SECURITY IN COMPUTING, FIFTH EDITION

Chapter 6: Networks

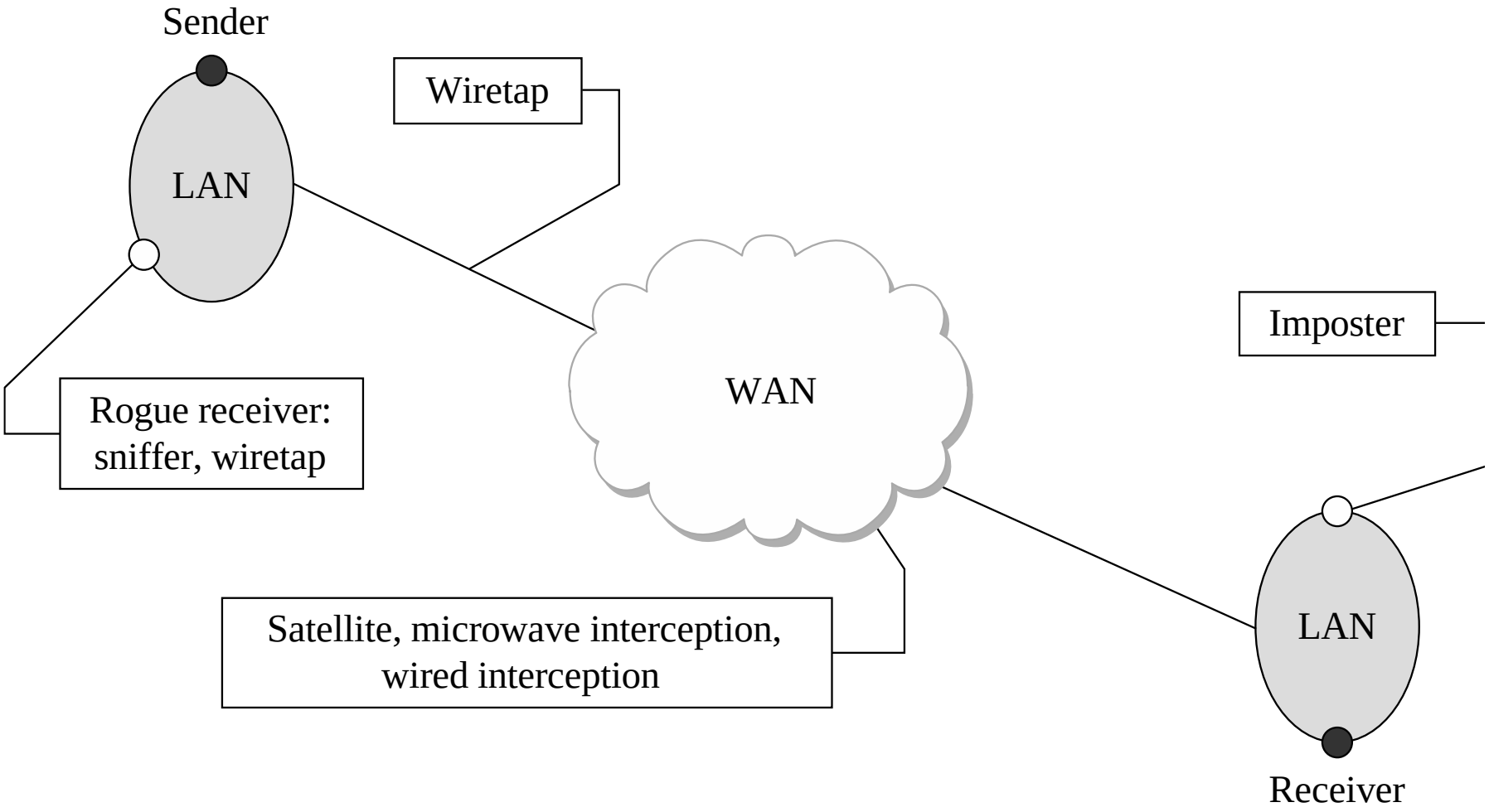
Objectives for Chapter 6

- Networking basics
- Network threats and vulnerabilities
- WiFi security
- Denial-of-service attacks
- Network encryption concepts and tools
- Types of firewalls and what they do
- Intrusion detection and prevention systems
- Security information and event management tools

