

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 1

Overview

The NIST Internal/Interagency Report NISTIR 7298 (*Glossary of Key Information Security Terms*, May 2013) defines the term *computer security* as follows:

“ Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.”

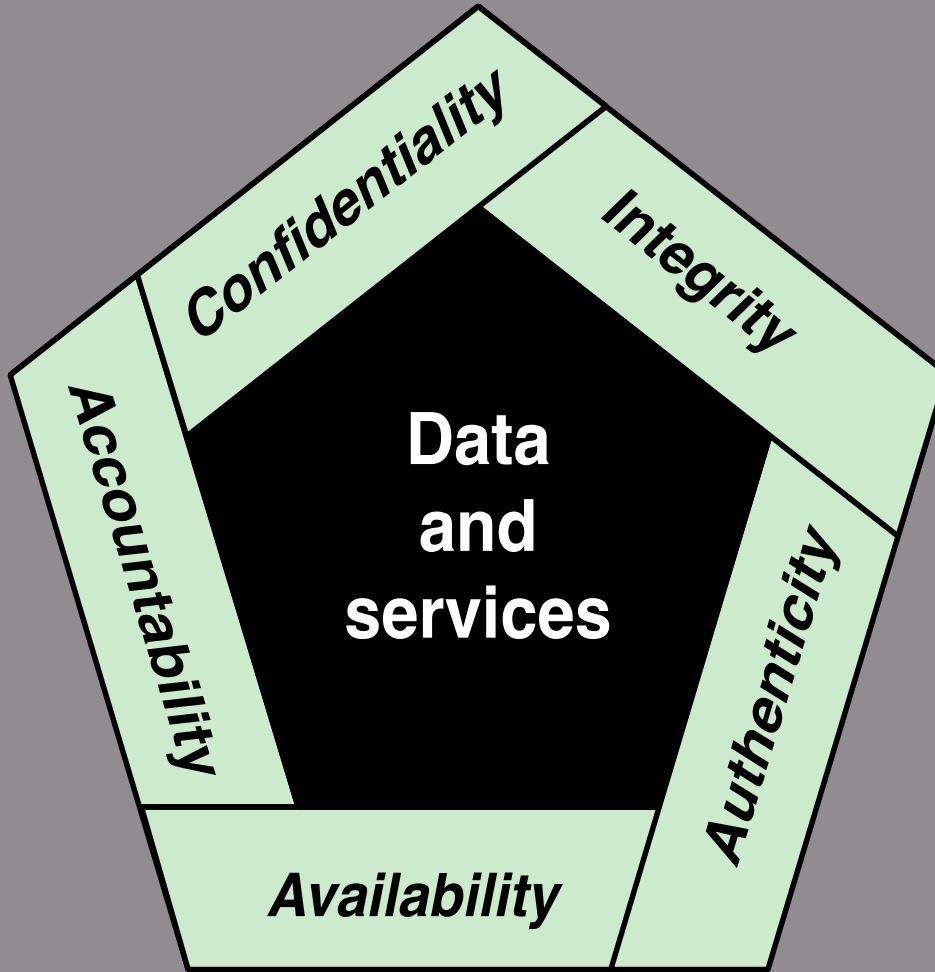


Figure 1.1 Essential Network and Computer Security Requirements

Key Security Concepts

Confidentiality

- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity

Availability

- Ensuring timely and reliable access to and use of information

Levels of Impact

Low

The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals

Moderate

The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals

High

The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals

Computer Security Challenges

1. Computer security is not as simple as it might first appear to the novice
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features
3. Procedures used to provide particular services are often counterintuitive
4. Physical and logical placement needs to be determined
5. Security mechanisms typically involve more than a particular algorithm or protocol and also require that participants be in possession of some secret information which raises questions about the creation, distribution, and protection of that secret information
6. Attackers only need to find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security
7. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process
8. Security requires regular and constant monitoring
9. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs
10. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

Table 1.1**Computer Security Terminology, from RFC 2828, *Internet Security Glossary*, May 2000****Adversary (threat agent)**

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure

A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Security Policy

A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Asset)

A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

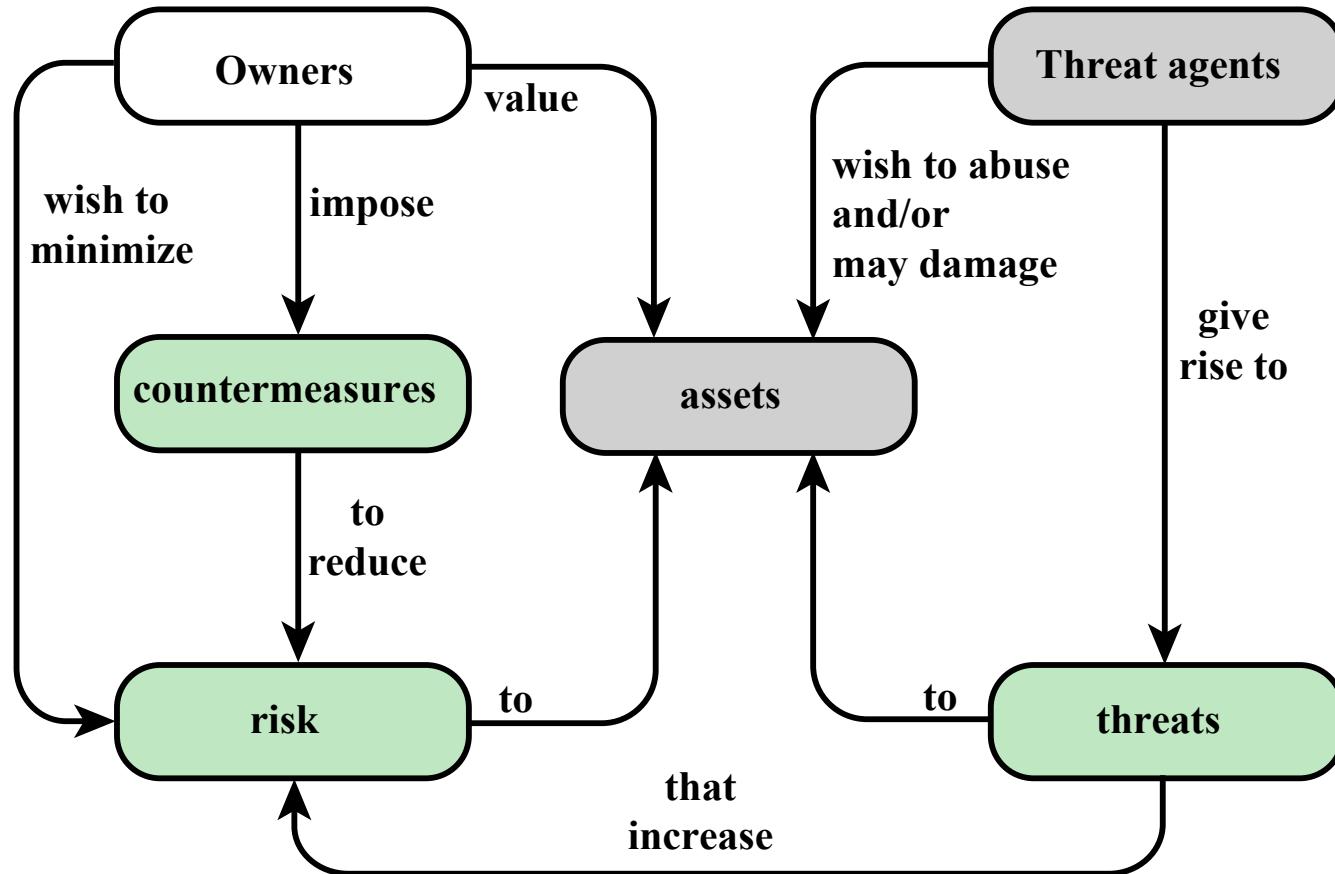
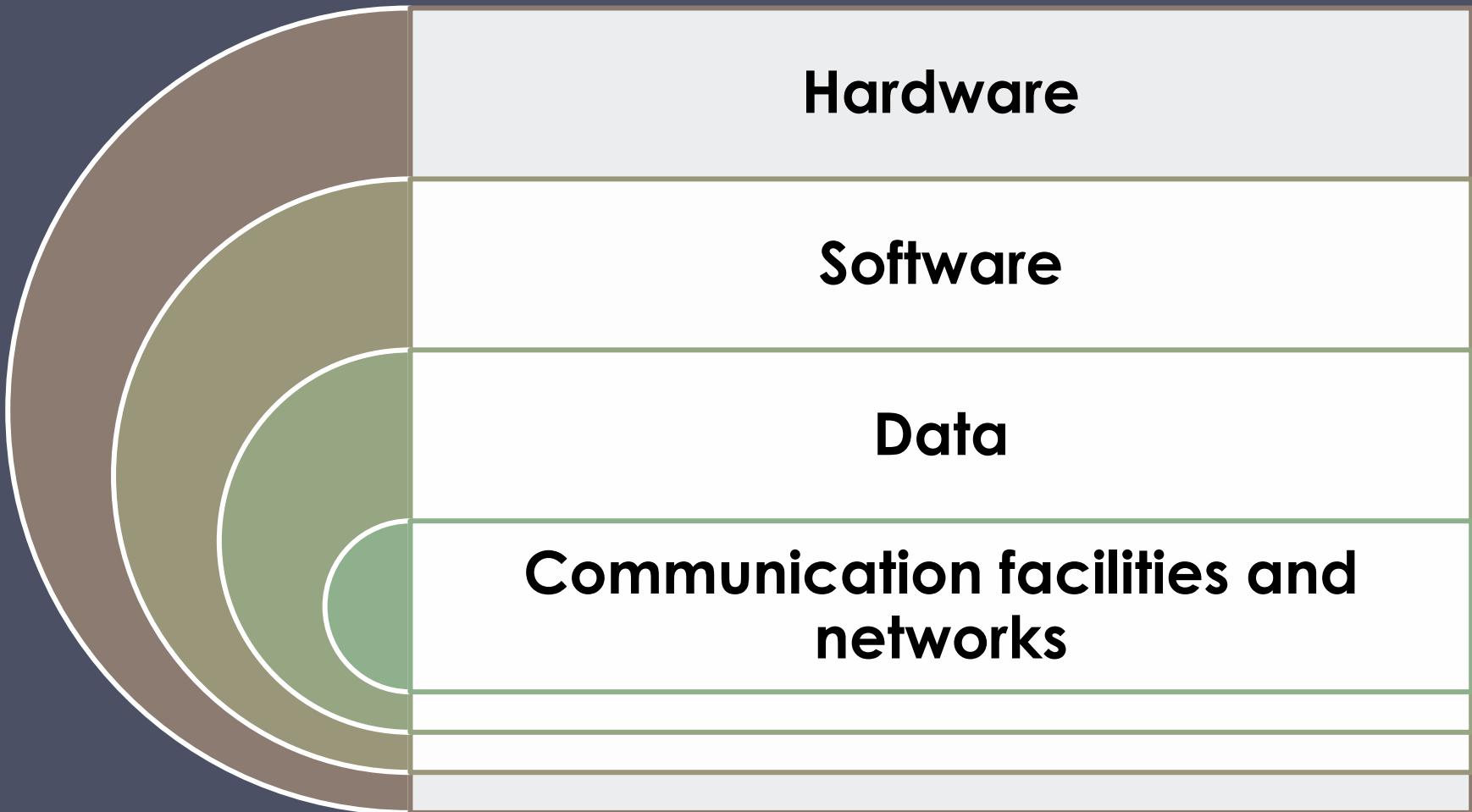


Figure 1.2 Security Concepts and Relationships

Assets of a Computer System



Vulnerabilities, Threats and Attacks

- Categories of vulnerabilities
 - Corrupted (loss of integrity)
 - Leaky (loss of confidentiality)
 - Unavailable or very slow (loss of availability)
- Threats
 - Capable of exploiting vulnerabilities
 - Represent potential security harm to an asset
- Attacks (threats carried out)
 - Passive – attempt to learn or make use of information from the system that does not affect system resources
 - Active – attempt to alter system resources or affect their operation
 - Insider – initiated by an entity inside the security parameter
 - Outsider – initiated from outside the perimeter

Countermeasures

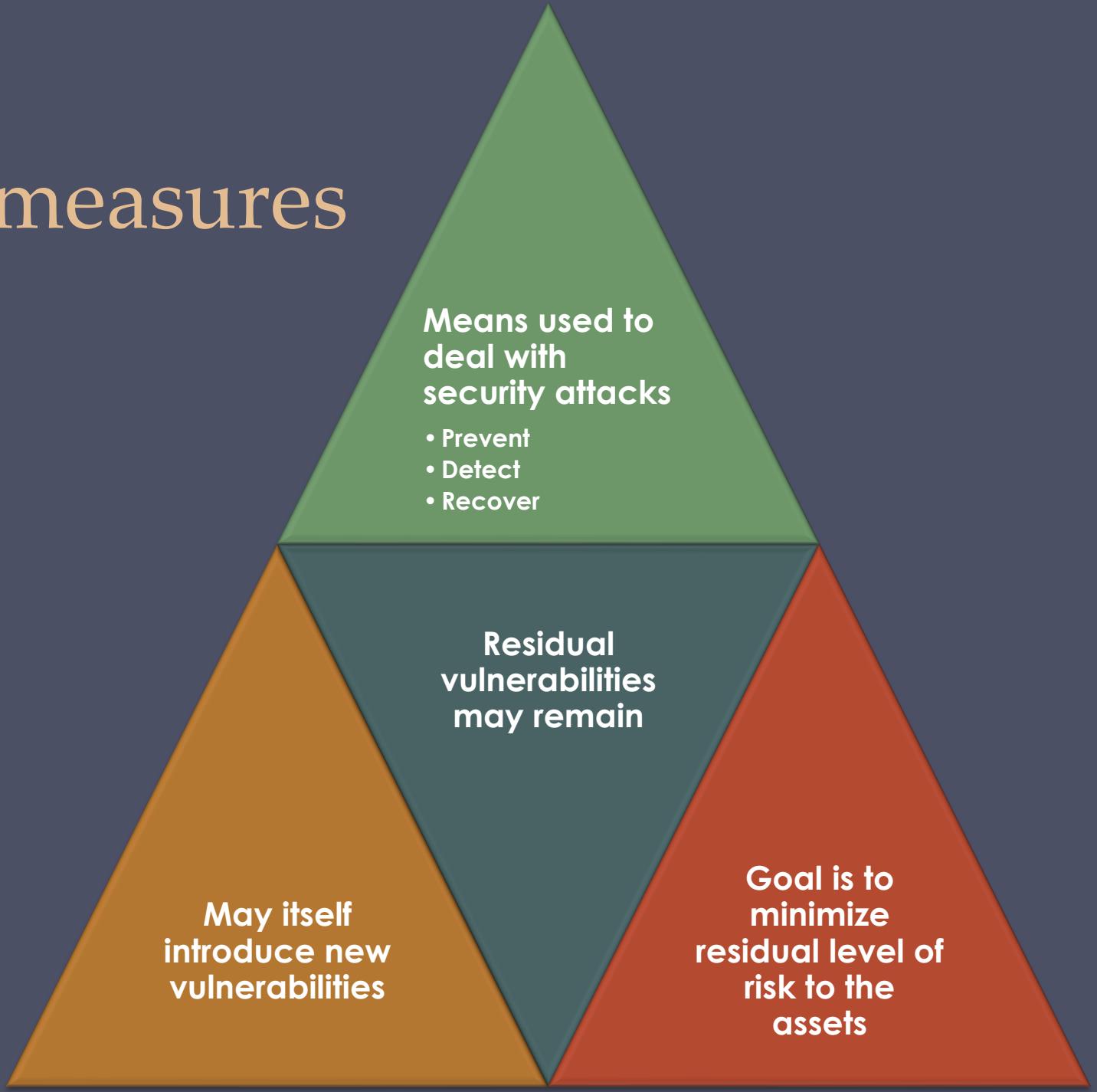


Table 1.2

Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	Exposure: Sensitive data are directly released to an unauthorized entity. Interception: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. Inference: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. Intrusion: An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. Falsification: False data deceive an authorized entity. Repudiation: An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	Incapacitation: Prevents or interrupts system operation by disabling a system component. Corruption: Undesirably alters system operation by adversely modifying system functions or data. Obstruction: A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	Misappropriation: An entity assumes unauthorized logical or physical control of a system resource. Misuse: Causes a system component to perform a function or service that is detrimental to system security.

