerability	An inherent weakness that may enable threats to harm system or networks

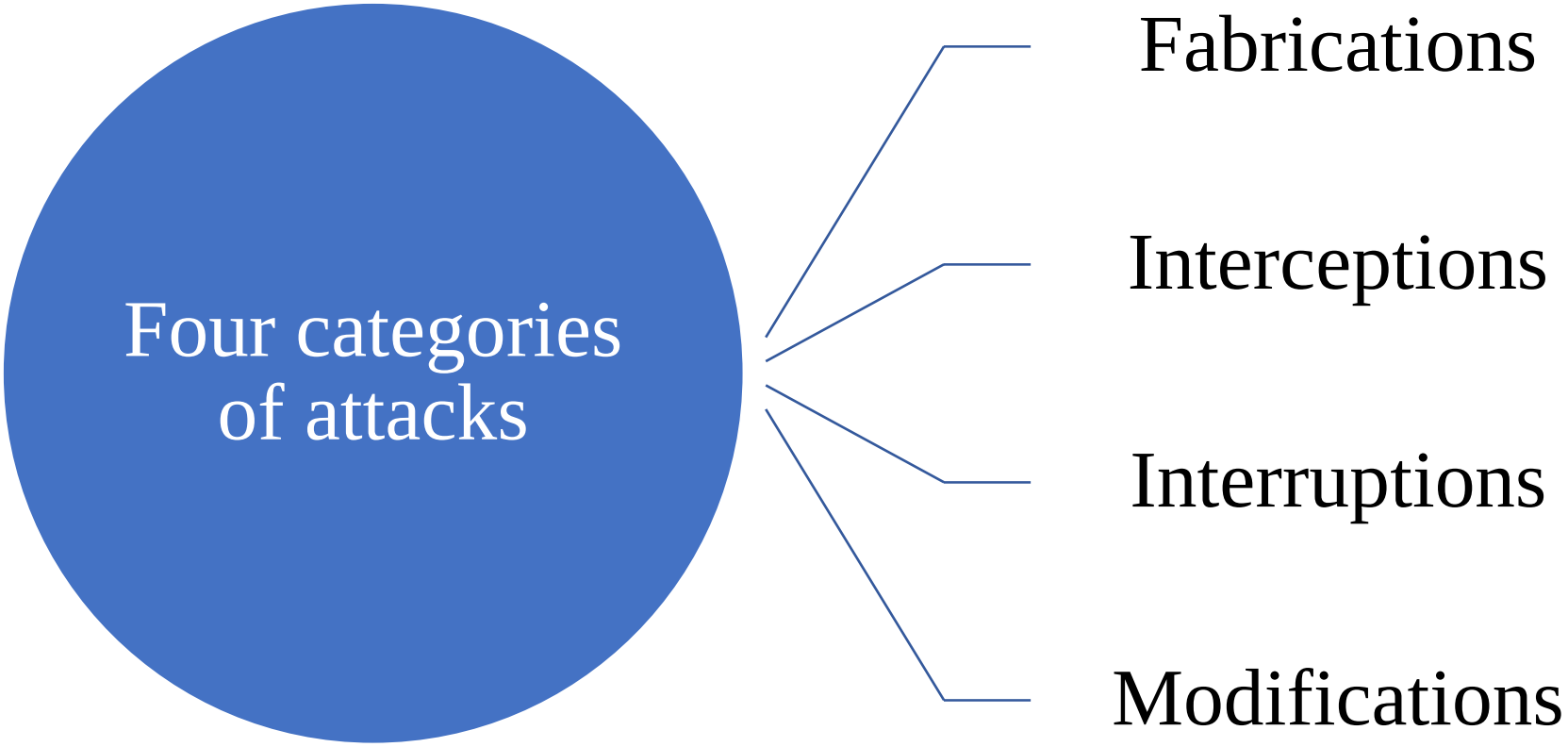
Most Common Threats

- Malicious software
- Hardware or software failure
- Internal attacker
- Equipment theft
- External attacker
- Natural disaster
- Industrial espionage
- Terrorism

Threat Types

Disclosure threats	• Sabotage • Espionage
Alteration threats	• Unauthorized changes
Denial or destruction threats	• DoS attack

What Is a Malicious Attack?



Types of Active Threats

- Birthday attacks
- Brute-force password attacks
- Dictionary password attacks
- IP address spoofing
- Hijacking
- Replay attacks
- Man-in-the-middle attacks
- Masquerading
- Social engineering
- Phishing
- Phreaking
- Pharming

What Is Malicious Software?