Network Transmission Media

- Cable
- Optical fiber
- Microwave
- WiFi
- Satellite communication

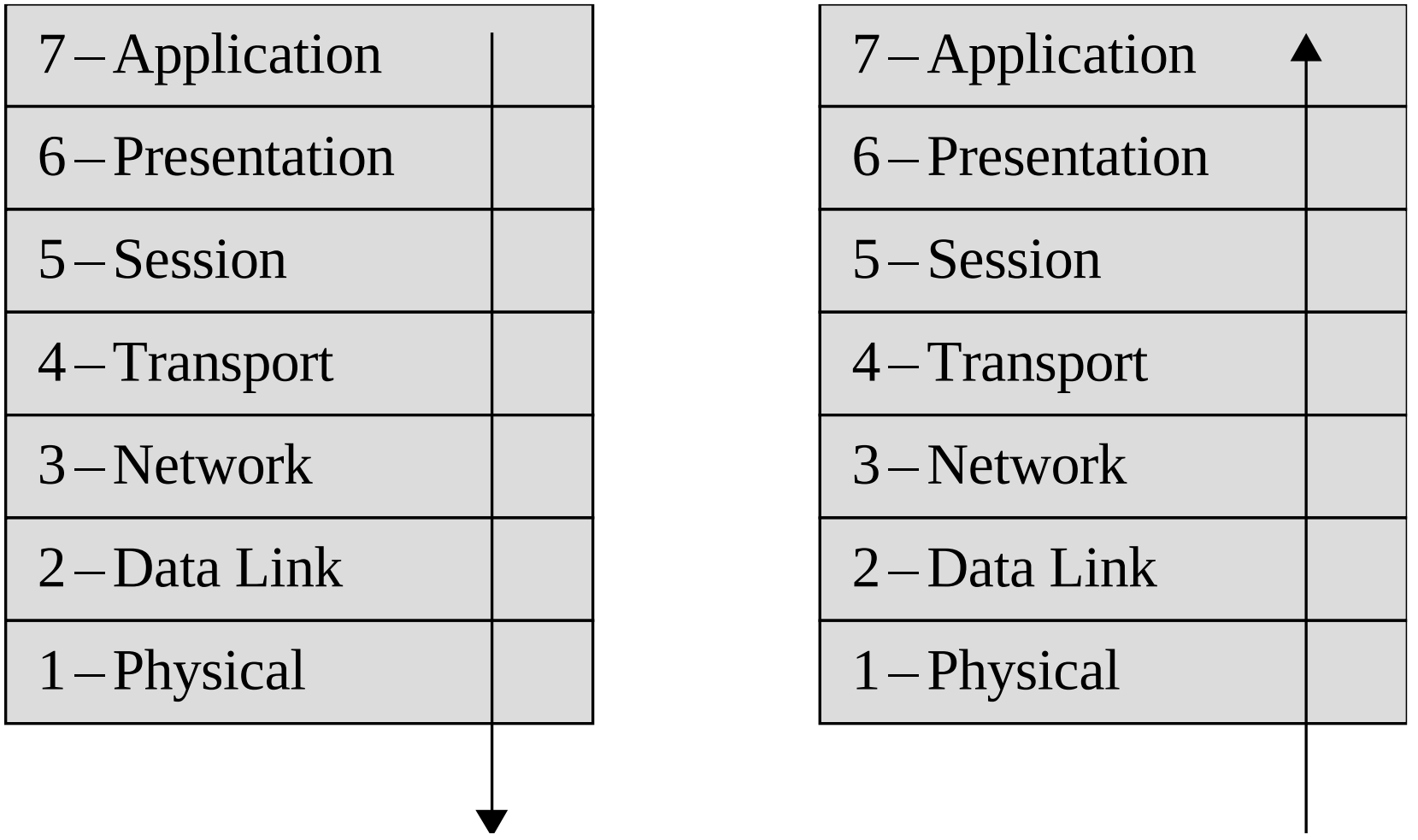
Communication Media Vulnerability



Communication Media Pros/Cons

Medium	Strengths	Weaknesses
Wire	• Widely used • Inexpensive to buy, install, maintain	• Susceptible to emanation • Susceptible to physical wiretapping
Optical fiber	• Immune to emanation • Difficult to wiretap	• Potentially exposed at connection points
Microwave	• Strong signal, not seriously affected by weather	• Exposed to interception along path of transmission • Requires line of sight location • Signal must be repeated approximately every 30 miles (50 kilometers)
Wireless (radio, WiFi)	• Widely available • Built into many computers	• Signal degrades over distance; suitable for short range • Signal interceptable in circular pattern around transmitter
Satellite	• Strong, fast signal	• Delay due to distance signal travels up and down • Signal exposed over wide area at receiving end