Threat
Consequences,
and the
Types of
Threat Actions
That Cause
Each
Consequence
Based on
RFC 4949

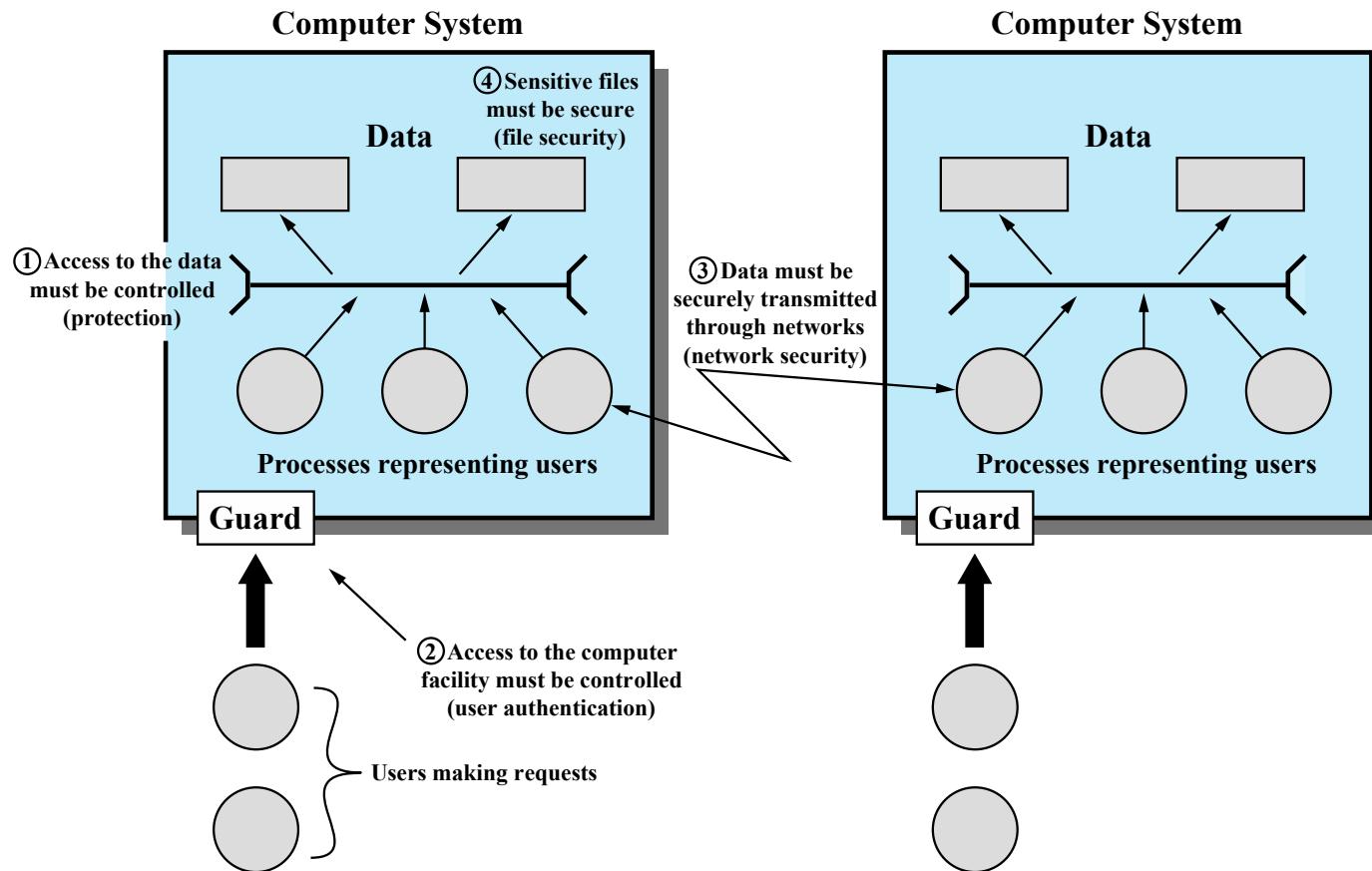


Figure 1.3 Scope of Computer Security. This figure depicts security concerns other than physical security, including control of access to computers systems, safeguarding of data transmitted over communications systems, and safeguarding of stored data.

Table 1.3
Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Passive and Active Attacks

Passive Attack

- Attempts to learn or make use of information from the system but does not affect system resources
- Eavesdropping on, or monitoring of, transmissions
- Goal of attacker is to obtain information that is being transmitted
- Two types:
 - Release of message contents
 - Traffic analysis

Active Attack

- Attempts to alter system resources or affect their operation
- Involve some modification of the data stream or the creation of a false stream
- Four categories:
 - Replay
 - Masquerade
 - Modification of messages
 - Denial of service

Access control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

Awareness and training: (i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulation, and policies related to the security of organizational information systems; and (ii) ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Audit and accountability: (i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Certification, accreditation, and security assessments: (i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

Configuration management: (i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.

Contingency planning: Establish, maintain, and implement plans for emergency response, backup operations, and postdisaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

Identification and authentication: Identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

Incident response: (i) Establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.

Maintenance: (i) Perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Table 1.4

Security Requirements (FIPS 200)

(page 1 of 2)

(Table can be found on pages 16-17 in the textbook.)

Media protection: (i) Protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.

Physical and environmental protection: (i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.

Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

Personnel security: (i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

Risk assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

Systems and services acquisition: (i) Allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

System and communications protection: (i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

System and information integrity: (i) Identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.

Table 1.4

Security Requirements (FIPS 200)

(page 2 of 2)

(Table can be found on pages 16-17 in the textbook.)

Fundamental Security Design Principles

Economy of mechanism

Fail-safe defaults

Complete mediation

Open design

Separation of privilege

Least privilege

Least common mechanism

Psychological acceptability

Isolation

Encapsulation

Modularity

Layering

Least astonishment

Attack Surfaces

Consist of the reachable and exploitable vulnerabilities in a system

Examples:

Open ports on outward facing Web and other servers, and code listening on those ports

Services available on the inside of a firewall

Code that processes incoming data, email, XML, office documents, and industry-specific custom data exchange formats

Interfaces, SQL, and Web forms

An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

Network Attack Surface

Vulnerabilities over an enterprise network, wide-area network, or the Internet

Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks

Software Attack Surface

Vulnerabilities in application, utility, or operating system code

Particular focus is Web server software

Human Attack Surface

Vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders

Standards

- Standards have been developed to cover management practices and the overall architecture of security mechanisms and services
- The most important of these organizations are:
 - National Institute of Standards and Technology (NIST)
 - NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private sector innovation
 - Internet Society (ISOC)
 - ISOC is a professional membership society that provides leadership in addressing issues that confront the future of the Internet, and is the organization home for the groups responsible for Internet infrastructure standards
 - International Telecommunication Union (ITU-T)
 - ITU is a United Nations agency in which governments and the private sector coordinate global telecom networks and services
 - International Organization for Standardization (ISO)
 - ISO is a nongovernmental organization whose work results in international agreements that are published as International Standards

Summary

- Computer security concepts
 - Definition
 - Challenges
 - Model
- Threats, attacks, and assets
 - Threats and attacks
 - Threats and assets
- Security functional requirements
- Standards
- Fundamental security design principles
- Attack surfaces and attack trees
 - Attack surfaces
 - Attack trees
- Computer security strategy
 - Security policy
 - Security implementation
 - Assurance and evaluation

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 2

Cryptographic Tools

Symmetric Encryption

- The universal technique for providing confidentiality for transmitted or stored data
- Also referred to as conventional encryption or single-key encryption
- Two requirements for secure use:
 - Need a strong encryption algorithm
 - Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure

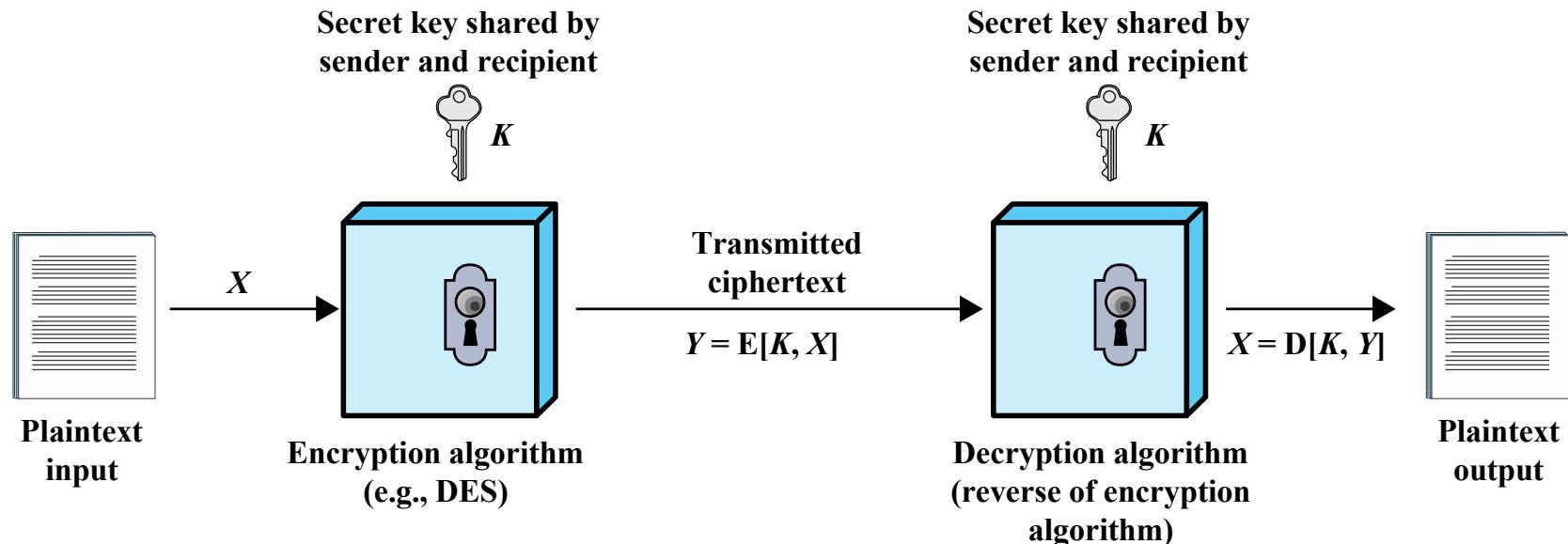


Figure 2.1 Simplified Model of Symmetric Encryption

Attacking Symmetric Encryption

Cryptanalytic Attacks

- Rely on:
 - Nature of the algorithm
 - Some knowledge of the general characteristics of the plaintext
 - Some sample plaintext-ciphertext pairs
- Exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or the key being used
 - If successful all future and past messages encrypted with that key are compromised

Brute-Force Attacks

- Try all possible keys on some ciphertext until an intelligible translation into plaintext is obtained
 - On average half of all possible keys must be tried to achieve success

Table 2.1

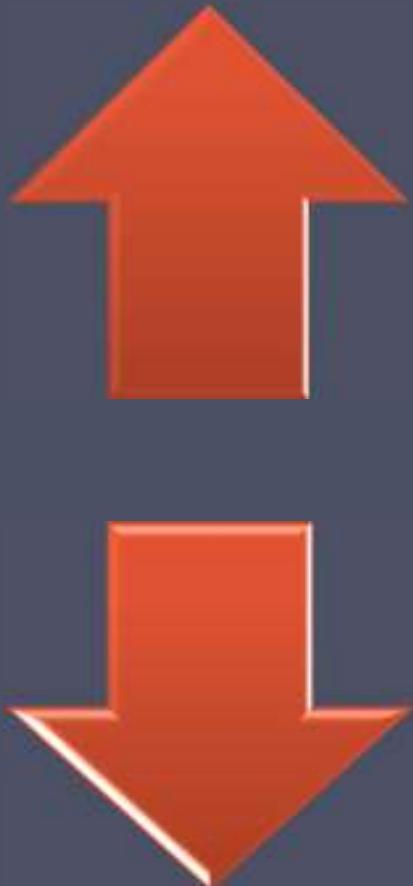
	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard

AES = Advanced Encryption Standard

Comparison of Three Popular Symmetric Encryption Algorithms

Data Encryption Standard (DES)



- Until recently was the most widely used encryption scheme
 - FIPS PUB 46
 - Referred to as the Data Encryption Algorithm (DEA)
 - Uses 64 bit plaintext block and 56 bit key to produce a 64 bit ciphertext block
- Strength concerns:
 - Concerns about the algorithm itself
 - DES is the most studied encryption algorithm in existence
 - Concerns about the use of a 56-bit key
 - The speed of commercial off-the-shelf processors makes this key length woefully inadequate

Table 2.2

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 decryptions/s	Time Required at 10^{13} decryptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	$2^{55} \text{ ns} = 1.125 \text{ years}$	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	$2^{127} \text{ ns} = 5.3 \times 10^{21}$ years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	$2^{167} \text{ ns} = 5.8 \times 10^{33}$ years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	$2^{191} \text{ ns} = 9.8 \times 10^{40}$ years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	$2^{255} \text{ ns} = 1.8 \times 10^{60}$ years	1.8×10^{56} years

Average Time Required for Exhaustive Key Search

Triple DES (3DES)

- Repeats basic DES algorithm three times using either two or three unique keys
- First standardized for use in financial applications in ANSI standard X9.17 in 1985
- Attractions:
 - 168-bit key length overcomes the vulnerability to brute-force attack of DES
 - Underlying encryption algorithm is the same as in DES
- Drawbacks:
 - Algorithm is sluggish in software
 - Uses a 64-bit block size

Advanced Encryption Standard (AES)

Needed a replacement for 3DES

3DES was not reasonable for long term use

NIST called for proposals for a new AES in 1997

Should have a security strength equal to or better than 3DES

Significantly improved efficiency

Symmetric block cipher

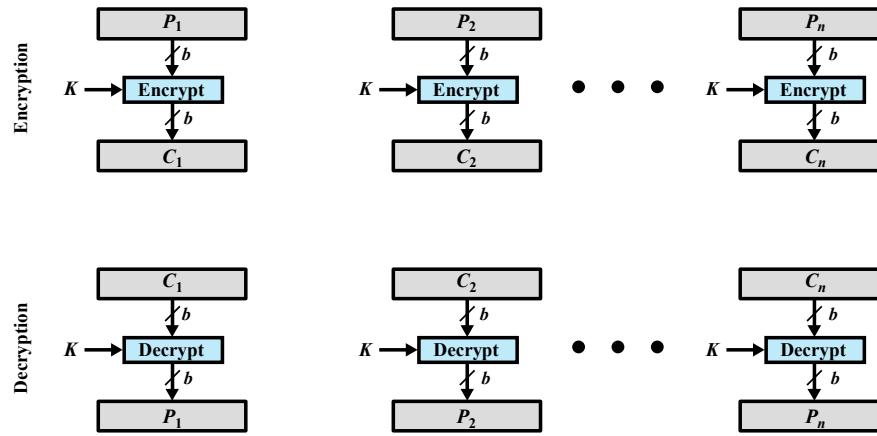
128 bit data and 128/192/256 bit keys

Selected Rijndael in November 2001

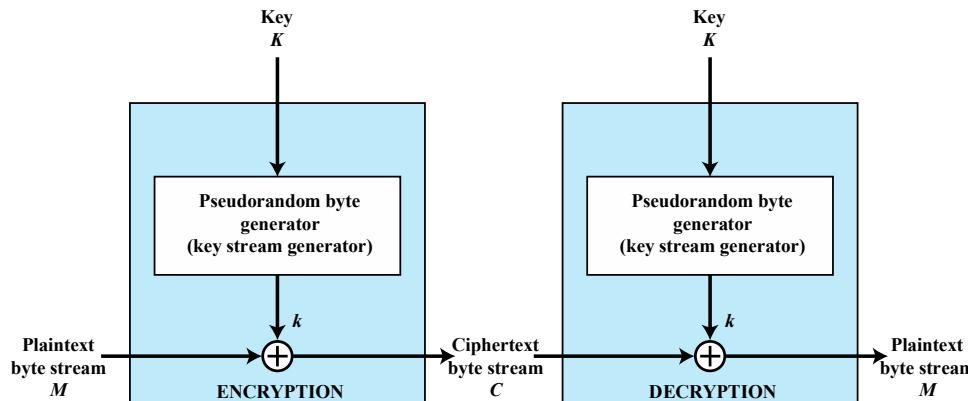
Published as FIPS 197

Practical Security Issues

- Typically symmetric encryption is applied to a unit of data larger than a single 64-bit or 128-bit block
- Electronic codebook (ECB) mode is the simplest approach to multiple-block encryption
 - Each block of plaintext is encrypted using the same key
 - Cryptanalysts may be able to exploit regularities in the plaintext
- Modes of operation
 - Alternative techniques developed to increase the security of symmetric block encryption for large sequences
 - Overcomes the weaknesses of ECB



(a) Block cipher encryption (electronic codebook mode)



(b) Stream encryption

Figure 2.2 Types of Symmetric Encryption

Block & Stream Ciphers

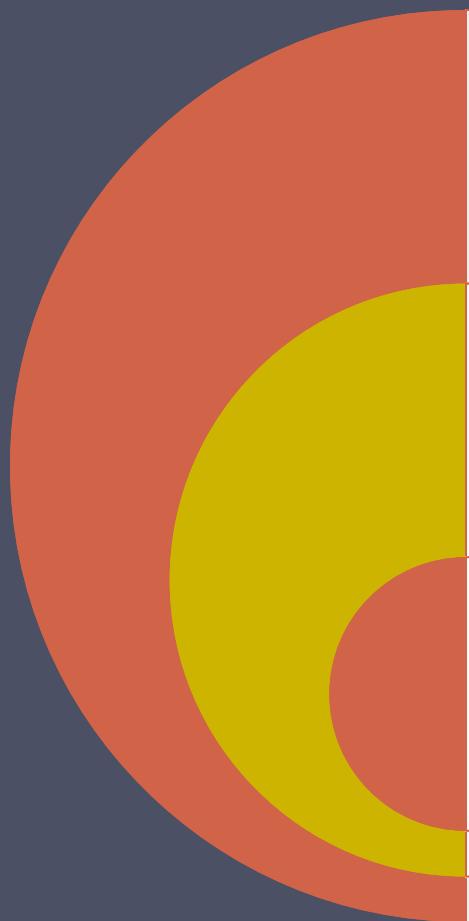
Block Cipher

- Processes the input one block of elements at a time
- Produces an output block for each input block
- Can reuse keys
- More common

