COURSE TECHNOLOGY
CENGAGE Learning™

Principals of Information Security, Fourth Edition

Chapter 7

Security Technology: Intrusion Detection and Prevention Systems, and Other Security Tools

Do not wait; the time will never be just right. Start where you stand and work with whatever tools you may have at your command, and better tools will be found as you go along.

NAPOLEON HILL (1883–1970) FOUNDER OF THE SCIENCE of SUCCESS

Learning Objectives

- Upon completion of this material, you should be able to:
  - Identify and describe the categories of intrusion detection and prevention systems, honeypots, honeynets, padded cel, the use of biometric access mechanisms and the basic principles of cryptography
  - Describe the operating principles of the most popular cryptographic tools
  - List and explicate the major protocols used for secure communications
  - Discuss the nature of the dominant methods of attack used against cryptosystems

Intrusion Detection and Prevention Systems

- Intrusion: occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm
- Intrusion prevention: consists of activities that seek to deter an intrusion from occurring

Intrusion Detection and Prevention Systems (cont'd.)

- Intrusion detection: consists of procedures and systems created and operated to detect system intrusions
- Intrusion reaction: encompasses actions an organization undertakes when intrusion event is detected
- Intrusion correction activities: finalize restoration of operations to a normal state

Why Use an IDPS?

- Prevent problem behaviors by increasing the perceived risk of discovery and punishment
- Detect attacks and other security violations
- Detect and deal with preambles to attacks
- Document existing threat to an organization
- Act as quality control for security design and administration, especially of large and complex enterprises
- Provide useful information about intrusions that take place

Types of IDPS

- IDSs operate as network-based, host-based, or application based systems
- Network-based IDPS is focused on protecting network information assets
  - Wireless IDPS: focuses on wireless networks
  - Network behavior analysis IDPS: examines traffic flow on a network in an attempt to recognize abnormal patterns