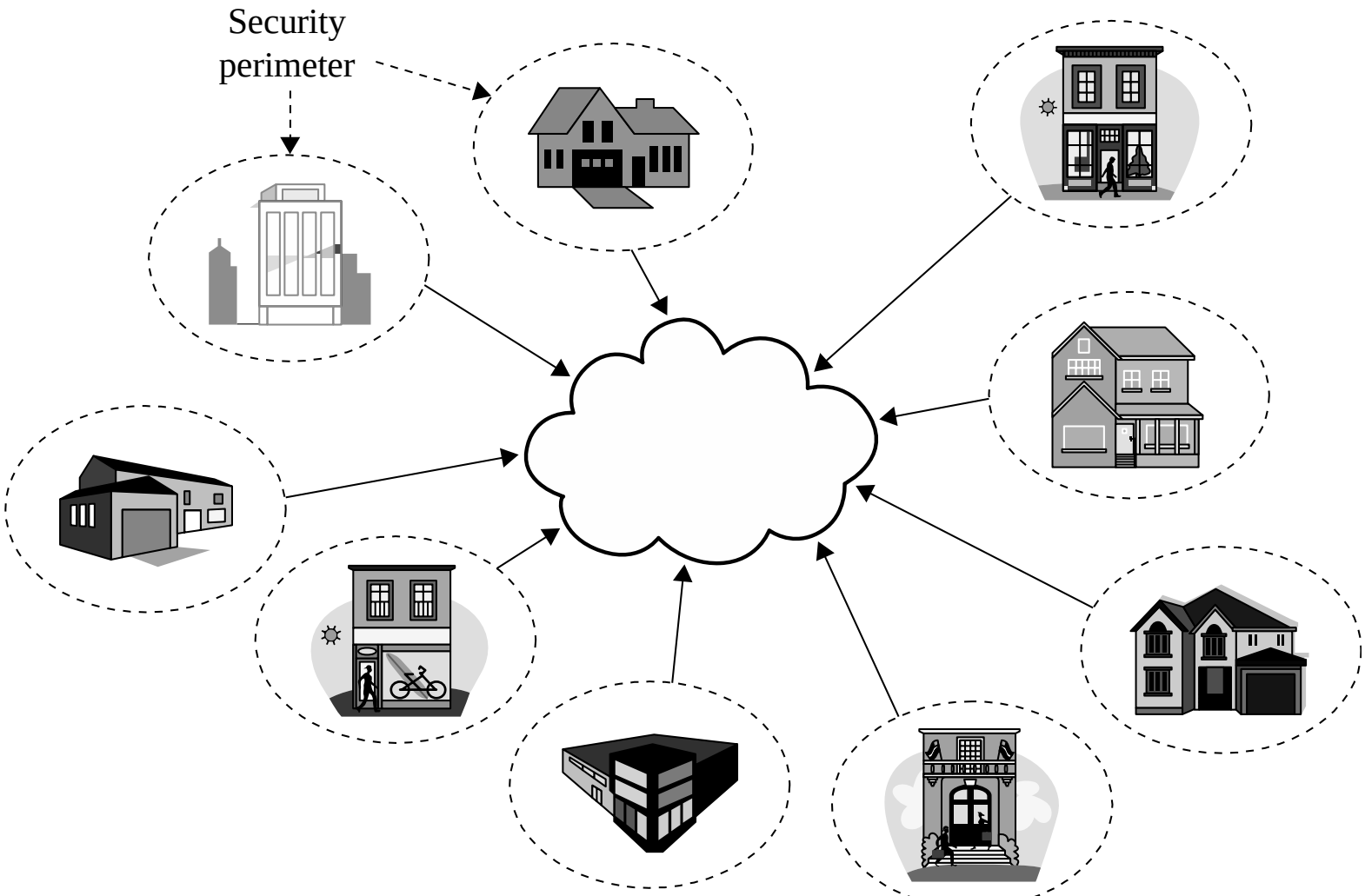
The OSI Model



Threats to Network Communications

- *Interception*, or unauthorized viewing
- *Modification*, or unauthorized change
- *Fabrication*, or unauthorized creation
- *Interruption*, or preventing authorized access