Stream Cipher

- Processes the input elements continuously
- Produces output one element at a time
- Primary advantage is that they are almost always faster and use far less code
- Encrypts plaintext one byte at a time
- Pseudorandom stream is one that is unpredictable without knowledge of the input key

Message Authentication



Protects against
active attacks

Verifies received
message is
authentic

Can use
conventional
encryption

- Contents have not been altered
- From authentic source
- Timely and in correct sequence

- Only sender and receiver share a key

Message Authentication Without Confidentiality

- Message encryption by itself does not provide a secure form of authentication
- It is possible to combine authentication and confidentiality in a single algorithm by encrypting a message plus its authentication tag
- Typically message authentication is provided as a separate function from message encryption
- Situations in which message authentication without confidentiality may be preferable include:
 - There are a number of applications in which the same message is broadcast to a number of destinations
 - An exchange in which one side has a heavy load and cannot afford the time to decrypt all incoming messages
 - Authentication of a computer program in plaintext is an attractive service
- Thus, there is a place for both authentication and encryption in meeting security requirements

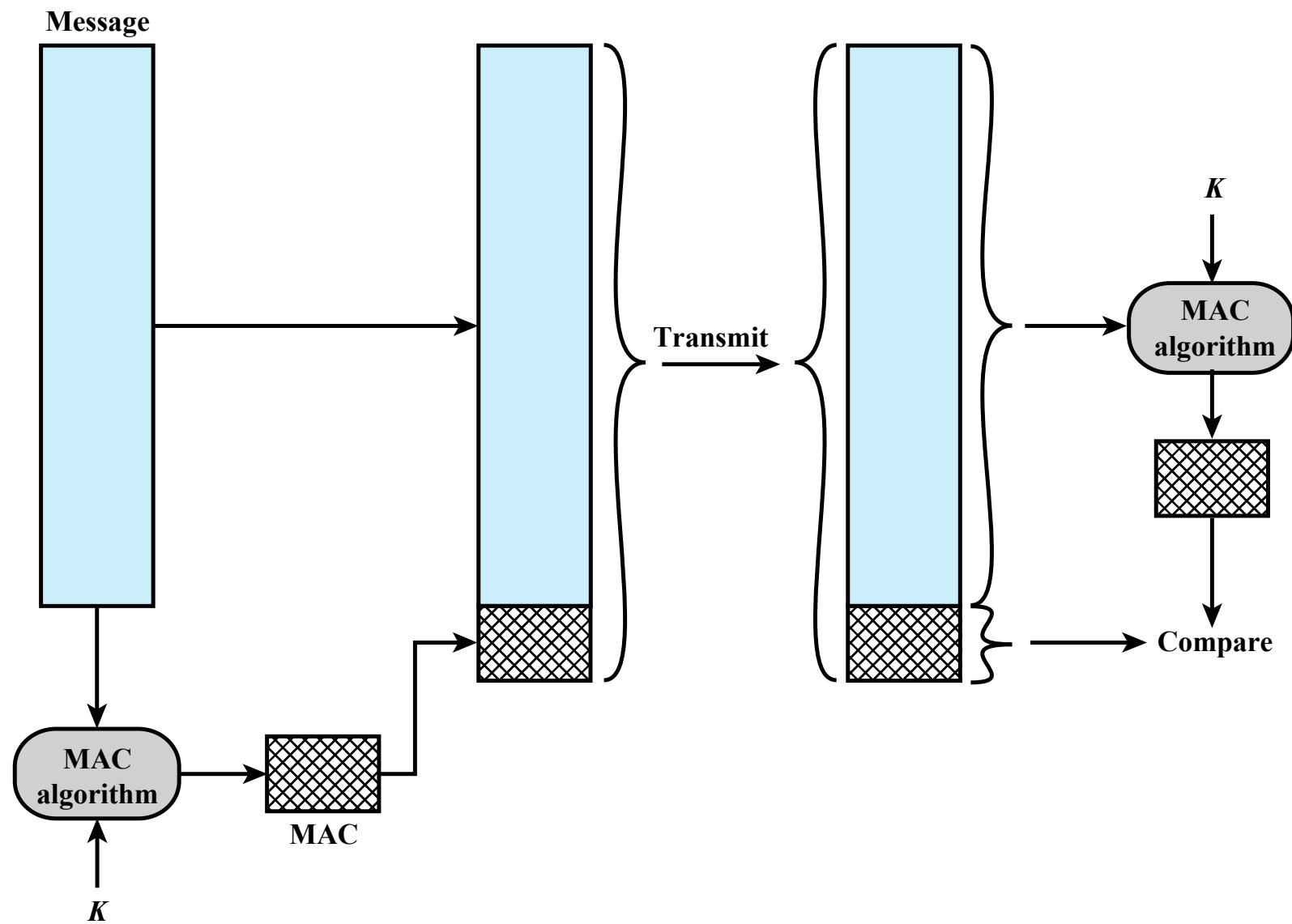


Figure 2.3 Message Authentication Using a Message Authentication Code (MAC).



201

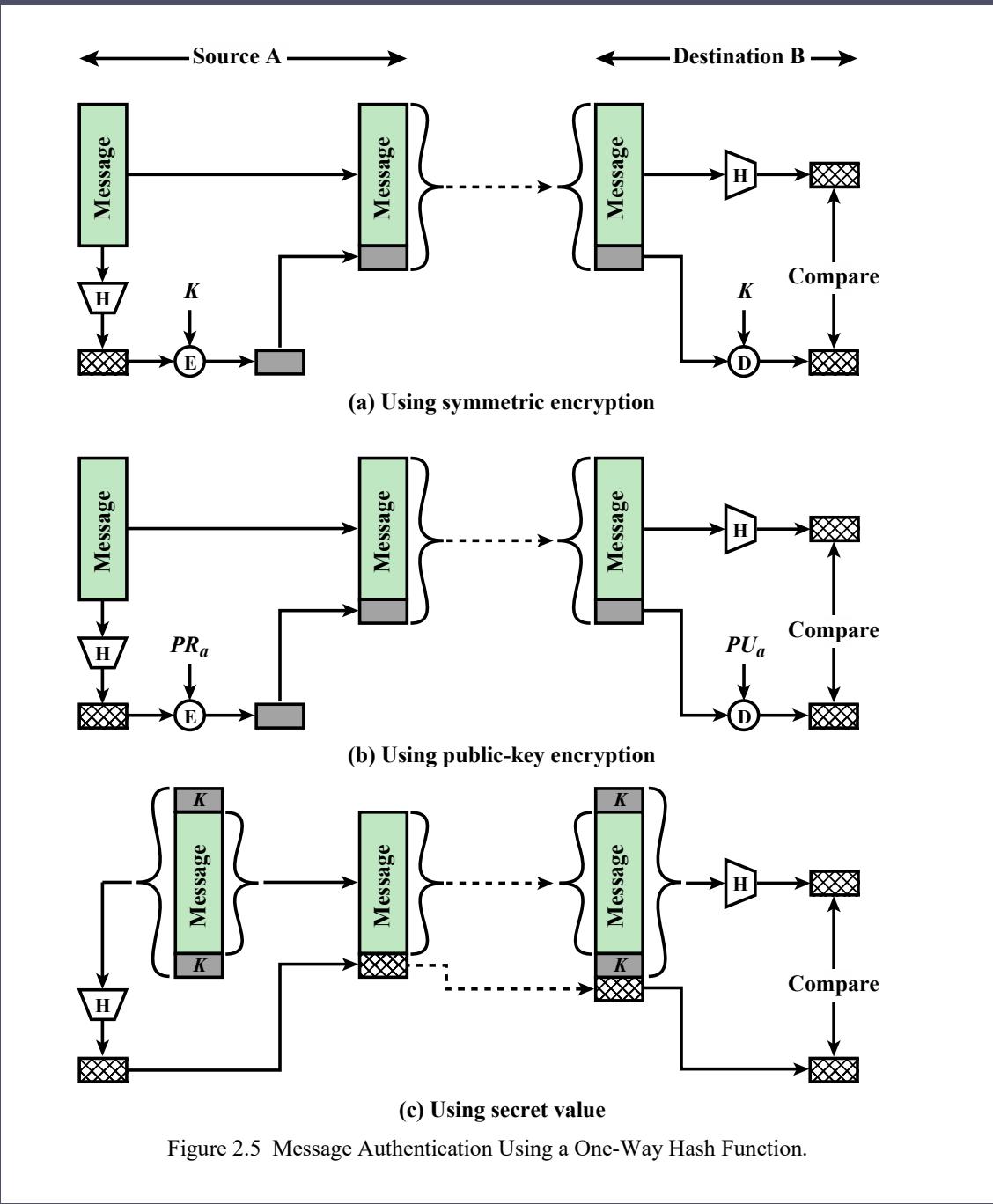


Figure 2.5 Message Authentication Using a One-Way Hash Function.

To be useful for message authentication, a hash function H must have the following properties:

- Can be applied to a block of data of any size
- Produces a fixed-length output
- $H(x)$ is relatively easy to compute for any given x
- One-way or pre-image resistant
 - Computationally infeasible to find x such that $H(x) = h$
- Computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$
- Collision resistant or strong collision resistance
 - Computationally infeasible to find any pair (x,y) such that $H(x) = H(y)$

Security of Hash Functions

There are two approaches to attacking a secure hash function:

Cryptanalysis

- Exploit logical weaknesses in the algorithm

Brute-force attack

- Strength of hash function depends solely on the length of the hash code produced by the algorithm

SHA most widely used hash algorithm

Additional secure hash function applications:

Passwords

- Hash of a password is stored by an operating system

Intrusion detection

- Store $H(F)$ for each file on a system and secure the hash values

Public-Key Encryption Structure

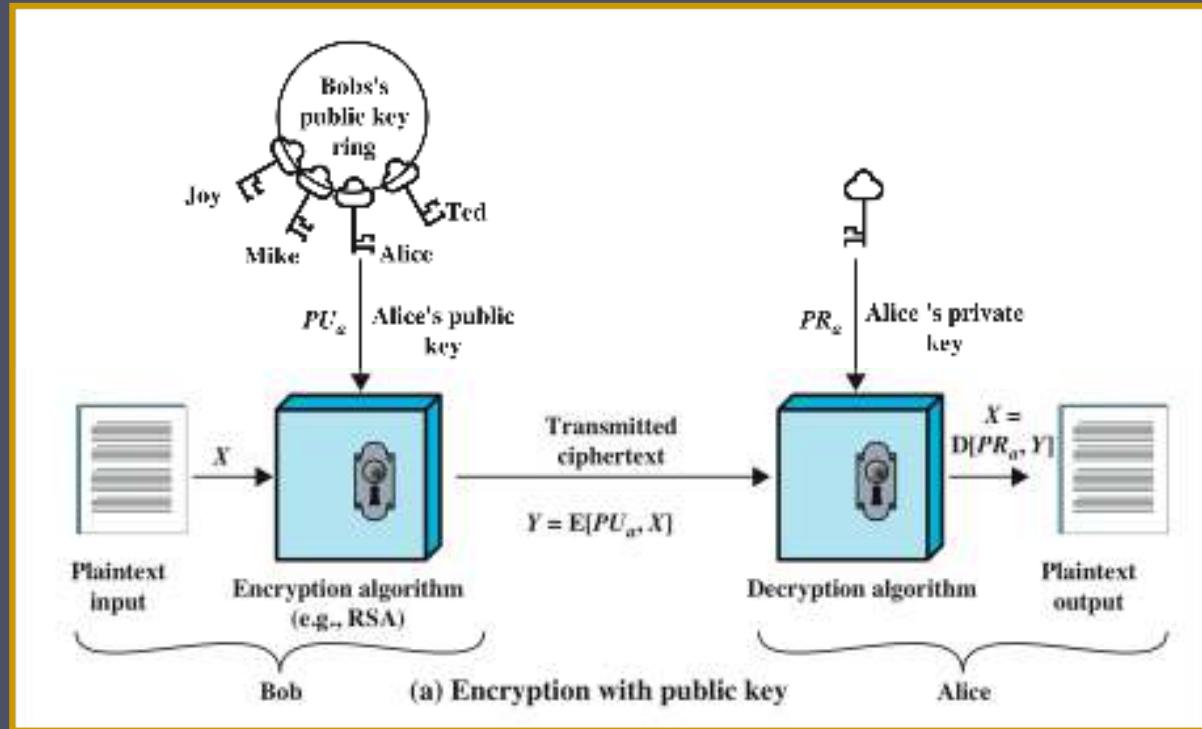
Publicly proposed by Diffie and Hellman in 1976

Based on mathematical functions

Asymmetric

- Uses two separate keys
- Public key and private key
- Public key is made public for others to use

Some form of protocol is needed for distribution



- **Plaintext**
 - Readable message or data that is fed into the algorithm as input
- **Encryption algorithm**
 - Performs transformations on the plaintext
- **Public and private key**
 - Pair of keys, one for encryption, one for decryption
- **Ciphertext**
 - Scrambled message produced as output
- **Decryption key**
 - Produces the original plaintext

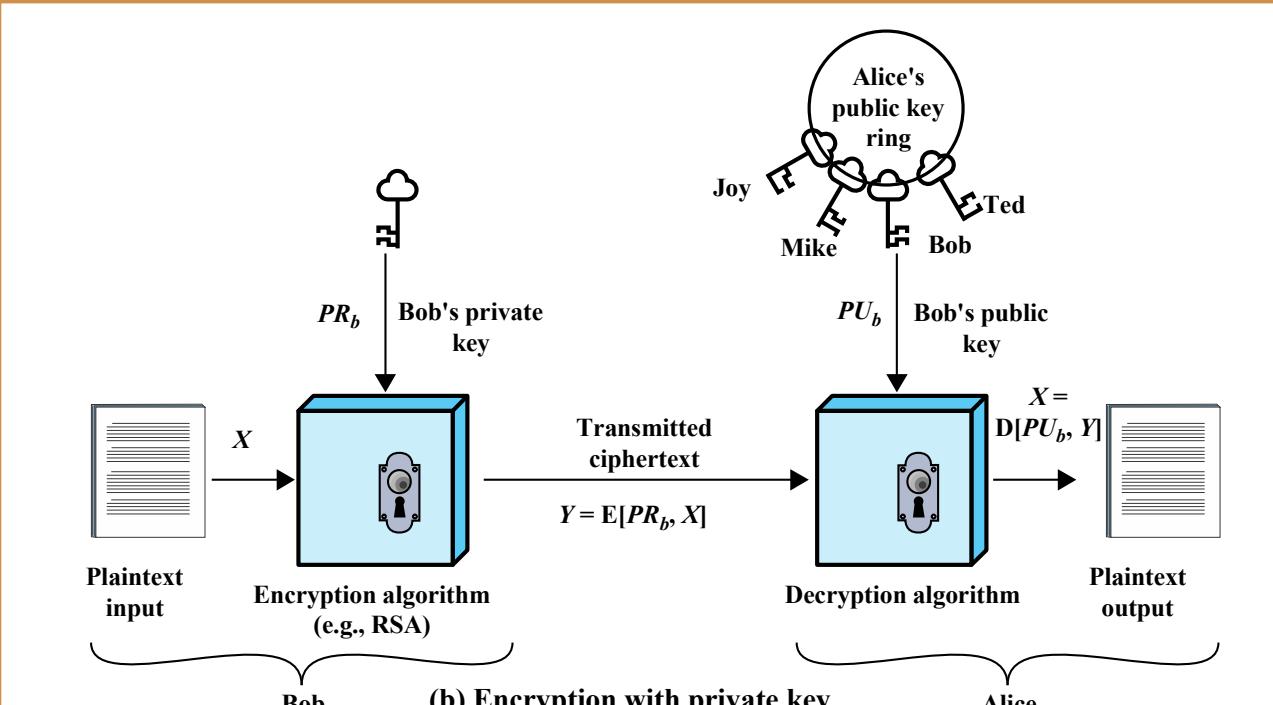


Figure 2.6 Public-Key Cryptography

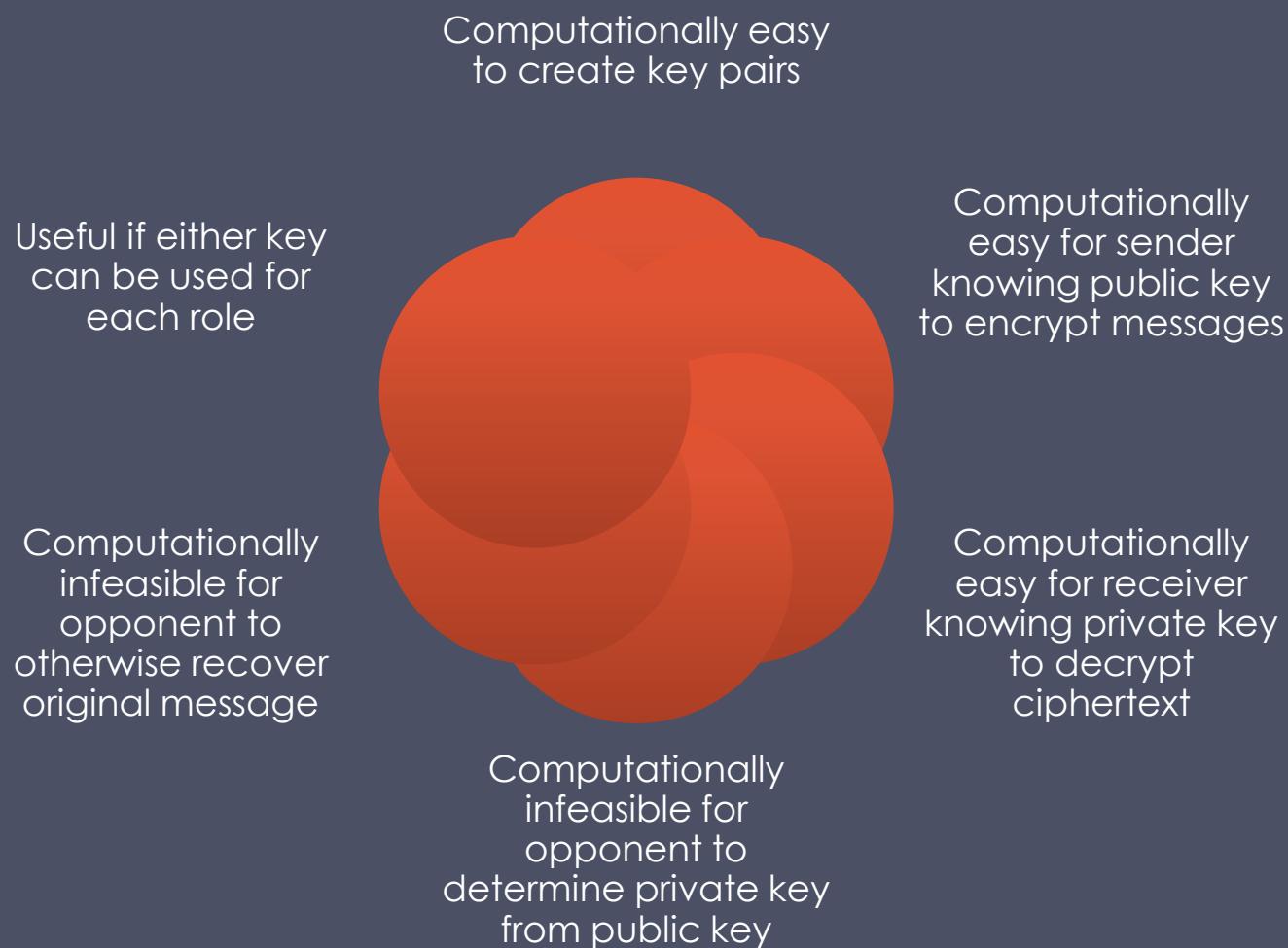
- User encrypts data using his or her own private key
- Anyone who knows the corresponding public key will be able to decrypt the message