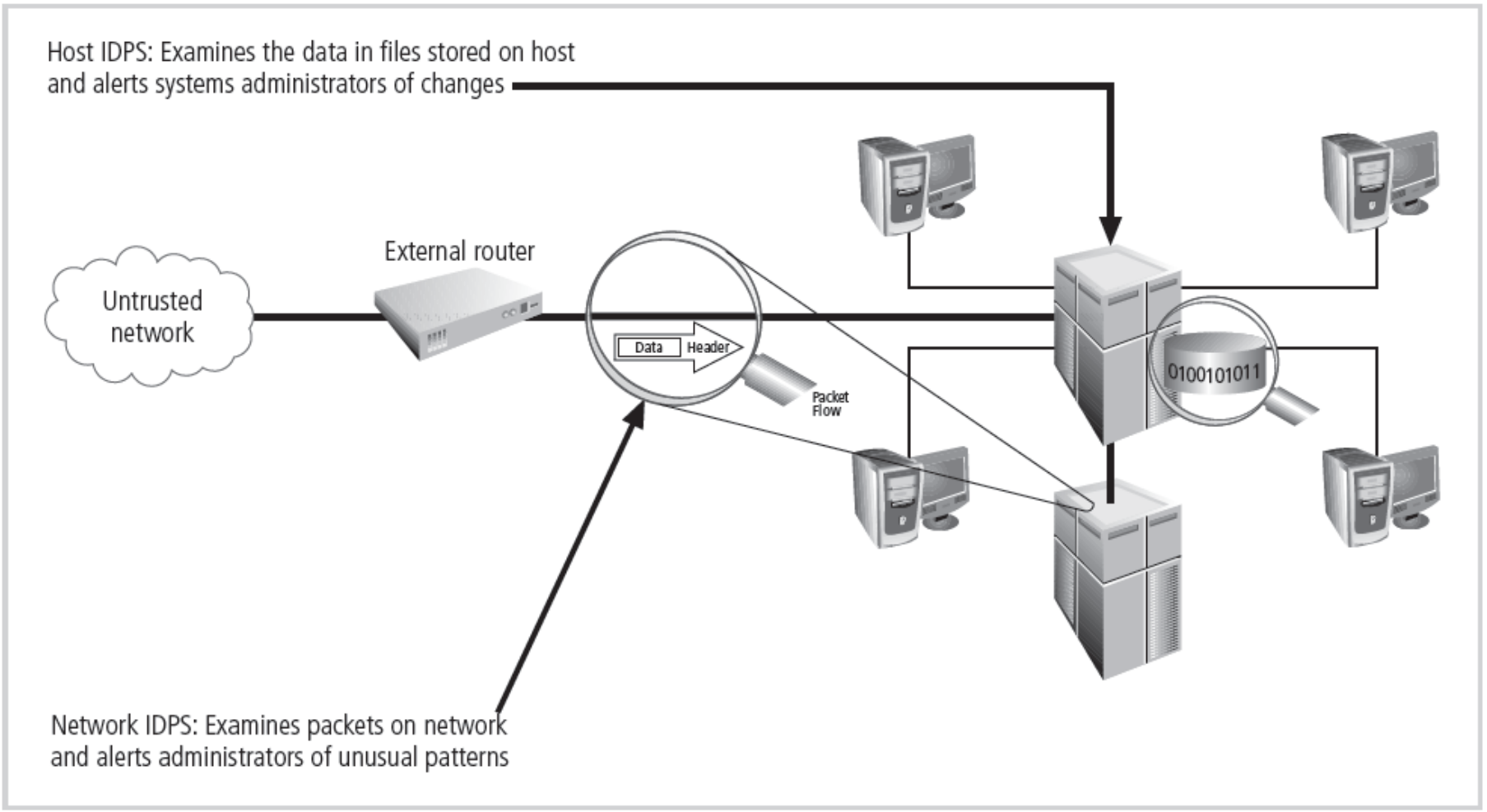

Figure 7-1 Intrusion Detection and Prevention Systems

Types of IDPS (cont'd.)

- Network-based IDPS
  - Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks
  - When examining packets, a NIDPS looks for attack patterns
  - Installed at specific place in the network where it can watch traffic going into and out of particular network segment

Types of IDPS (cont'd.)

- Advantages of NIDPSs
  - Can enable organization to use a few devices to monitor large network
  - NIDPSs not usually susceptible to direct attack and may not be detectable by attackers
- Disadvantages of NIDPSs
  - Can become overwhelmed by network volume and fail to recognize attacks
  - Require access to all traffic to be monitored
  - Cannot analyze encrypted packets
  - Cannot reliably ascertain if attack was successful or not

Types of IDPS (cont'd.)

- Wireless NIDPS
  - Monitors and analyzes wireless network traffic
  - Issues associated with it include physical security, sensor range, access point and wireless switch locations, wired network connections, cost
- Network behavior analysis systems
  - Examine network traffic in order to identify problems related to the flow of traffic
  - Types of events commonly detected include DoS attacks, scanning, worms, unexpected application services, policy violations

Types of IDPS (cont'd.)

- Host-based IDPS
  - Resides on a particular computer or server and monitors activity only on that system
  - Advantage over NIDPS: can usually be installed so that it can access information encrypted when traveling over network

Types of IDPS (cont'd.)

- Advantages of HIDPSs
  - Can detect local events on host systems and detect attacks that may elude a network-based IDPS
  - Functions where encrypted traffic will have been decrypted and is available for processing
  - Not affected by use of switched network protocols
  - Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

Types of IDPS (cont'd.)

- Disadvantages of HIDPSs
  - Pose more management issues
  - Vulnerable both to direct attacks and attacks against host operating system
  - Does not detect multi-host scanning, nor scanning of non-host network devices
  - Susceptible to some denial-of-service attacks
  - Can use large amounts of disk space
  - Can inflict a performance overhead on its host systems