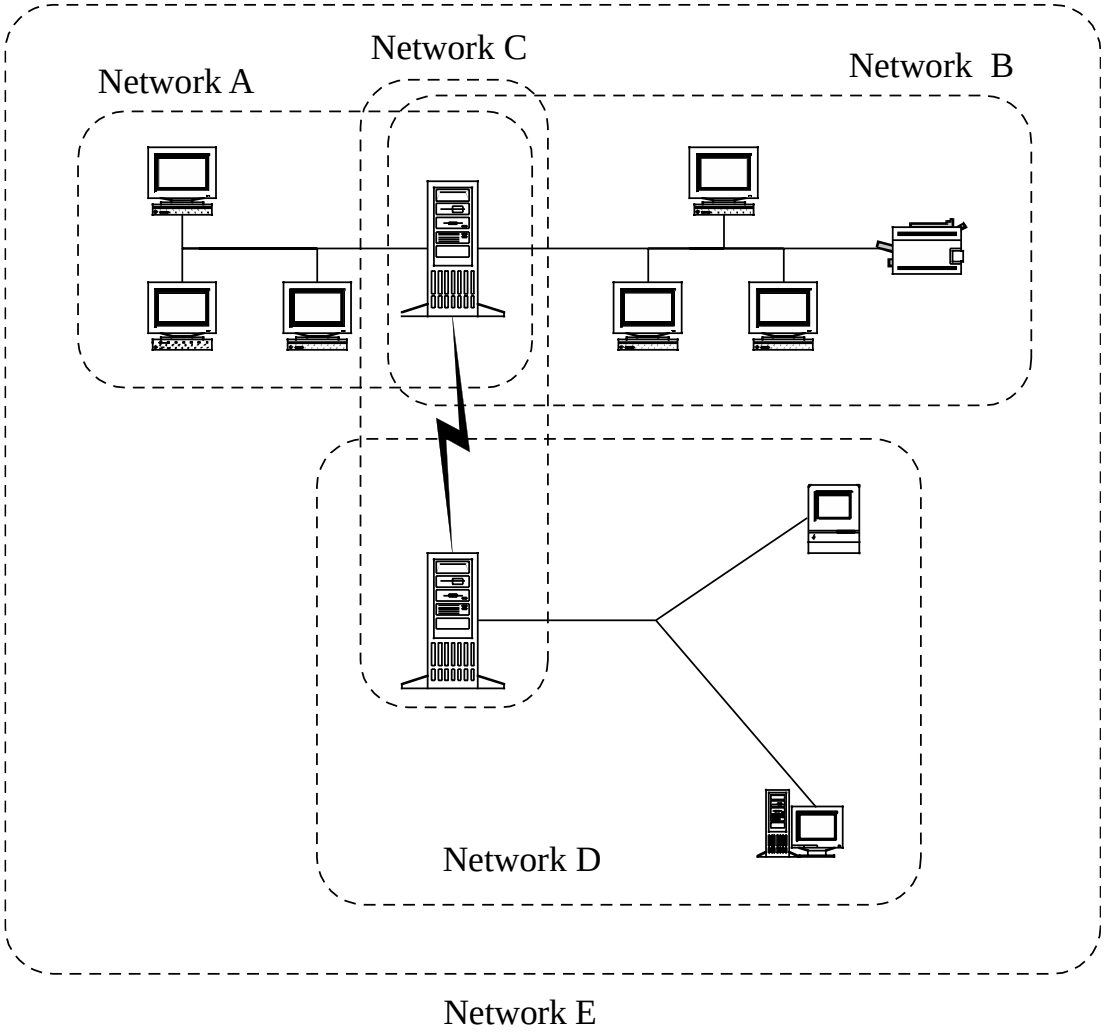
Security Perimeters