Table 2.3

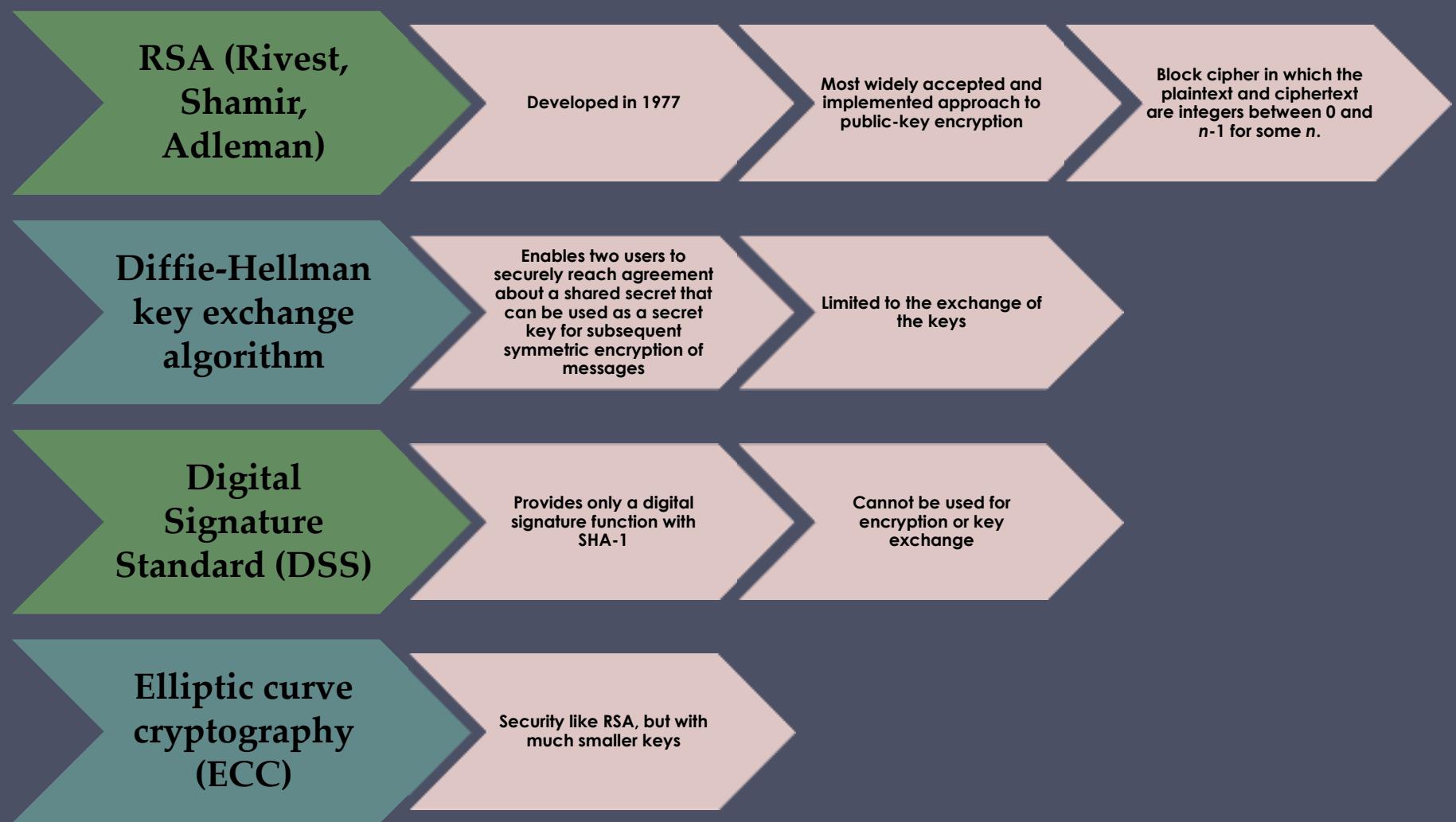
Applications for Public-Key Cryptosystems

Algorithm	Digital Signature	Symmetric Key Distribution	Encryption of Secret Keys
RSA	Yes	Yes	Yes
Diffie-Hellman	No	Yes	No
DSS	Yes	No	No
Elliptic Curve	Yes	Yes	Yes

Requirements for Public-Key Cryptosystems



Asymmetric Encryption Algorithms



Digital Signatures

- NIST FIPS PUB 186-4 defines a digital signature as:

"The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation."
- Thus, a digital signature is a data-dependent bit pattern, generated by an agent as a function of a file, message, or other form of data block
- FIPS 186-4 specifies the use of one of three digital signature algorithms:
 - Digital Signature Algorithm (DSA)
 - RSA Digital Signature Algorithm
 - Elliptic Curve Digital Signature Algorithm (ECDSA)

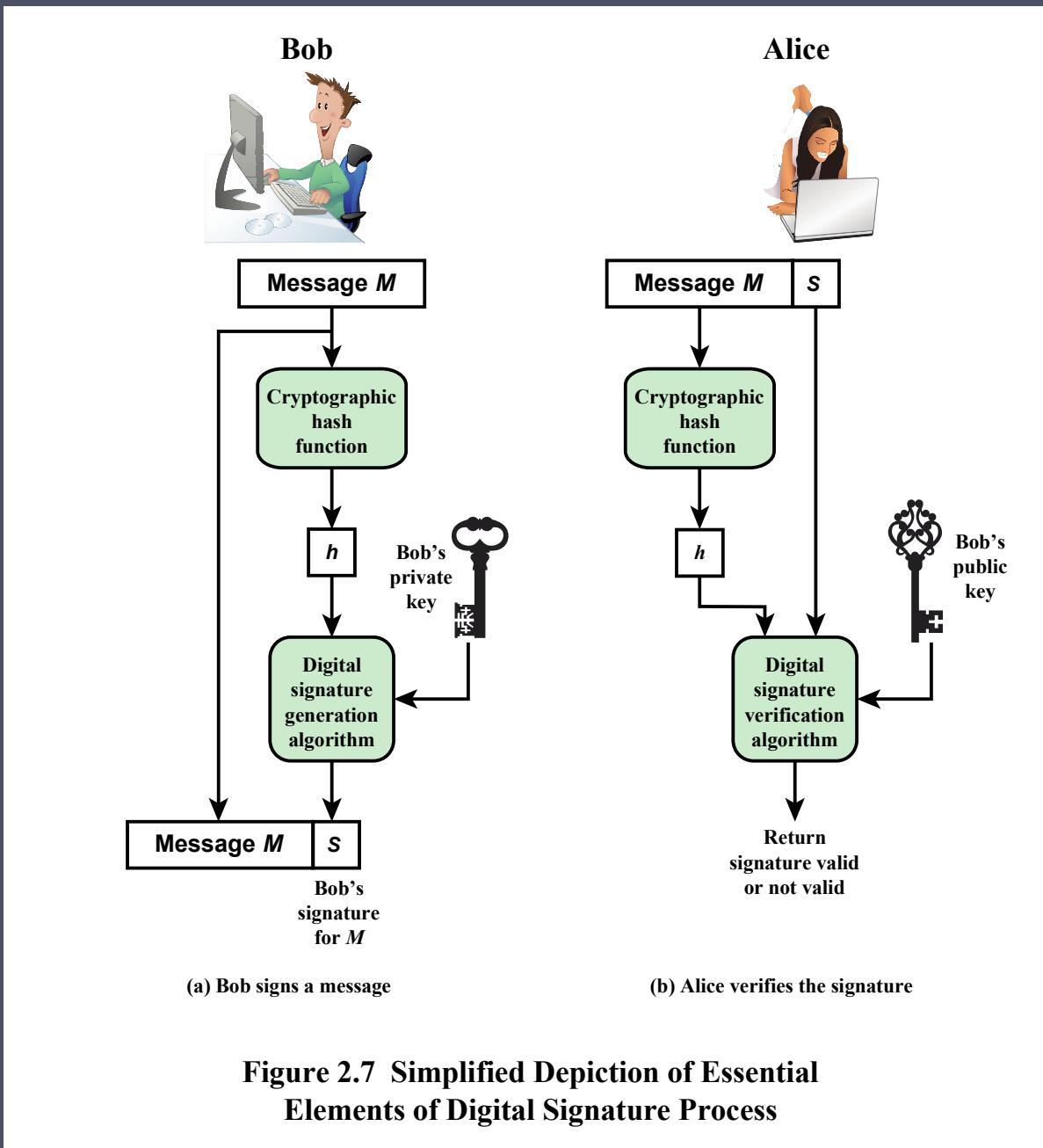


Figure 2.7 Simplified Depiction of Essential Elements of Digital Signature Process

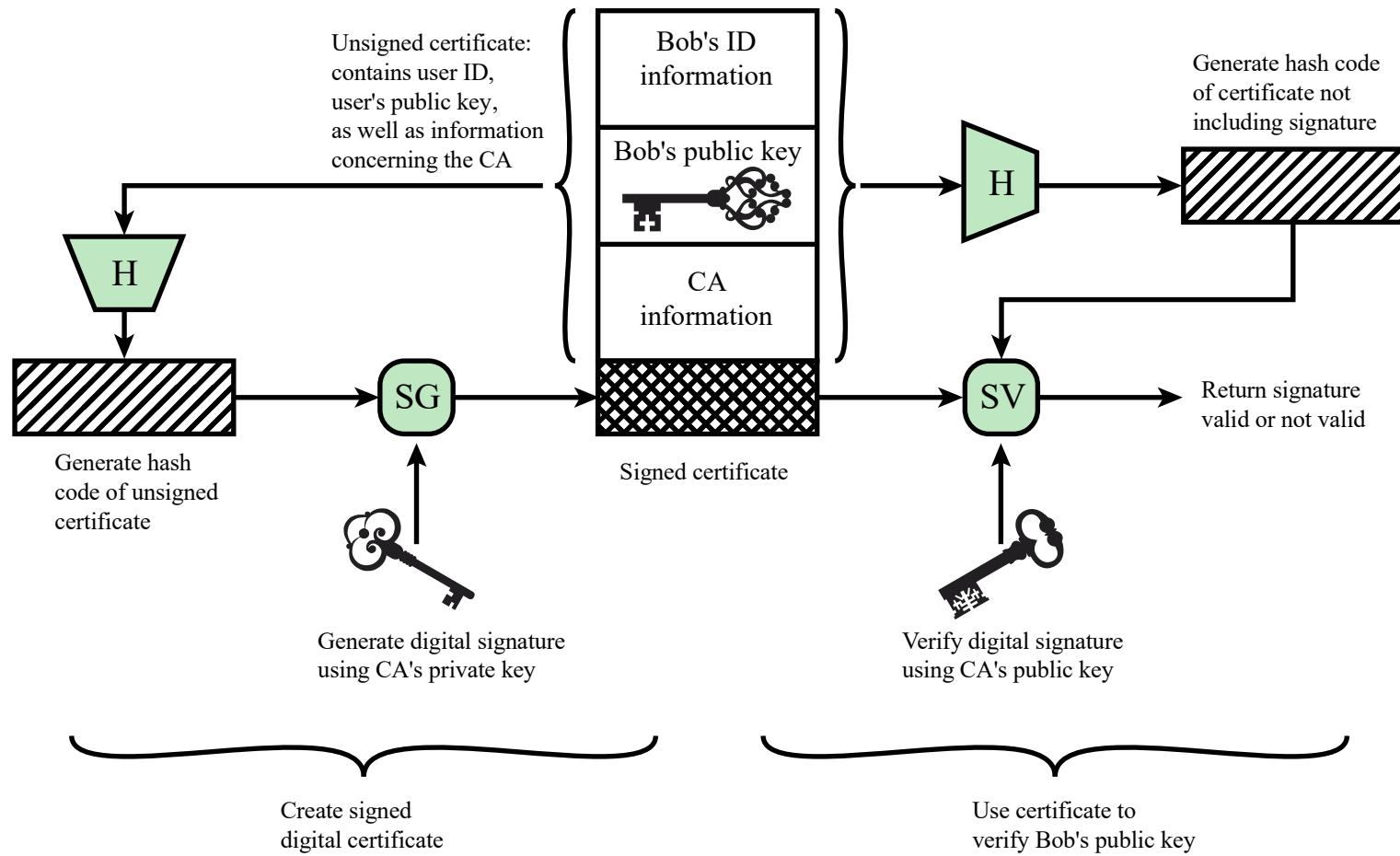
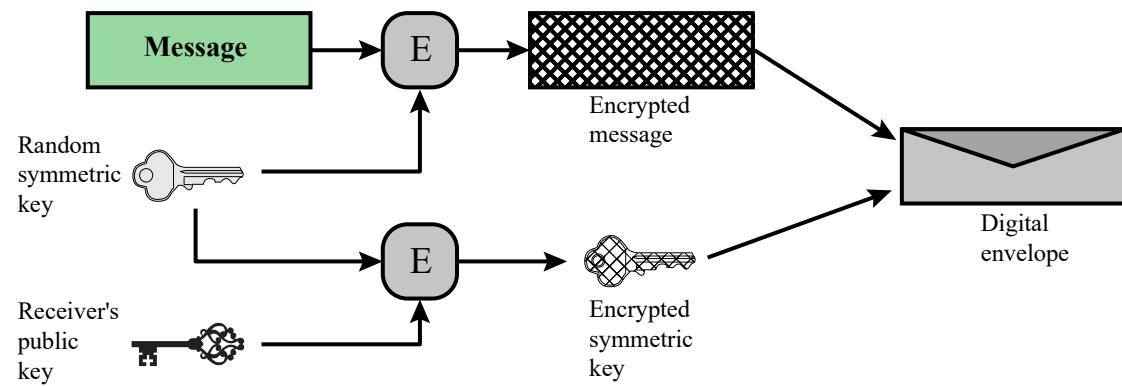
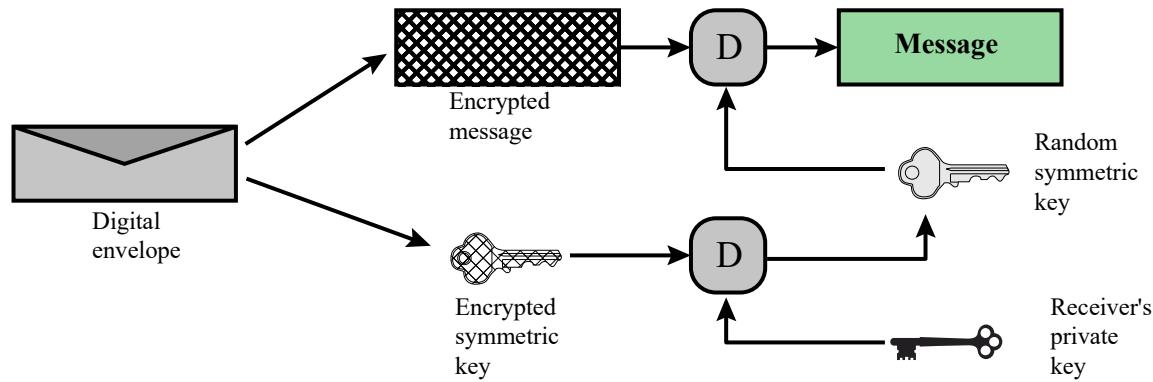


Figure 2.8 Public-Key Certificate Use



(a) Creation of a digital envelope



(b) Opening a digital envelope

Figure 2.9 Digital Envelopes

Random Numbers

**Uses include
generation of:**

- Keys for public-key algorithms
- Stream key for symmetric stream cipher
- Symmetric key for use as a temporary session key or in creating a digital envelope
- Handshaking to prevent replay attacks
- Session key

Random Number Requirements

Randomness

- Criteria:
 - Uniform distribution
 - Frequency of occurrence of each of the numbers should be approximately the same
 - Independence
 - No one value in the sequence can be inferred from the others

Unpredictability

- Each number is statistically independent of other numbers in the sequence
- Opponent should not be able to predict future elements of the sequence on the basis of earlier elements

Random versus Pseudorandom

Cryptographic applications typically make use of algorithmic techniques for random number generation

- Algorithms are deterministic and therefore produce sequences of numbers that are not statistically random

Pseudorandom numbers are:

- Sequences produced that satisfy statistical randomness tests
- Likely to be predictable

True random number generator (TRNG):

- Uses a nondeterministic source to produce randomness
- Most operate by measuring unpredictable natural processes
 - e.g. radiation, gas discharge, leaky capacitors
- Increasingly provided on modern processors

Practical Application: Encryption of Stored Data

Common to encrypt transmitted data

Much less common for stored data

There is often little protection beyond domain authentication and operating system access controls

Data are archived for indefinite periods

Even though erased, until disk sectors are reused data are recoverable

Approaches to encrypt stored data:

Use a commercially available encryption package

Back-end appliance

Library based tape encryption

Background laptop/PC data encryption

Summary

- Confidentiality with symmetric encryption
 - Symmetric encryption
 - Symmetric block encryption algorithms
 - Stream ciphers
- Message authentication and hash functions
 - Authentication using symmetric encryption
 - Message authentication without message encryption
 - Secure hash functions
 - Other applications of hash functions
- Random and pseudorandom numbers
 - The use of random numbers
 - Random versus pseudorandom
- Public-key encryption
 - Structure
 - Applications for public-key cryptosystems
 - Requirements for public-key cryptography
 - Asymmetric encryption algorithms
- Digital signatures and key management
 - Digital signature
 - Public-key certificates
 - Symmetric key exchange using public-key encryption
 - Digital envelopes
- Practical Application: Encryption of Stored Data

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 3

User Authentication

NIST SP 800-63-3 (*Digital Authentication Guideline*, October 2016) defines digital user authentication as:

“The process of establishing confidence in user identities that are presented electronically to an information system.”