Software that:

- Causes damage
- Escalates security privileges
- Divulges private data
- Modifies or deletes data

Virus

- Attaches itself to or copies itself into another program on a computer
- Tricks the computer into following instructions not intended by the original program developer
- Infects a host program and may cause that host program to replicate itself to other computers
- User who runs infected program authenticates the virus

Worm

- A self-contained program that replicates and sends copies of itself to other computers without user input or action
- Does not need a host program to infect
- Is a standalone program

Trojan Horse

- Malware that masquerades as a useful program
- Trojans can:
  - Hide programs that collect sensitive information
  - Open backdoors into computers
  - Actively upload and download files

Rootkit

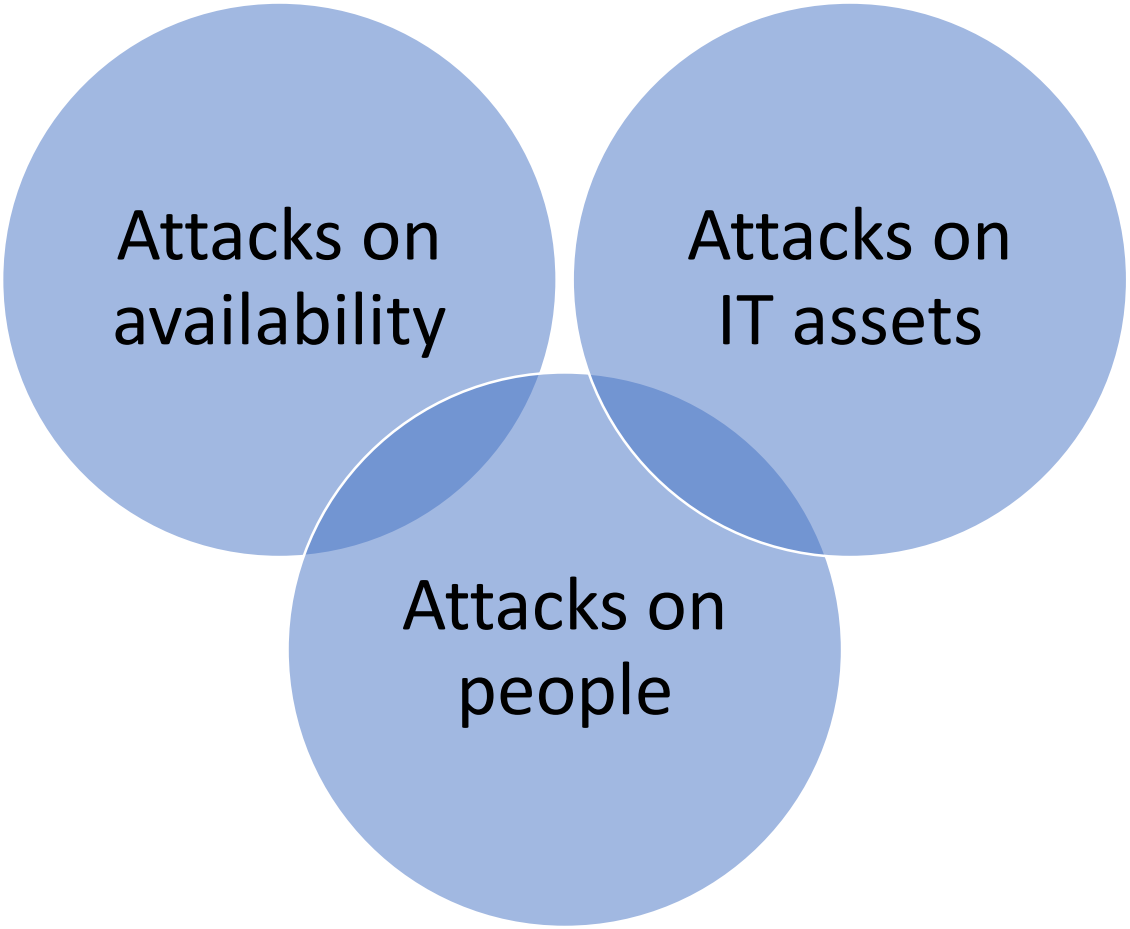
- Modifies or replaces one or more existing programs to hide traces of attacks
- Many different types of rootkits
- Conceals its existence once installed
- Is difficult to detect and remove

Spyware

Type of malware that specifically threatens the confidentiality of information

- Monitors keystrokes
- Scans files on the hard drive
- Snoops other applications
- Installs other spyware programs
- Reads cookies
- Changes default homepage on the web browser