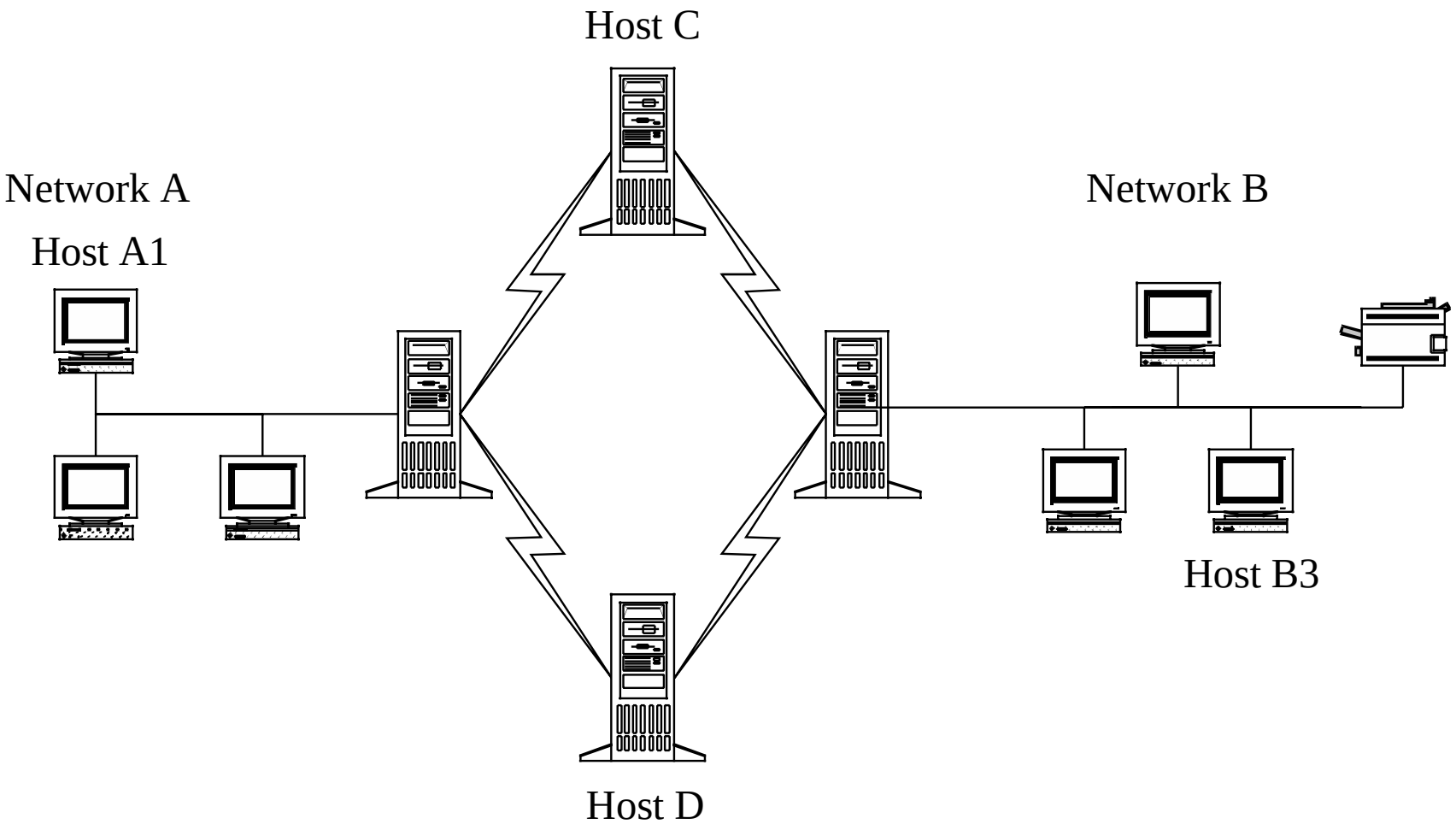
What Makes a Network Vulnerable to Interception?