Table 3.1 Identification and Authentication Security Requirements (SP 800-171)

Basic Security Requirements:	
1	Identify information system users, processes acting on behalf of users, or devices.
2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Derived Security Requirements:	
3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.
4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.
5	Prevent reuse of identifiers for a defined period.
6	Disable identifiers after a defined period of inactivity.
7	Enforce a minimum password complexity and change of characters when new passwords are created.
8	Prohibit password reuse for a specified number of generations.
9	Allow temporary password use for system logons with an immediate change to a permanent password.
10	Store and transmit only cryptographically-protected passwords.
11	Obscure feedback of authentication information.

(Table can be found on page 65 in the textbook)

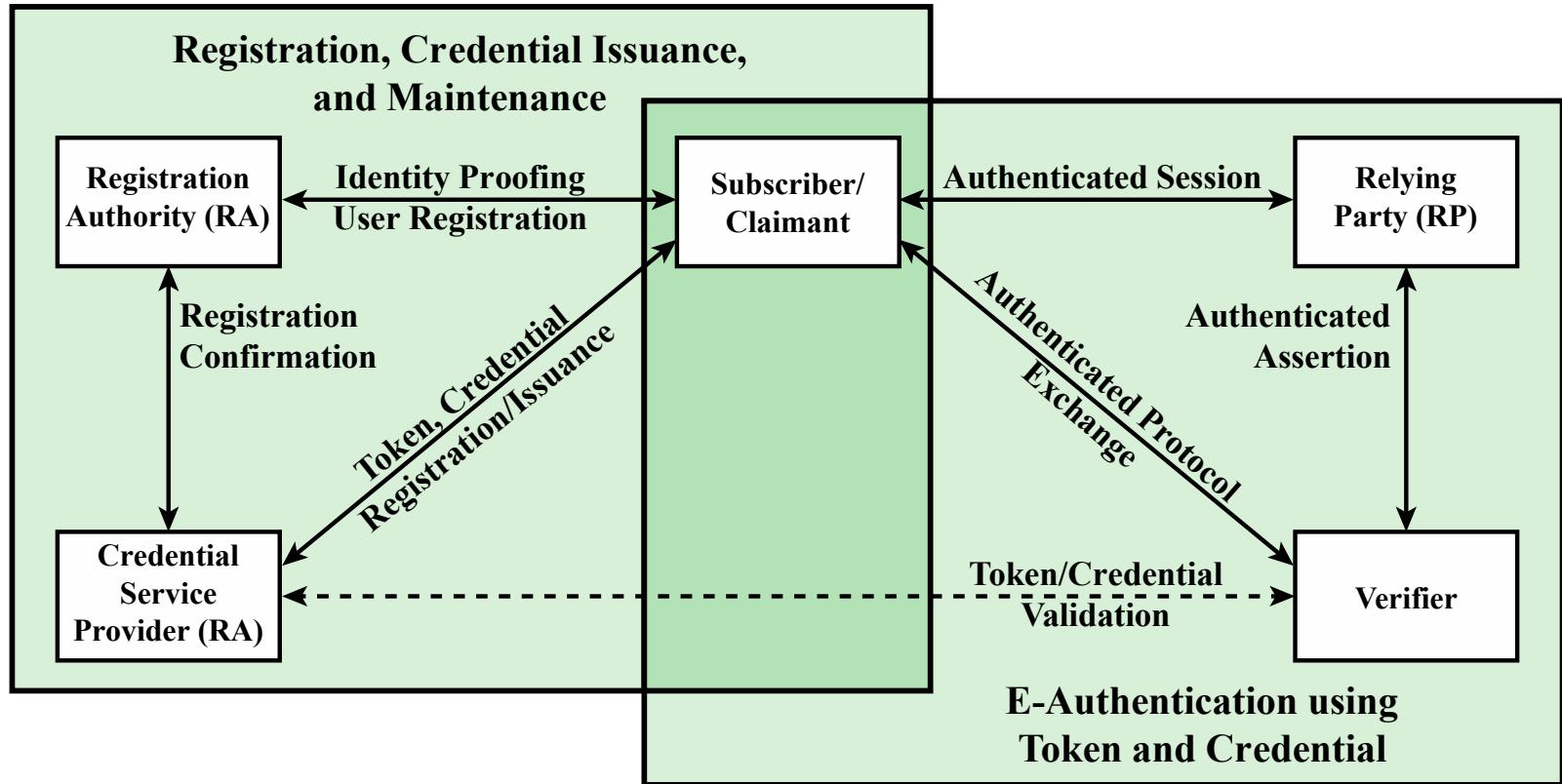


Figure 3.1 The NIST SP 800-63-2 E-Authentication Architectural Model

The four means of authenticating user identity are based on:

Something the individual knows

- Password, PIN, answers to prearranged questions

Something the individual possesses (token)

- Smartcard, electronic keycard, physical key

Something the individual is (static biometrics)

- Fingerprint, retina, face

Something the individual does (dynamic biometrics)

- Voice pattern, handwriting, typing rhythm

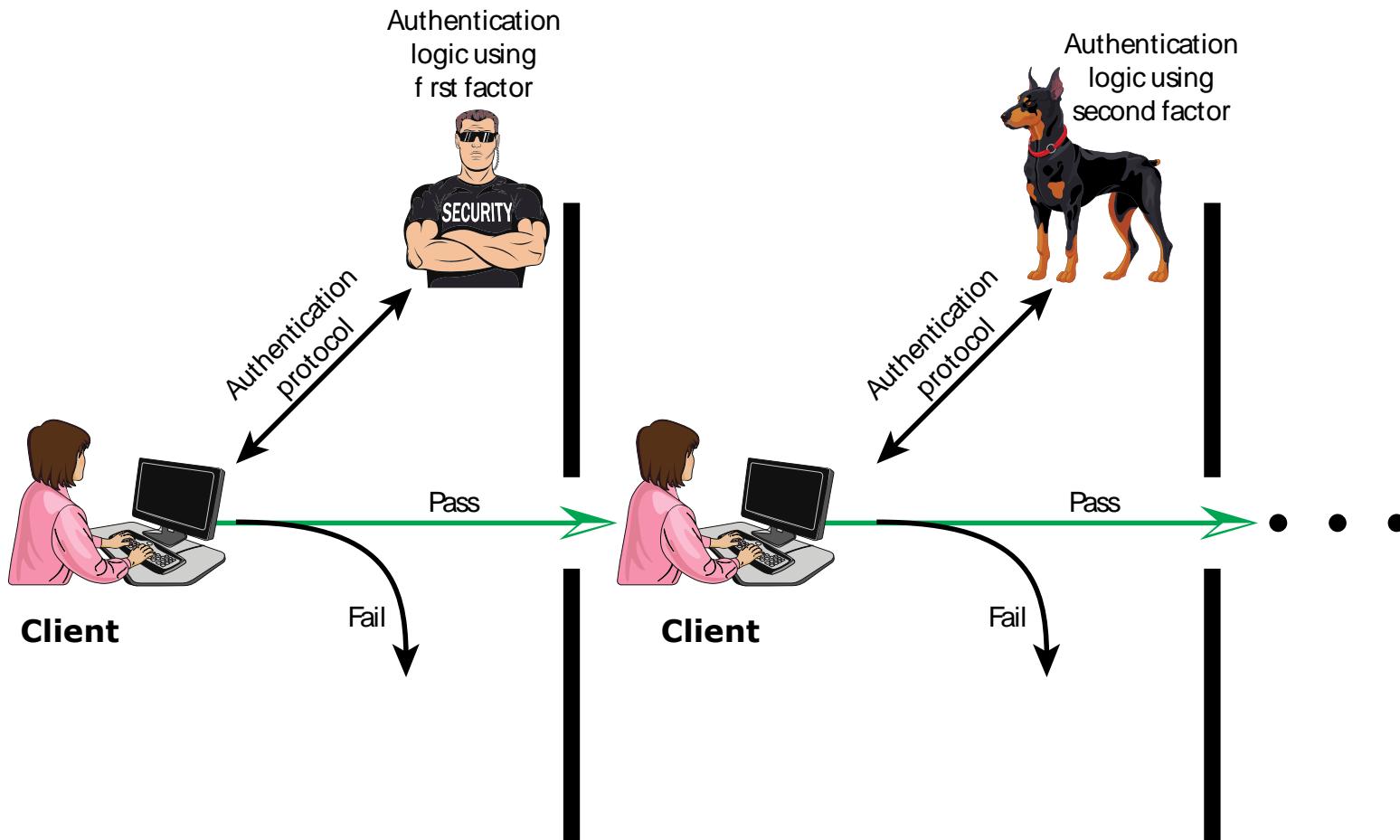
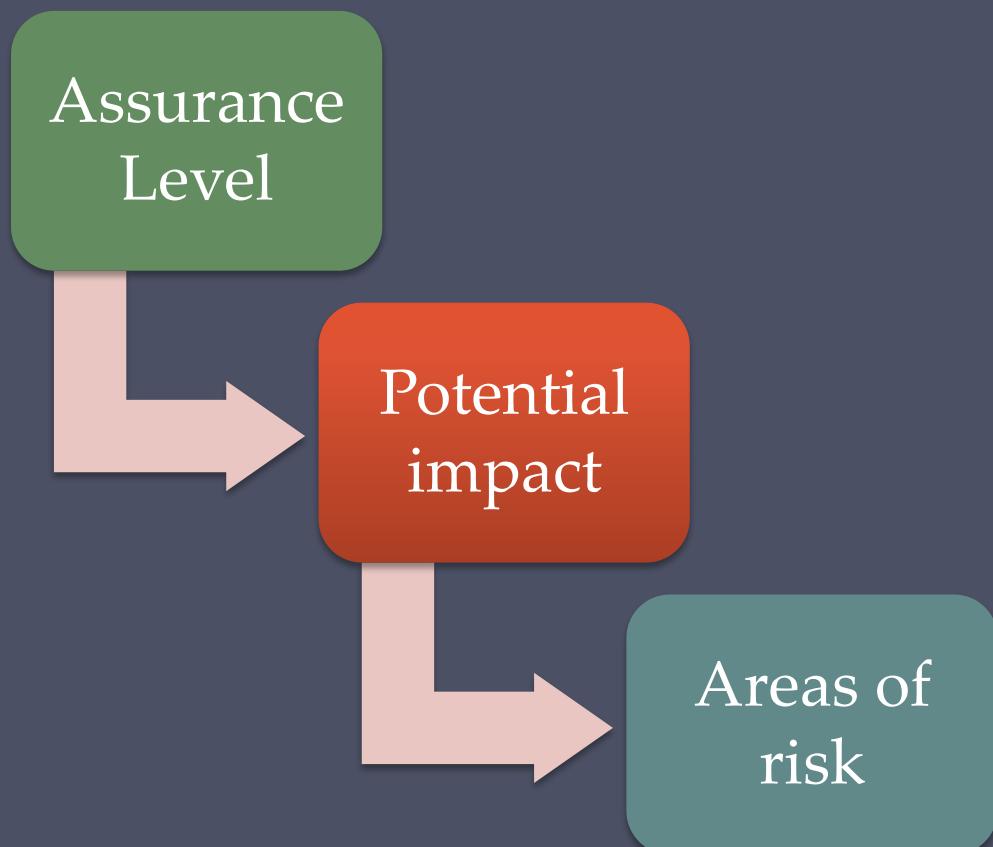


Figure 3.2 Multifactor Authentication

Risk Assessment for User Authentication

- There are three separate concepts:



Assurance Level

Describes an organization's degree of certainty that a user has presented a credential that refers to his or her identity

More specifically is defined as:

The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued

The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued

Four levels of assurance

Level 1

- Little or no confidence in the asserted identity's validity

Level 2

- Some confidence in the asserted identity's validity

Level 3

- High confidence in the asserted identity's validity

Level 4

- Very high confidence in the asserted identity's validity

Potential Impact

- FIPS 199 defines three levels of potential impact on organizations or individuals should there be a breach of security:
 - Low
 - An authentication error could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals
 - Moderate
 - An authentication error could be expected to have a serious adverse effect
 - High
 - An authentication error could be expected to have a severe or catastrophic adverse effect

Table 3.2

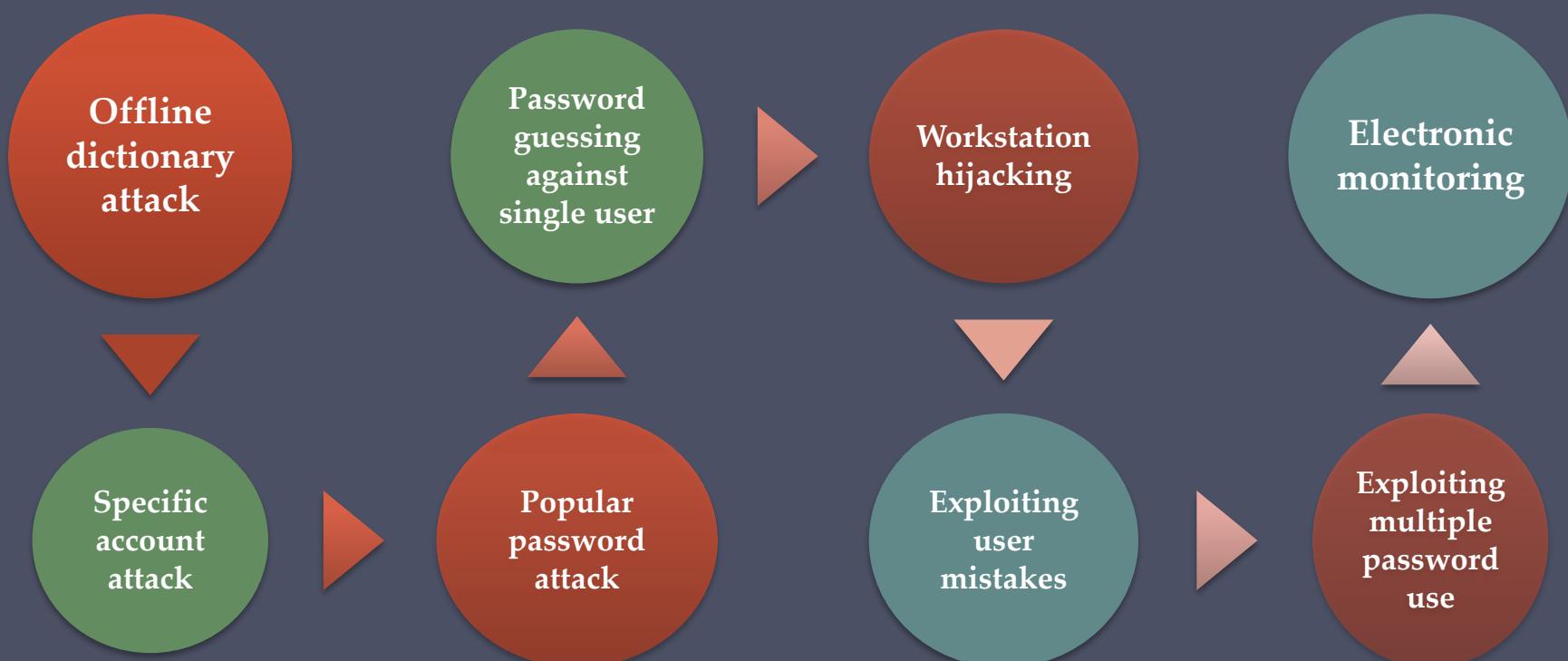
Potential Impact Categories for Authentication Errors	Assurance Level Impact Profiles			
	1	2	3	4
Inconvenience, distress, or damage to standing or reputation	Low	Mod	Mod	High
	Low	Mod	Mod	High
Financial loss or organization liability	None	Low	Mod	High
Harm to organization programs or interests	None	Low	Mod	High
Unauthorized release of sensitive information				Mod/ High
Personal safety	None	None	Low	Mod/ High
Civil or criminal violations	None	Low	Mod	High