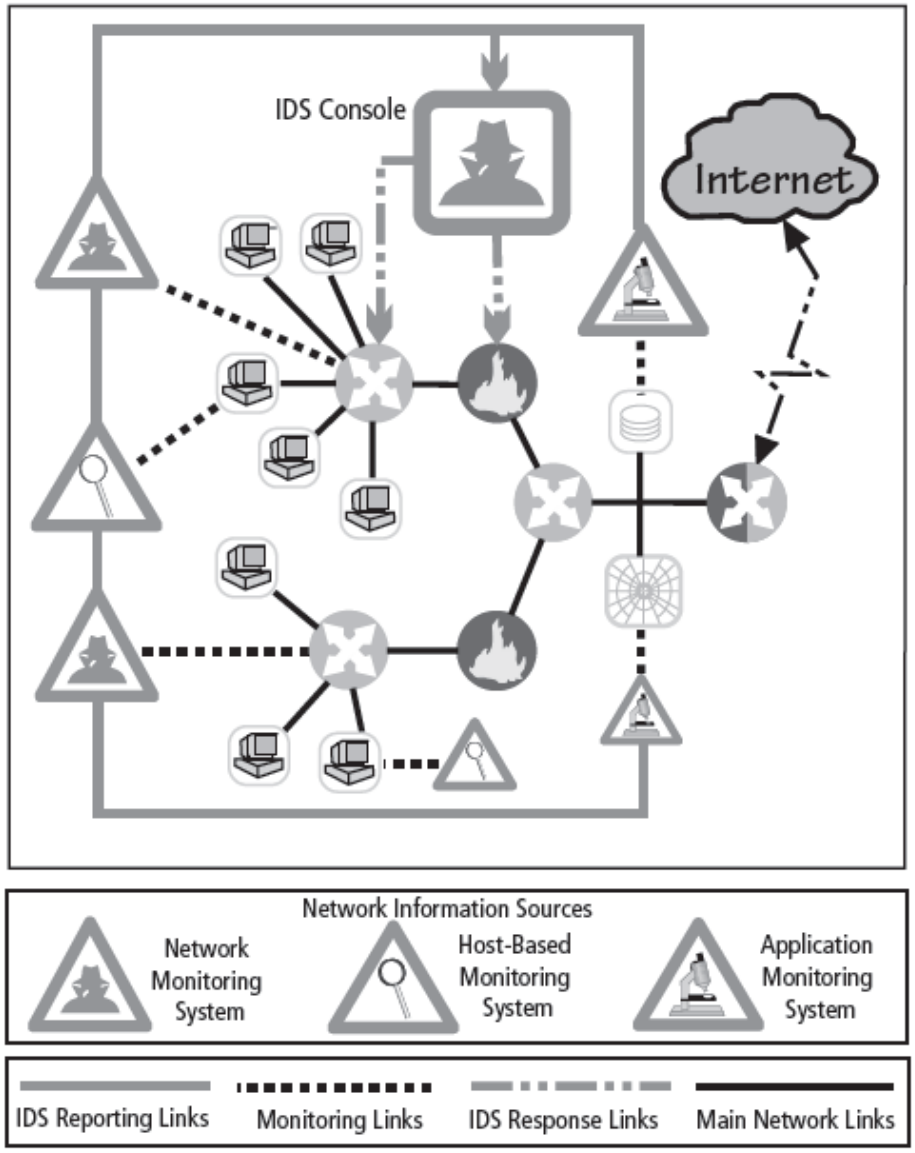

Figure 7-4 Centralized IDPS Control[13]