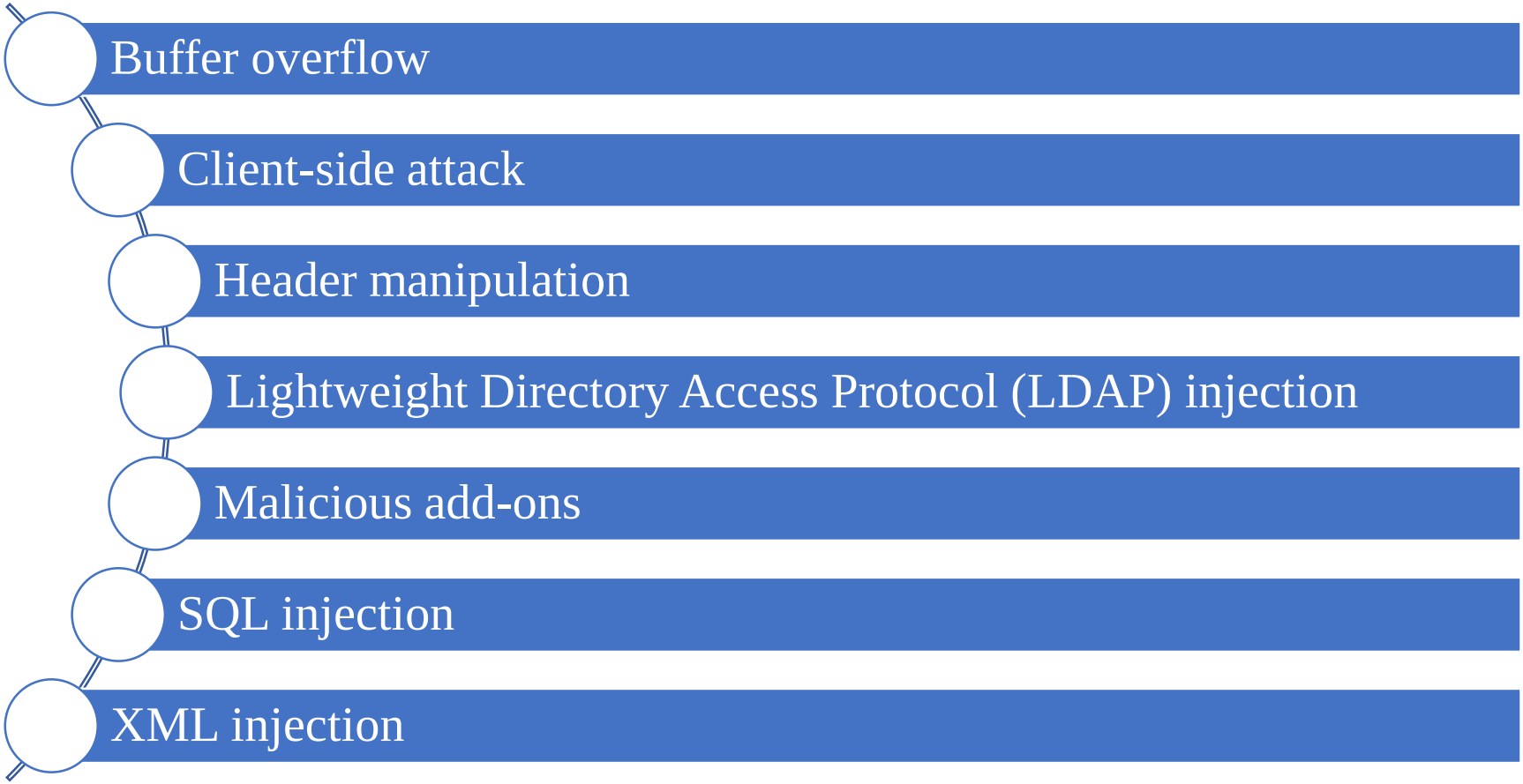
What Are Common Types of Attacks?



Social Engineering Attacks

Wireless Network Attacks

Web Application Attacks



What Is a Countermeasure?