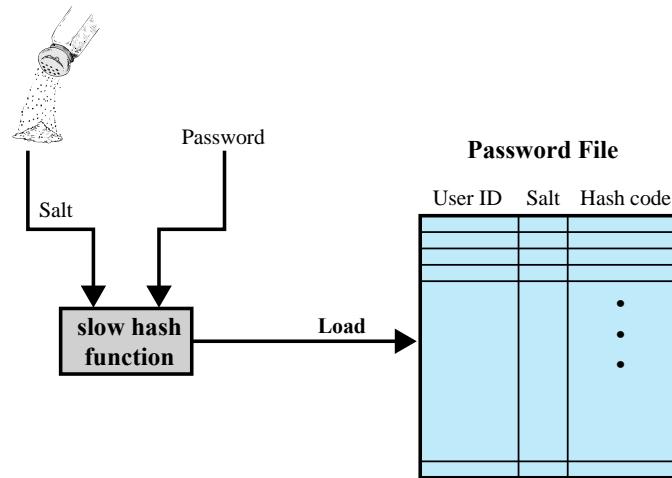
Maximum Potential Impacts for Each Assurance Level

Password-Based Authentication

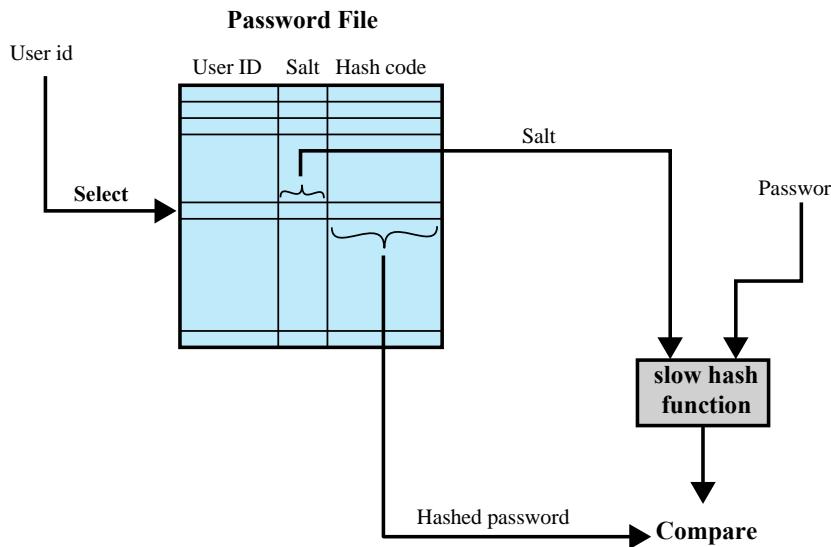
- Widely used line of defense against intruders
 - User provides name/login and password
 - System compares password with the one stored for that specified login
- The user ID:
 - Determines that the user is authorized to access the system
 - Determines the user's privileges
 - Is used in discretionary access control

Password Vulnerabilities





(a) Loading a new password



(b) Verifying a password

Figure 3.3 UNIX Password Scheme

UNIX Implementation

Original scheme

- Up to eight printable characters in length
- 12-bit salt used to modify DES encryption into a one-way hash function
- Zero value repeatedly encrypted 25 times
- Output translated to 11 character sequence

Now regarded as inadequate

- Still often required for compatibility with existing account management software or multivendor environments

Improved Implementations

Much stronger hash/salt schemes available for Unix

OpenBSD uses Blowfish block cipher based hash algorithm called Bcrypt

- Most secure version of Unix hash/salt scheme
- Uses 128-bit salt to create 192-bit hash value

Recommended hash function is based on MD5

- Salt of up to 48-bits
- Password length is unlimited
- Produces 128-bit hash
- Uses an inner loop with 1000 iterations to achieve slowdown

Password Cracking

Dictionary attacks

- Develop a large dictionary of possible passwords and try each against the password file
- Each password must be hashed using each salt value and then compared to stored hash values

Rainbow table attacks

- Pre-compute tables of hash values for all salts
- A mammoth table of hash values
- Can be countered by using a sufficiently large salt value and a sufficiently large hash length

Password crackers exploit the fact that people choose easily guessable passwords

- Shorter password lengths are also easier to crack

John the Ripper

- Open-source password cracker first developed in 1996
- Uses a combination of brute-force and dictionary techniques

Modern Approaches

- Complex password policy
 - Forcing users to pick stronger passwords
- However password-cracking techniques have also improved
 - The processing capacity available for password cracking has increased dramatically
 - The use of sophisticated algorithms to generate potential passwords
 - Studying examples and structures of actual passwords in use

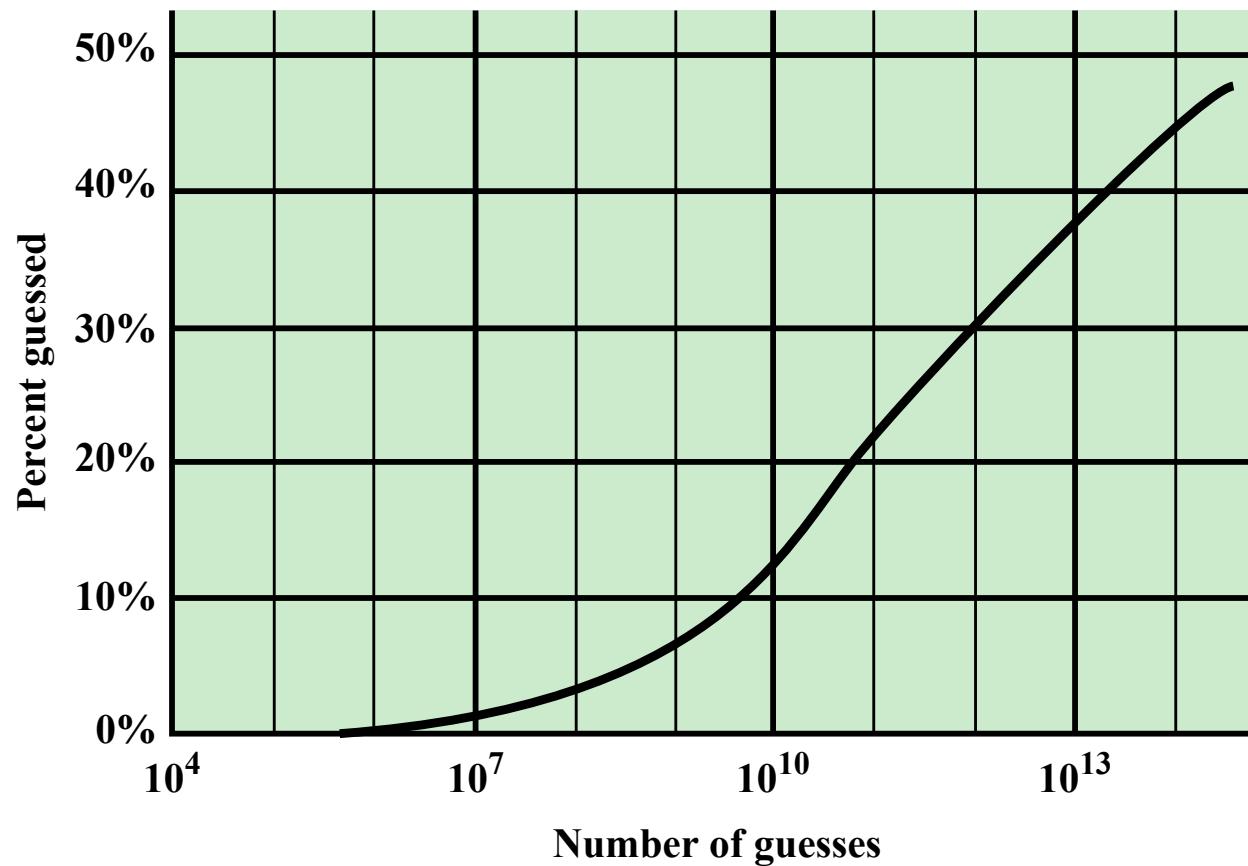


Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses

Password File Access Control

Can block offline guessing attacks by denying access to encrypted passwords

Make available only to privileged users

Shadow password file

Vulnerabilities

Weakness in the OS that allows access to the file

Accident with permissions making it readable

Users with same password on other systems

Access from backup media

Sniff passwords in network traffic

Password Selection Strategies

User education

Users can be told the importance of using hard to guess passwords and can be provided with guidelines for selecting strong passwords



Computer generated passwords

Users have trouble remembering them



Reactive password checking

System periodically runs its own password cracker to find guessable passwords



Complex password policy

User is allowed to select their own password, however the system checks to see if the password is allowable, and if not, rejects it

Goal is to eliminate guessable passwords while allowing the user to select a password that is memorable

Proactive Password Checking

- Rule enforcement
 - Specific rules that passwords must adhere to
- Password checker
 - Compile a large dictionary of passwords not to use
- Bloom filter
 - Used to build a table based on hash values
 - Check desired password against this table

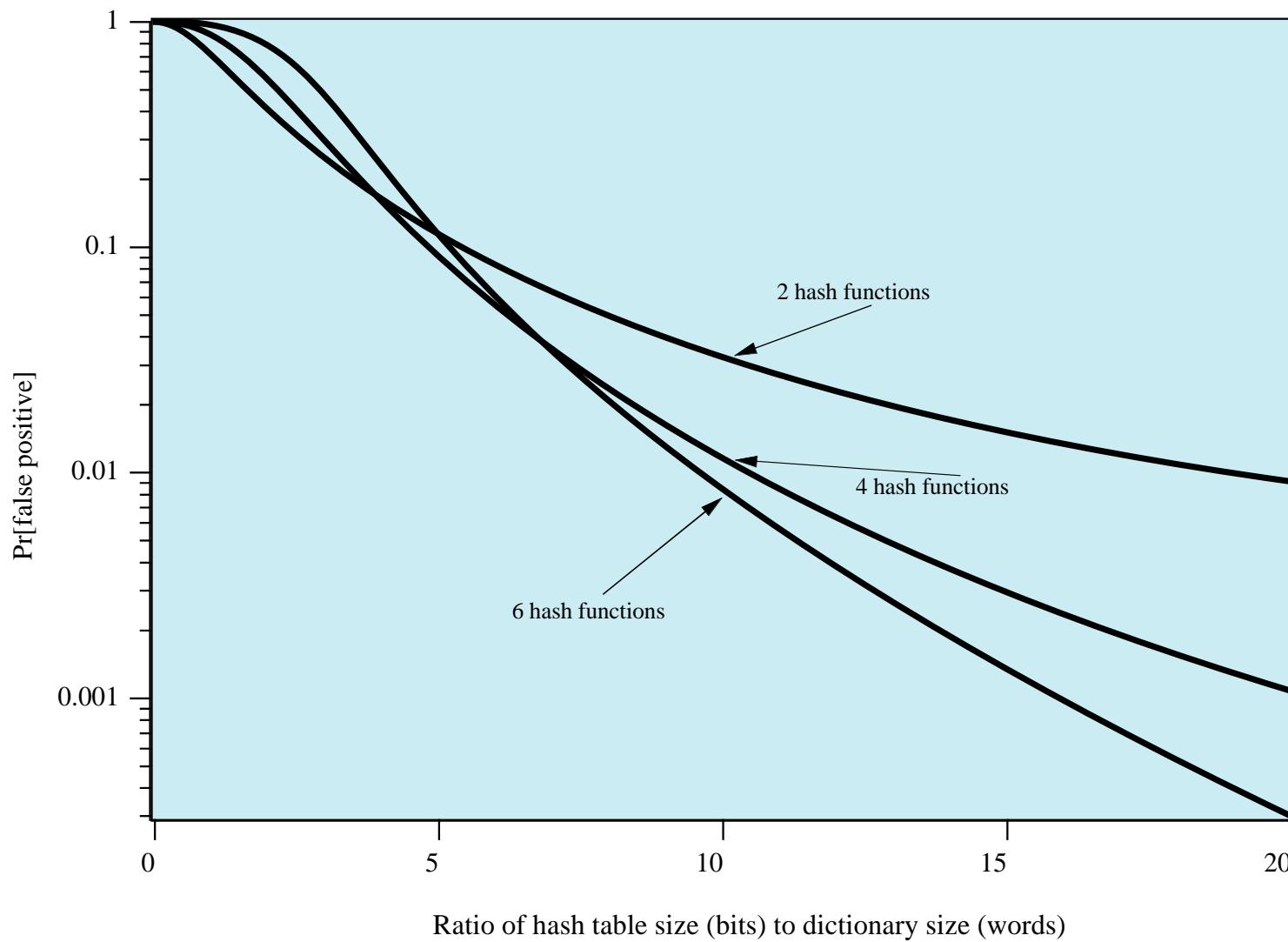


Figure 3.5 Performance of Bloom Filter

Table 3.3

Card Type	Defining Feature	Example
Embossed	Raised characters only, on front	Old credit card
Magnetic stripe	Magnetic bar on back, characters on front	Bank card
Memory	Electronic memory inside	Prepaid phone card
Smart	Electronic memory and processor inside	Biometric ID card
Contact	Electrical contacts exposed on surface	
Contactless	Radio antenna embedded inside	

Types of Cards Used as Tokens

Memory Cards

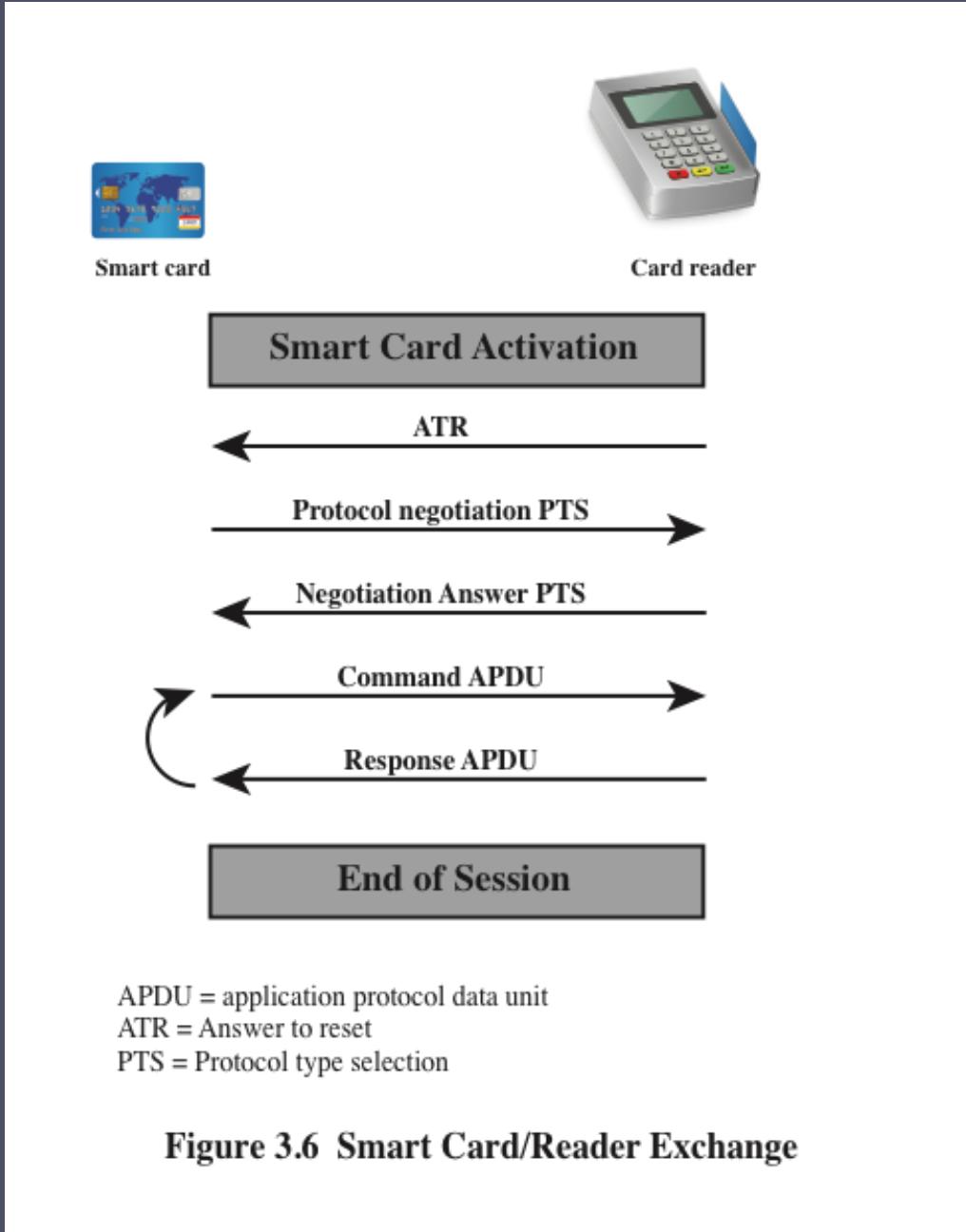
- Can store but do not process data
- The most common is the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
 - Hotel room
 - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
 - Requires a special reader
 - Loss of token
 - User dissatisfaction