- Anonymity
  - An attacker can attempt many attacks, anonymously, from thousands of miles away
- Many points of attack
  - Large networks mean many points of potential entry
- Sharing
  - Networked systems open up potential access to more users than do single computers
- System complexity
  - One system is very complex and hard to protect; networks of many different systems, with disparate OSs, vulnerabilities, and purposes are that much more complex
- Unknown perimeter
  - Networks, especially large ones, change all the time, so it can be hard to tell which systems belong and are behaving, and impossible to tell which systems bridge networks
- Unknown path
  - There may be many paths, including untrustworthy ones, from one host to another

Unknown Perimeter



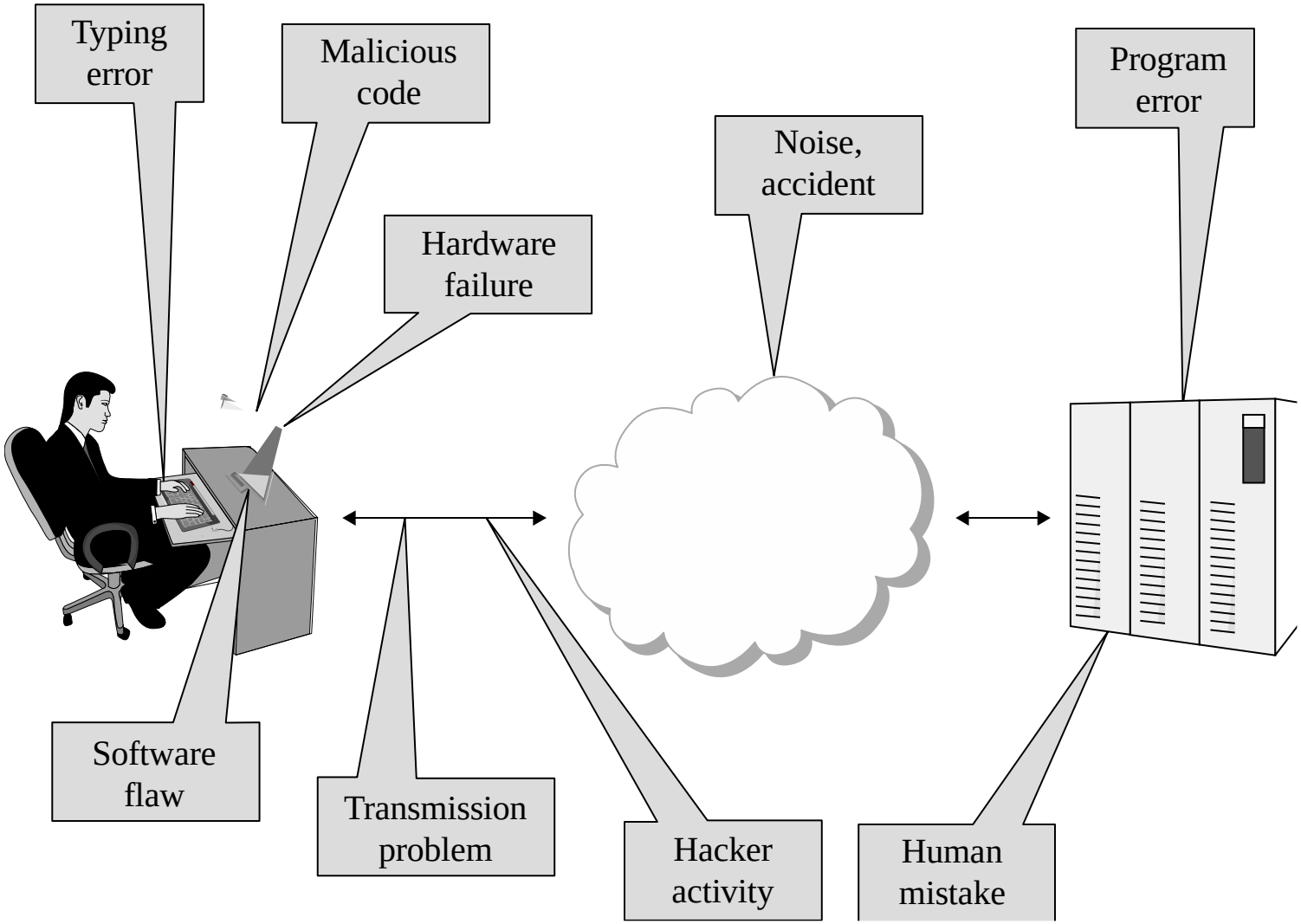
Unknown Path



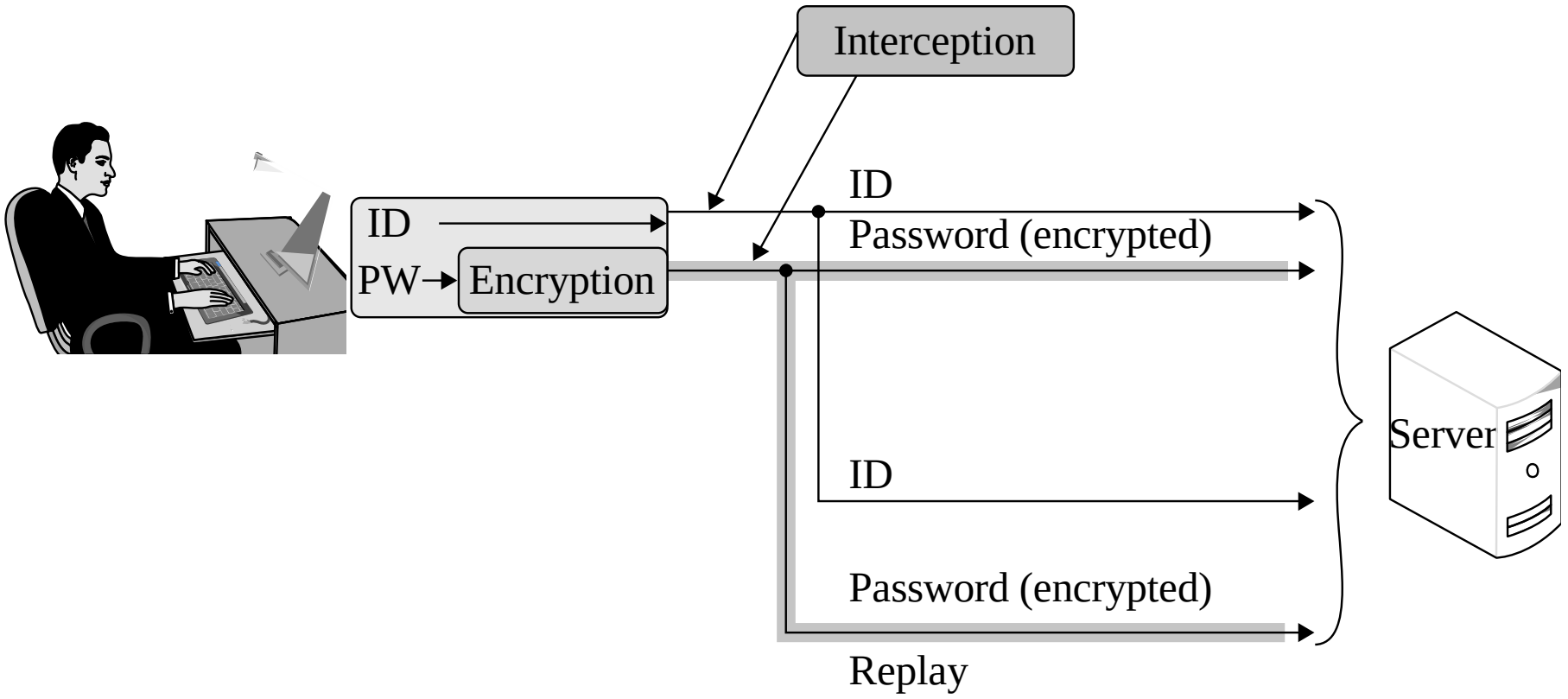
Modification and Fabrication

- Data corruption
  - May be intentional or unintentional, malicious or nonmalicious, directed or random
- Sequencing
  - Permuting the order of data, such as packets arriving in sequence
- Substitution
  - Replacement of one piece of a data stream with another
- Insertion
  - A form of substitution in which data values are inserted into a stream
- Replay
  - Legitimate data are intercepted and reused

Sources of Data Corruption



Simple Replay Attack



Interruption: Loss of Service

- Routing
  - Internet routing protocols are complicated, and one misconfiguration can poison the data of many routers
- Excessive demand
  - Network capacity is finite and can be exhausted; an attacker can generate enough demand to overwhelm a critical part of a network
- Component failure
  - Component failures tend to be sporadic and unpredictable, and will cause loss of service if not planned for