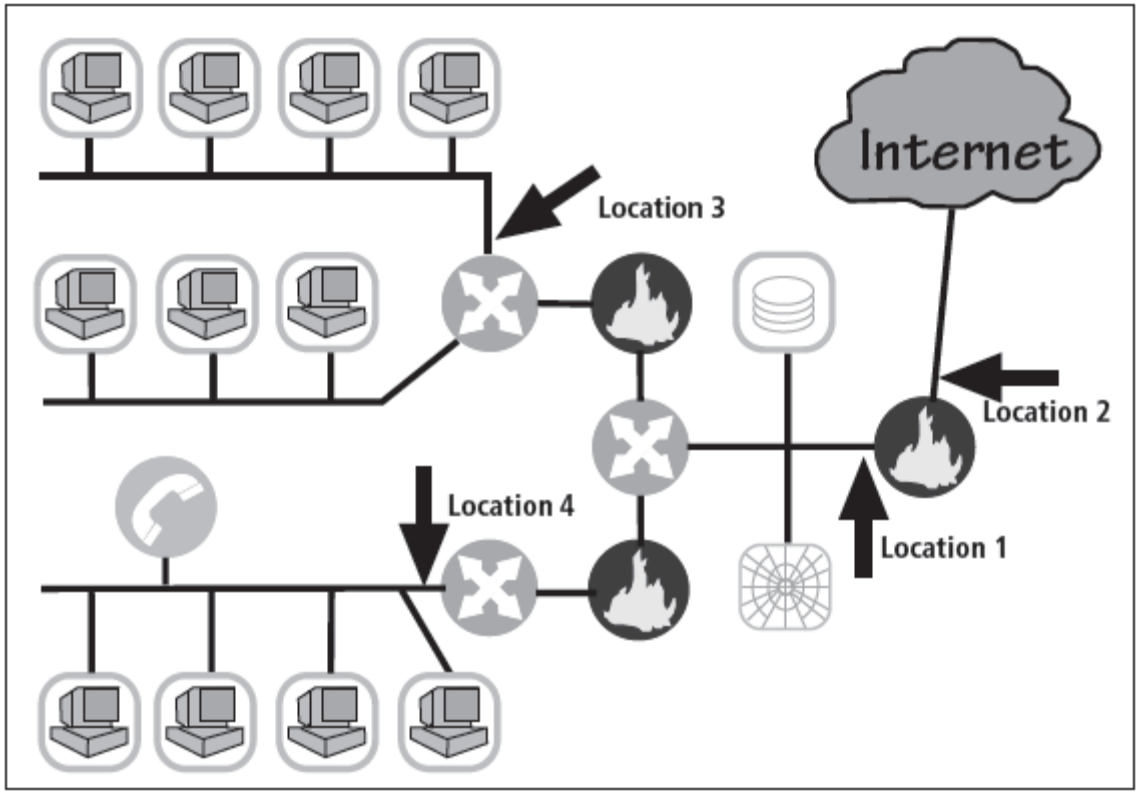

Figure 7-7 Network IDPS Sensor Locations[17]

Honeypots, Honeynets, and Padded Cell Systems

- Honeypots: decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves
- Honeynets: collection of honeypots connecting several honey pot systems on a subnet
- Honeypots designed to:
  - Divert attacker from accessing critical systems
  - Collect information about attacker's activity
  - Encourage attacker to stay on system long enough for administrators to document event and, perhaps, respond

Honeypots, Honeynets, and Padded Cell Systems (cont'd.)

- Padded cell: honeypot that has been protected so it cannot be easily compromised
- In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDS
- When the IDS detects attackers, it seamlessly transfers them to a special simulated environment where they can cause no harm—the nature of this host environment is what gives approach the name padded cell

Honeypots, Honeynets, and Padded Cell Systems (cont'd.)

- Advantages
  - Attackers can be diverted to targets they cannot damage
  - Administrators have time to decide how to respond to attacker
  - Attackers' actions can be easily and more extensively monitored, and records can be used to refine threat models and improve system protections
  - Honey pots may be effective at catching insiders who are snooping around a network

Honeypots, Honeynets, and Padded Cell Systems (cont'd.)

- Disadvantages
  - Legal implications of using such devices are not well defined
  - Honeypots and padded cells have not yet been shown to be generally useful security technologies
  - Expert attacker, once diverted into a decoy system, may become angry and launch a more hostile attack against an organization's systems
  - Administrators and security managers will need a high level of expertise to use these systems

Biometric Access Control

- Based on the use of some measurable human characteristic or trait to authenticate the identity of a proposed systems user (a supplicant)
- Relies upon recognition
- Includes fingerprint comparison, palm print comparison, hand geometry, facial recognition using a photographic id card or digital camera, retinal print, iris pattern
- Characteristics considered truly unique: fingerprints, retina of the eye, iris of the eye