Smart Tokens

- **Physical characteristics:**
 - Include an embedded microprocessor
 - A smart token that looks like a bank card
 - Can look like calculators, keys, small portable objects
- **User interface:**
 - Manual interfaces include a keypad and display for human/token interaction
- **Electronic interface**
 - A smart card or other token requires an electronic interface to communicate with a compatible reader/writer
 - Contact and contactless interfaces
- **Authentication protocol:**
 - Classified into three categories:
 - Static
 - Dynamic password generator
 - Challenge-response

Smart Cards

- Most important category of smart token
 - Has the appearance of a credit card
 - Has an electronic interface
 - May use any of the smart token protocols
- Contain:
 - An entire microprocessor
 - Processor
 - Memory
 - I/O ports
- Typically include three types of memory:
 - Read-only memory (ROM)
 - Stores data that does not change during the card's life
 - Electrically erasable programmable ROM (EEPROM)
 - Holds application data and programs
 - Random access memory (RAM)
 - Holds temporary data generated when applications are executed



Electronic Identity Cards (eID)

Use of a smart card as a national identity card for citizens

Can serve the same purposes as other national ID cards, and similar cards such as a driver's license, for access to government and commercial services

Can provide stronger proof of identity and can be used in a wider variety of applications

In effect, is a smart card that has been verified by the national government as valid and authentic

Most advanced deployment is the German card *neuer Personalausweis*

Has human-readable data printed on its surface

- Personal data
- Document number
- Card access number (CAN)
- Machine readable zone (MRZ)

Table 3.4

Electronic Functions and Data for eID Cards

Function	Purpose	PACE Password	Data	Uses
ePass (mandatory)	Authorized offline inspection systems read the data	CAN or MRZ	Face image; two fingerprint images (optional), MRZ data	Offline biometric identity verification reserved for government access
eID (activation optional)	Online applications read the data or access functions as authorized	eID PIN	Family and given names; artistic name and doctoral degree; date and place of birth; address and community ID; expiration date	Identification; age verification; community ID verification; restricted identification (pseudonym); revocation query
	Offline inspection systems read the data and update the address and community ID	CAN or MRZ		
eSign (certificate optional)	A certification authority installs the signature certificate online	eID PIN	Signature key; X.509 certificate	Electronic signature creation
	Citizens make electronic signature with eSign PIN	CAN		

CAN = card access number

MRZ = machine readable zone

PACE = password authenticated connection establishment

PIN = personal identification number

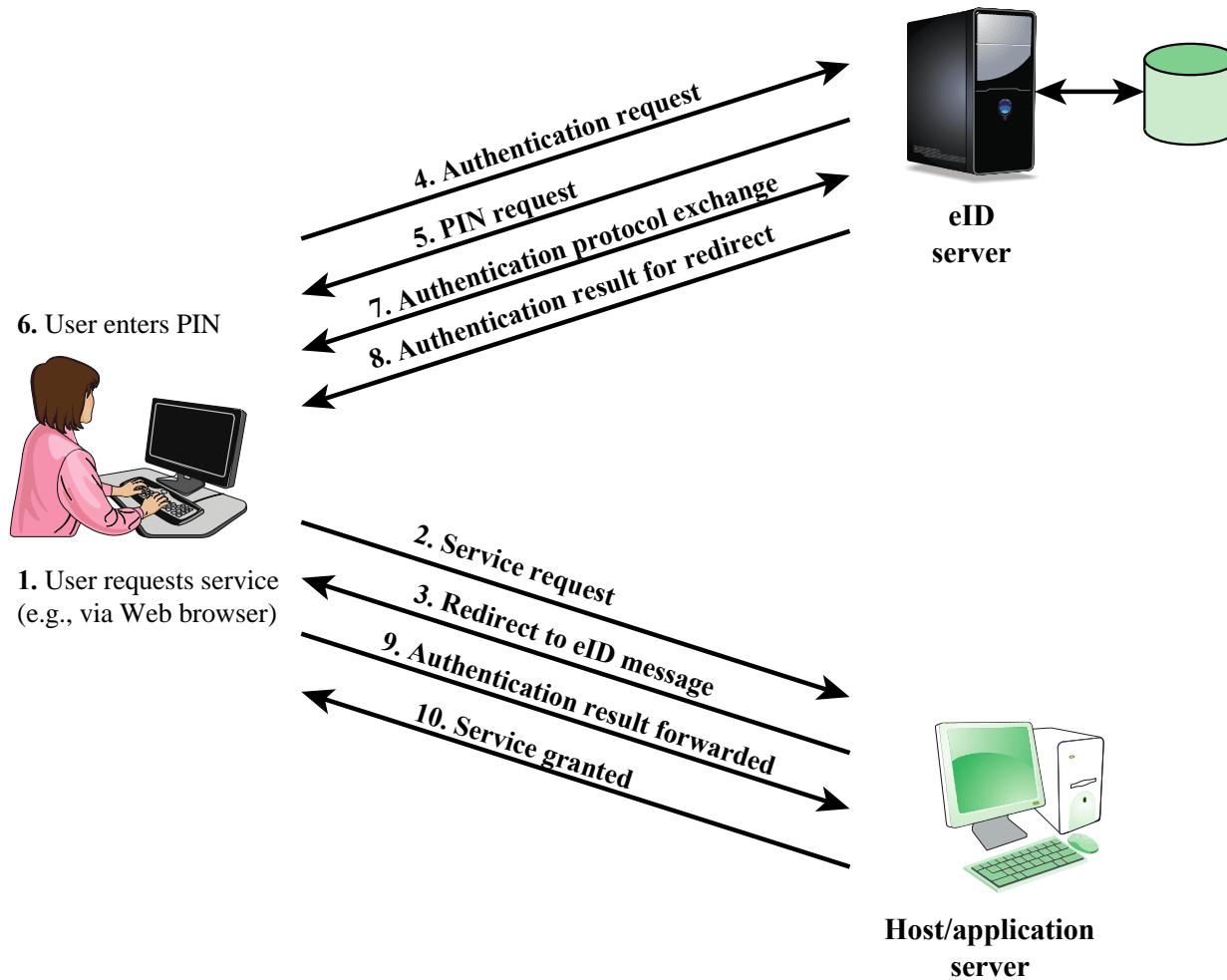


Figure 3.7 User Authentication with eID

Password Authenticated Connection Establishment (PACE)

Ensures that the contactless RF chip in the eID card cannot be read without explicit access control

For online applications, access is established by the user entering the 6-digit PIN (which should only be known to the holder of the card)

For offline applications, either the MRZ printed on the back of the card or the six-digit card access number (CAN) printed on the front is used

Biometric Authentication

- Attempts to authenticate an individual based on unique physical characteristics
- Based on pattern recognition
- Is technically complex and expensive when compared to passwords and tokens
- Physical characteristics used include:
 - Facial characteristics
 - Fingerprints
 - Hand geometry
 - Retinal pattern
 - Iris
 - Signature
 - Voice

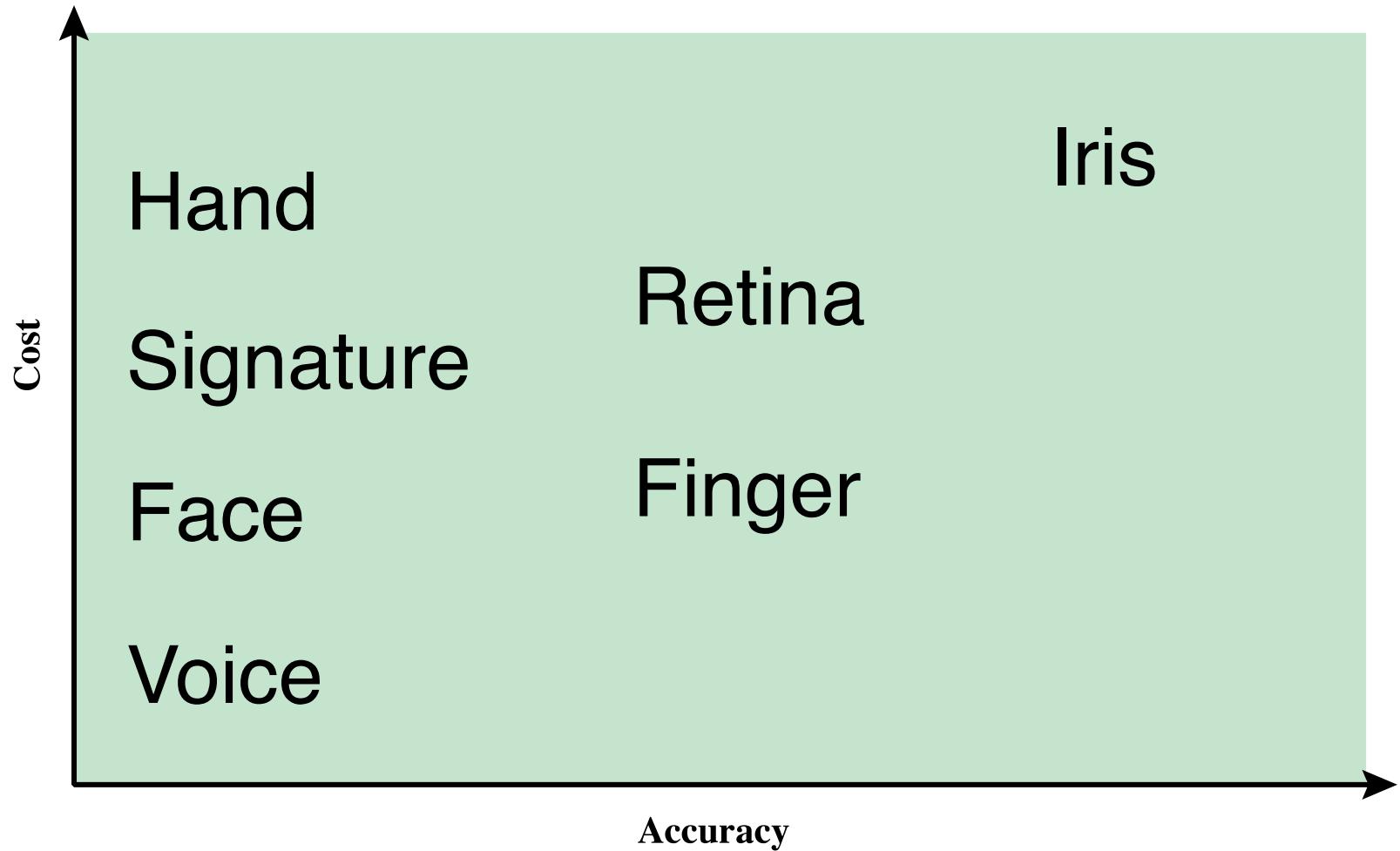
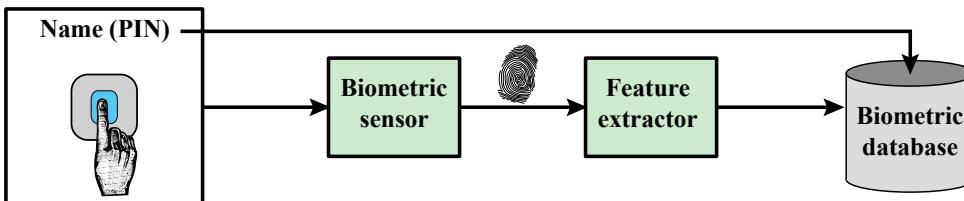
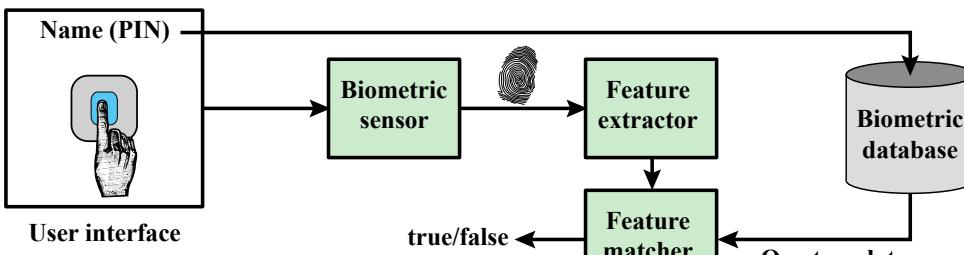


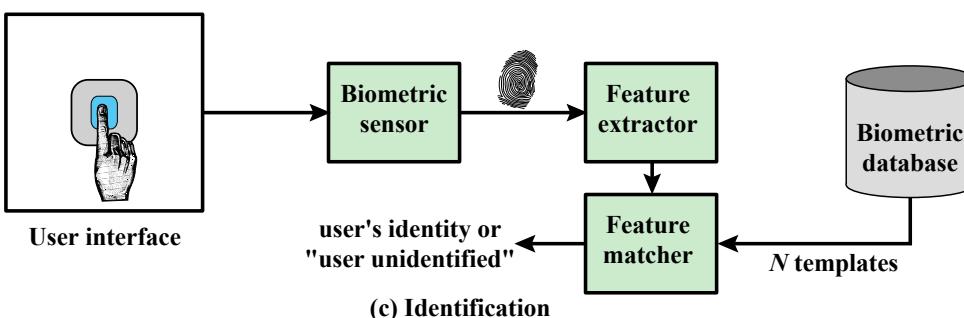
Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.



(a) Enrollment



(b) Verification



(c) Identification

Figure 3.9 A Generic Biometric System. Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