Port Scanning

```
Nmap scan report
192.168.1.1 / somehost.com (online) ping results
address: 192.168.1.1 (ipv4)
hostnames: somehost.com (user)
The 83 ports scanned but not shown below are in state: closed
Port       State      Service Reason       Product  Version  Extra info
21   tcp   open       ftp     syn-ack      ProFTPD  1.3.1
22   tcp   filtered   ssh     no-response
25   tcp   filtered   smtp    no-response
80   tcp   open       http    syn-ack      Apache   2.2.3    (CentOS)
106  tcp   open       pop3pw  syn-ack      poppassd
110  tcp   open       pop3    syn-ack      Courier pop3d
111  tcp   filtered   rpcbind no-response
113  tcp   filtered   auth    no-response
143  tcp   open        imap    syn-ack      Courier Imapd       released
2004
443  tcp   open       http    syn-ack      Apache  2.2.3       (CentOS)
465  tcp   open       unknown syn-ack
646  tcp   filtered   ldp     no-response
993  tcp   open       imap    syn-ack      Courier Imapd       released
2004
995  tcp   open                syn-ack
2049 tcp   filtered   nfs     no-response
3306 tcp   open       mysql   syn-ack      MySQL   5.0.45
8443 tcp   open       unknown syn-ack
34 sec. scanned
1 host(s) scanned
1 host(s) online
0 host(s) offline
```

Failed Countermeasure: WEP

- Wired equivalent privacy, or WEP, was designed at the same time as the original 802.11 WiFi standards as the mechanism for securing those communications
- Weaknesses in WEP were first identified in 2001, four years after release
- More weaknesses were discovered over the course of years, until any WEP-encrypted communication could be cracked in a matter of minutes

How WEP Works

- Client and access point (AP) have a pre-shared key
- AP sends a random number to the client, which the client then encrypts using the key and returns to the AP
- The AP decrypts the number using the key and checks that it's the same number to authenticate the client
- Once the client is authenticated, the AP and client communicate using messages encrypted with the key

WEP Weaknesses

- Weak encryption key
  - WEP allows to be either 64- or 128-bit, but 24 of those bits are reserved for initialization vectors (IV), thus reducing effective key size to 40 or 140 bits
  - Keys were either alphanumeric or hex phrases that users typed in and were therefore vulnerable to dictionary attacks
- Static key
  - Since the key was just a value the user typed in at the client and AP, and since users rarely changed those keys, one key would be used for many months of communications
- Weak encryption process
  - A 40-bit key can be brute forced easily. Flaws that were eventually discovered in the RC4 encryption algorithm WEP uses made the 104-bit keys easy to crack as well

WEP Weaknesses (cont.)

- Weak encryption algorithm
  - WEP used RC4 in a strange way (always a bad sign), which resulted in a flaw that allowed attackers to decrypt large portions of any WEP communication
- IV collisions
  - There were only 16 million possible values of IV, which, in practice, is not that many to cycle through for cracking. Also, they were not as randomly selected as they should have been, with some values being much more common than others
- Faulty integrity check
  - WEP messages included a checksum to identify transmission errors but did not use one that could address malicious modification
- No authentication
  - Any client that knows the AP's SSID and MAC address is assumed to be legitimate

WPA (WiFi Protected Access)

- WPA was designed in 2003 as a replacement for WEP and was quickly followed in 2004 by WPA2, the algorithm that remains the standard today
- Non-static encryption key
  - WPA uses a hierarchy of keys: New keys are generated for confidentiality and integrity of each session, and the encryption key is automatically changed on each packet
  - This way, the keys that are most important are used in very few places and indirect ways, protecting them from disclosure
- Authentication
  - WPA allows authentication by password, token, or certificate

WPA (cont.)

- Strong encryption
  - WPA adds support for AES, a much more reliably strong encryption algorithm
- Integrity protection
  - WPA includes a 64-bit cryptographic integrity check
- Session initiation
  - WPA sessions begin with authentication and a four-way handshake that results in separate keys for encryption and integrity on both ends
- While there are some attacks against WPA, they are either of very limited effectiveness or require weak passwords