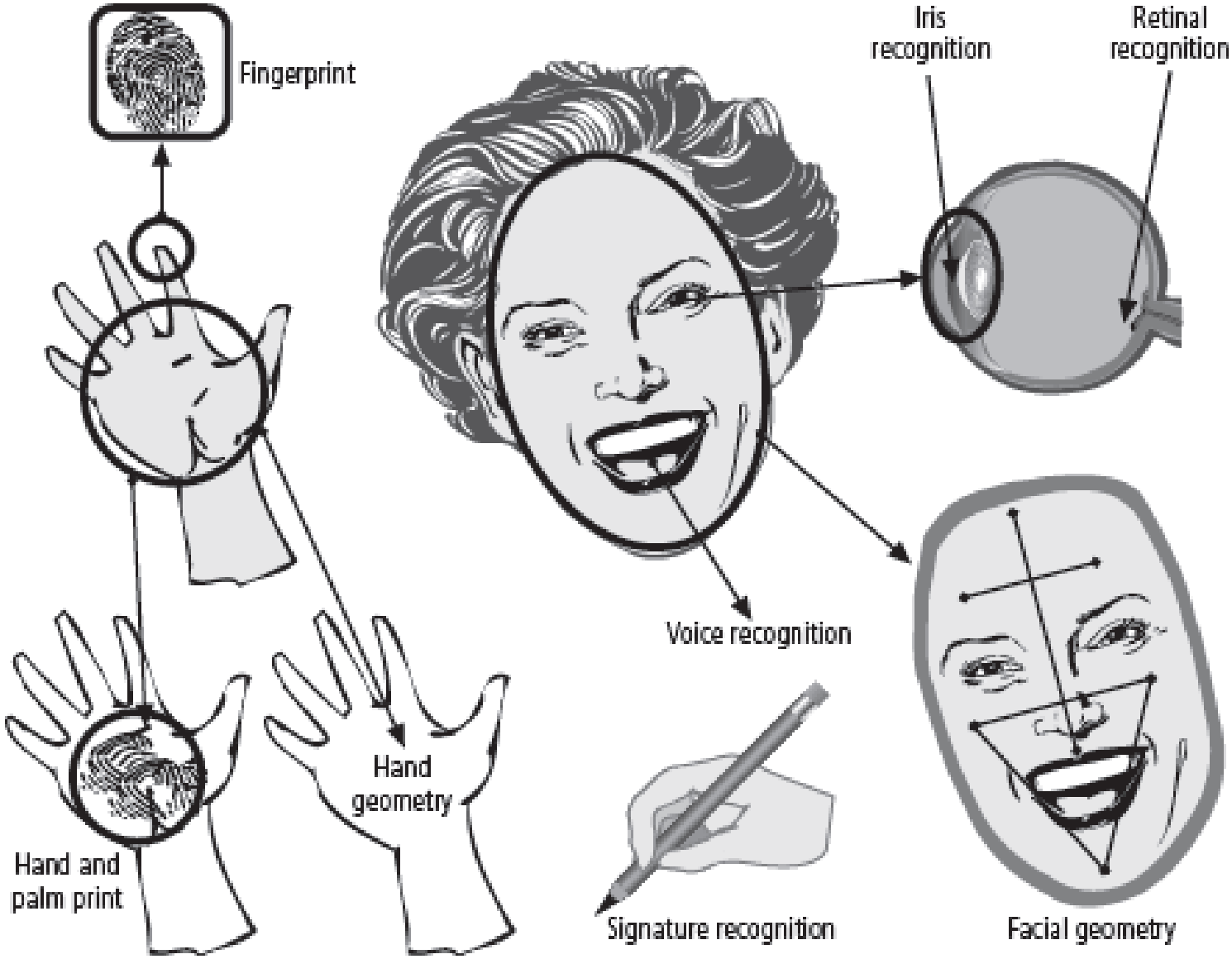

Figure 7-20 Biometric Recognition Characteristics

Effectiveness of Biometrics

- Biometric technologies evaluated on three basic criteria:
  - False reject rate: the rejection of legitimate users
  - False accept rate: the acceptance of unknown users
  - Crossover error rate (CER): the point where false reject and false accept rates cross when graphed

Acceptability of Biometrics

- Balance must be struck between how acceptable security system is to users and its effectiveness in maintaining security
- Many biometric systems that are highly reliable and effective are considered intrusive
- As a result, many information security professionals, in an effort to avoid confrontation and possible user boycott of biometric controls, don’t implement them

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Keystroke Dynamics	L	L	L	M	L	M	M
Hand Vein	M	M	M	M	M	M	H
Iris	H	H	H	M	H	L	H
Retina	H	H	M	L	H	L	H
Signature	L	L	L	H	L	H	L
Voice	M	L	L	M	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
DNA	H	H	H	L	H	L	L

Table 7-3 Ranking of Biometric Effectiveness and Acceptance
H=High, M=Medium, L=Low
Reproduced from The '123' of Biometric Technology, 2003, by Yun, Yau Wei[22]

End

- Summery