Countermeasures

- Detect vulnerabilities
- Prevent attacks
- Respond to the effects of successful attacks

Get help from

- Law enforcement agencies
- Forensic experts
- Security consultants
- Security incident response teams (SIRTs)

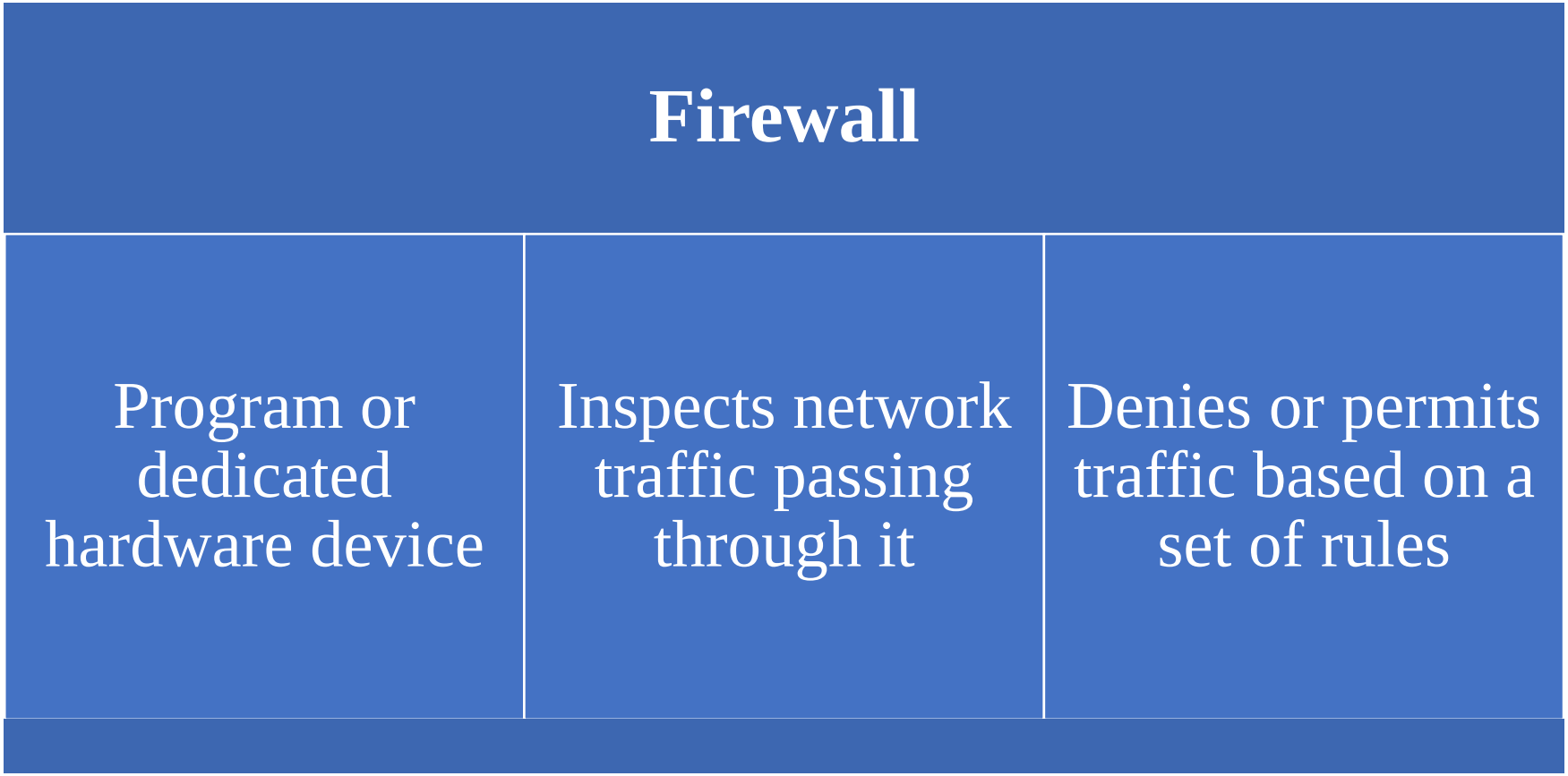
Countering Malware

- Create a user education program
- Post regular bulletins about malware problems
- Never transfer files from an unknown or untrusted source (unless anti-malware is installed)
- Test new programs or open suspect files on a quarantine computer
- Install anti-malware software, make sure it remains current, and schedule regular malware scans
- Use a secure logon and authentication process

Countering Malware (cont.)

- Stay abreast of developments in malware
  - National Cyber Security Alliance (NCSA)
    www.staysafeonline.org
  - United States Computer Emergency Readiness Team (US-CERT)
    http://us-cert.gov

Protecting Your System with Firewalls



Summary

- Malicious software and countermeasures
- Common attacks and countermeasures
- Social engineering and how to reduce risks
- Threats and types of attacks on wireless networks
- Threats and types of attacks on web applications

Please write the test

Thank you