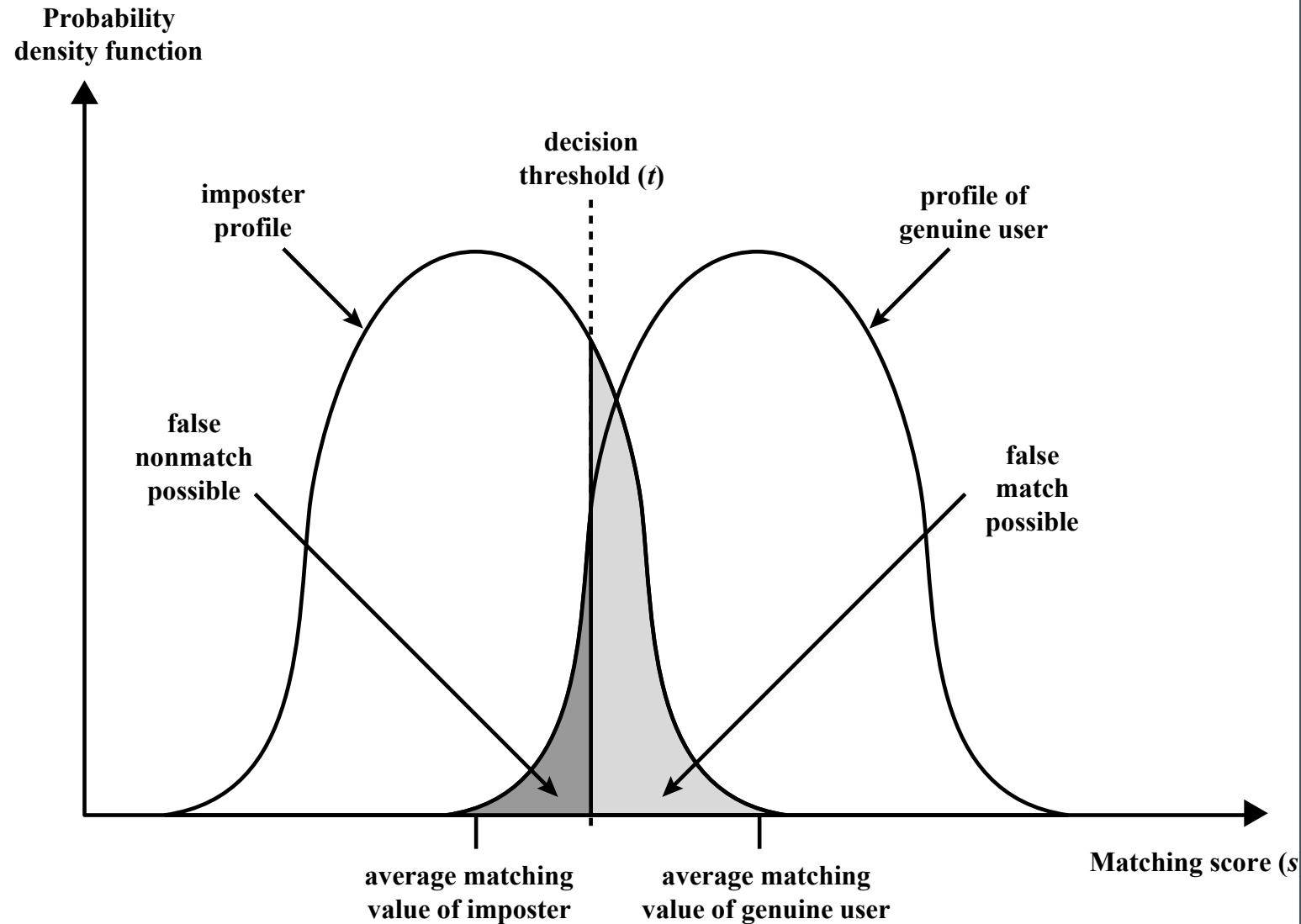


Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

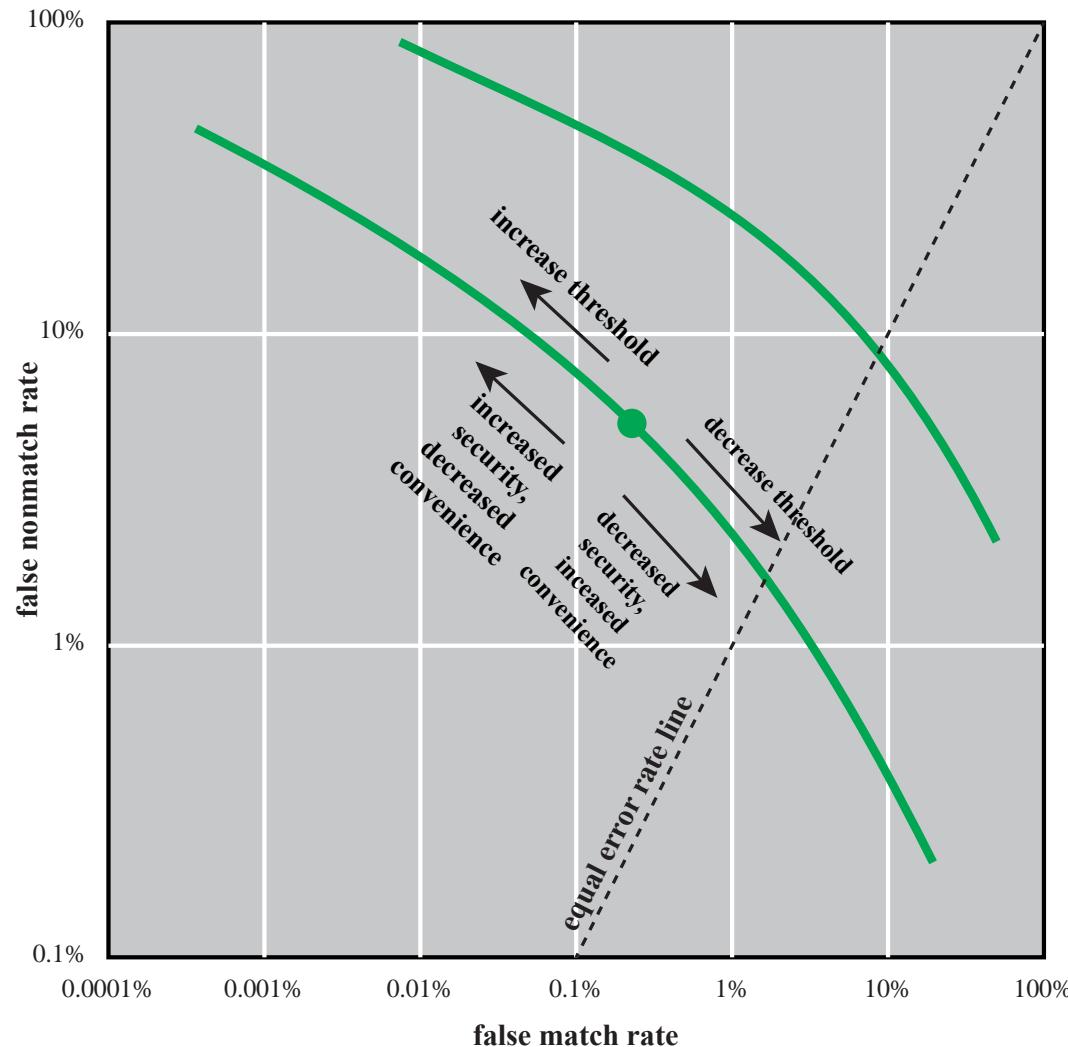


Figure 3.11 Idealized Biometric Measurement Operating Characteristic Curves (log-log scale)

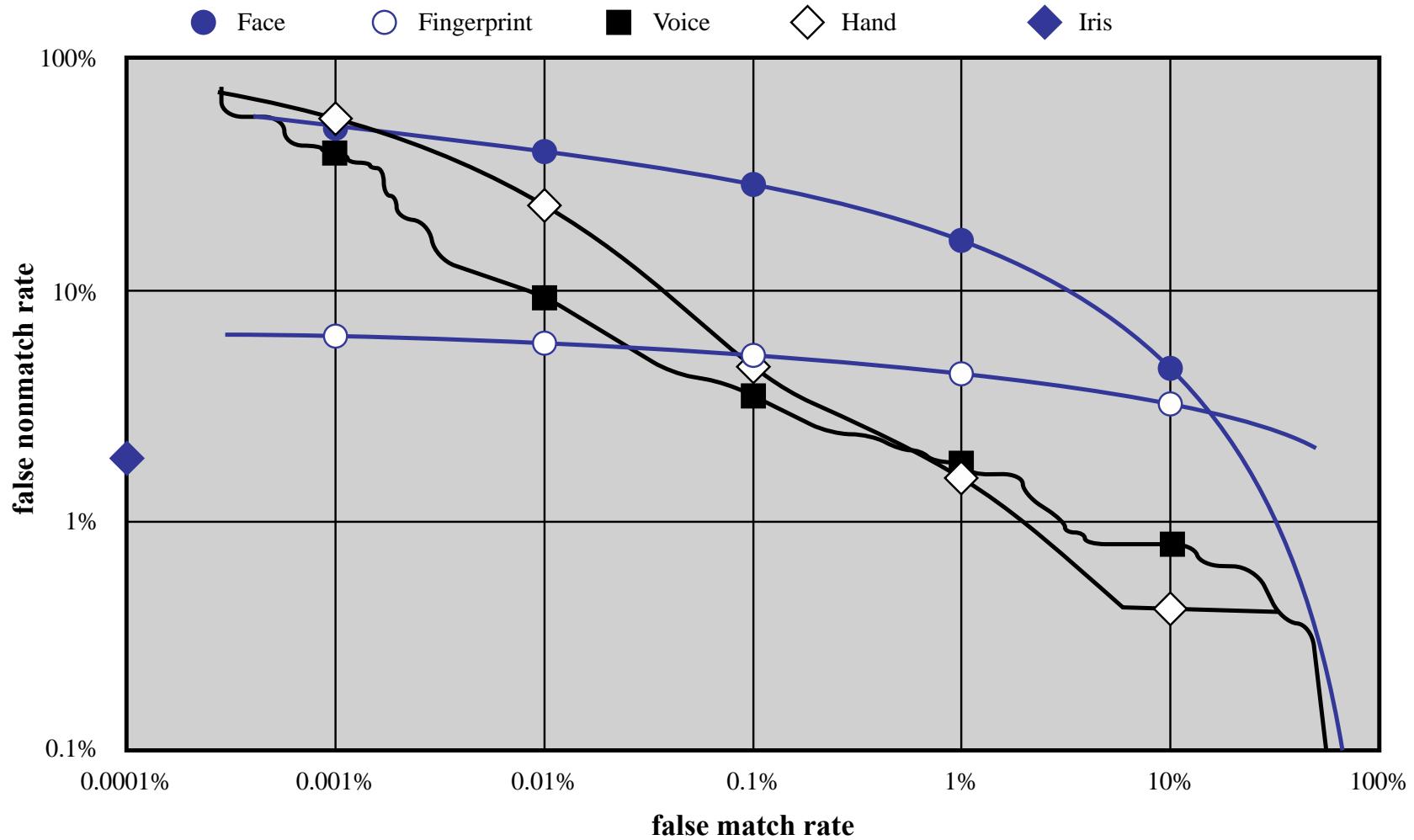


Figure 3.12 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

Remote User Authentication

- Authentication over a network, the Internet, or a communications link is more complex
- Additional security threats such as:
 - Eavesdropping, capturing a password, replaying an authentication sequence that has been observed
- Generally rely on some form of a challenge-response protocol to counter threats

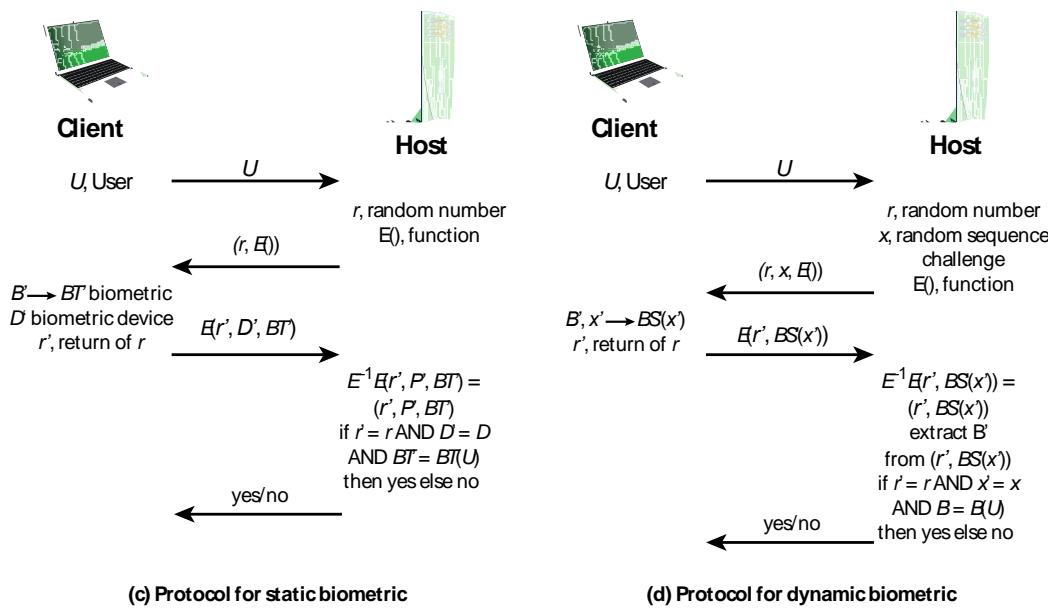
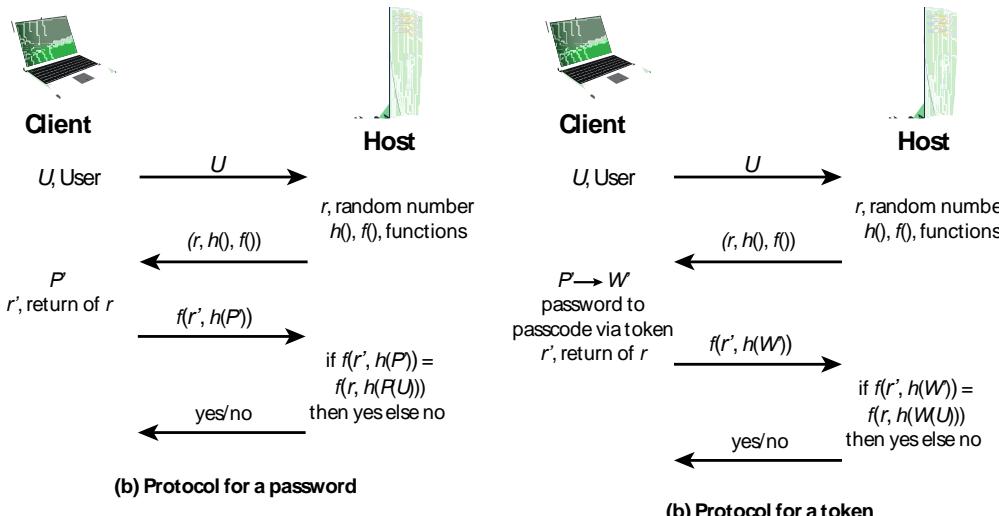


Figure 3.13 Basic Challenge-Response Protocols for Remote User Authentication

Table 3.5

Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

Attacks	Authenticators	Examples	Typical defenses
Client attack	Password	Guessing, exhaustive search	Large entropy; limited attempts
	Token	Exhaustive search	Large entropy; limited attempts, theft of object requires presence
	Biometric	False match	Large entropy; limited attempts
Host attack	Password	Plaintext theft, dictionary/exhaustive search	Hashing; large entropy; protection of password database
	Token	Passcode theft	Same as password; 1-time passcode
	Biometric	Template theft	Capture device authentication; challenge response
Eavesdropping, theft, and copying	Password	"Shoulder surfing"	User diligence to keep secret; administrator diligence to quickly revoke compromised passwords; multifactor authentication
	Token	Theft, counterfeiting hardware	Multifactor authentication; tamper resistant/evident token
	Biometric	Copying (spoofing) biometric	Copy detection at capture device and capture device authentication
Replay	Password	Replay stolen password response	Challenge-response protocol
	Token	Replay stolen passcode response	Challenge-response protocol; 1-time passcode
	Biometric	Replay stolen biometric template response	Copy detection at capture device and capture device authentication via challenge-response protocol
Trojan horse	Password, token, biometric	Installation of rogue client or capture device	Authentication of client or capture device within trusted security perimeter
Denial of service	Password, token, biometric	Lockout by multiple failed authentications	Multifactor with token

(Table is on page 96 in the textbook)

AUTHENTICATION SECURITY ISSUES

Trojan Horse
An application or physical device masquerades as an authentic application or device for the purpose of capturing a user password, passcode, or biometric

Denial-of-Service
Attempts to disable a user authentication service by flooding the service with numerous authentication attempts

Client Attacks
Adversary attempts to achieve user authentication without access to the remote host or the intervening communications path

Eavesdropping
Adversary attempts to learn the password by some sort of attack that involves the physical proximity of user and adversary

Host Attacks
Directed at the user file at the host where passwords, token passcodes, or biometric templates are stored

Replay
Adversary repeats a previously captured user response

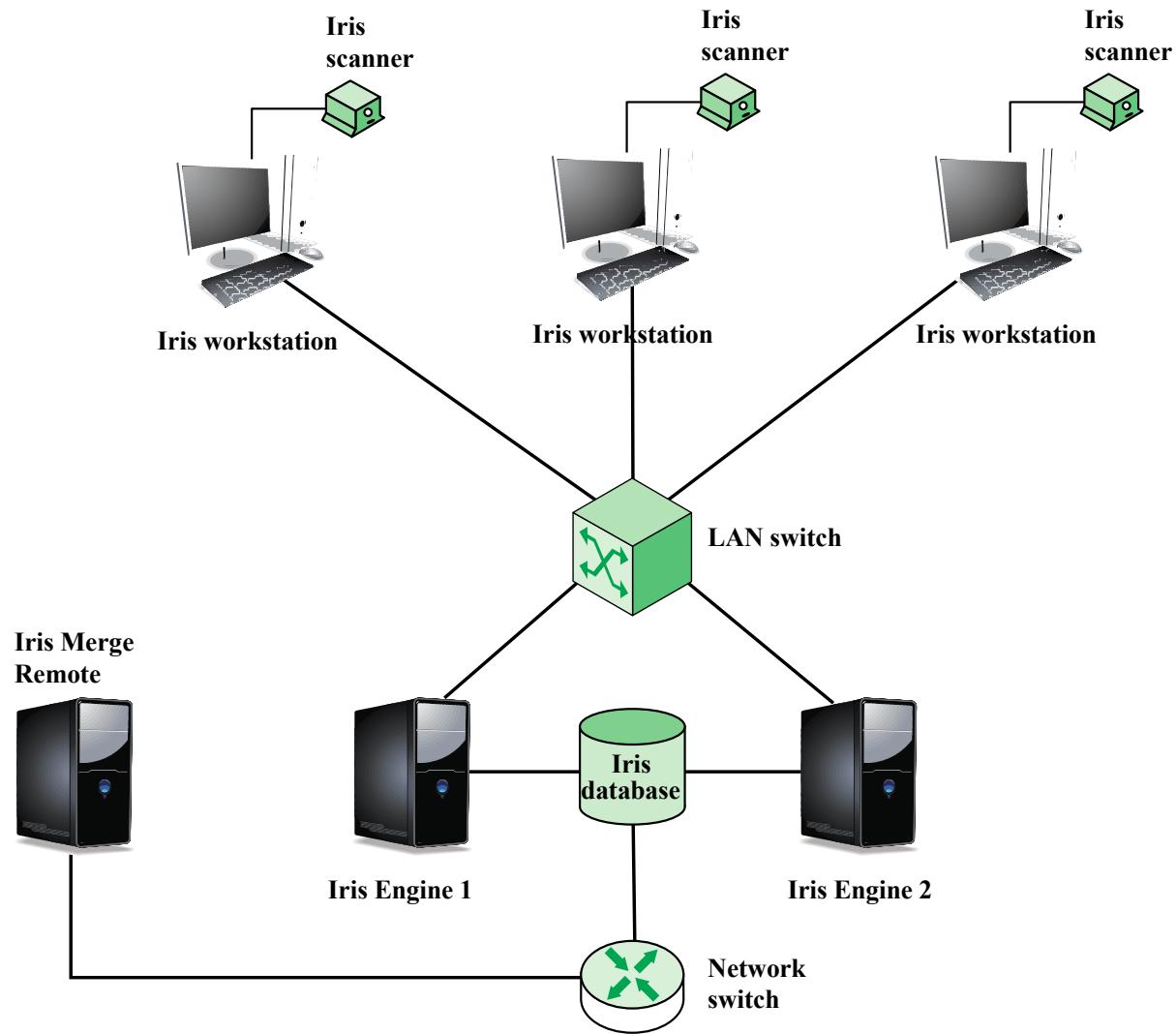


Figure 3.14 General Iris Scan Site Architecture for UAE System

Case Study: ATM Security Problems

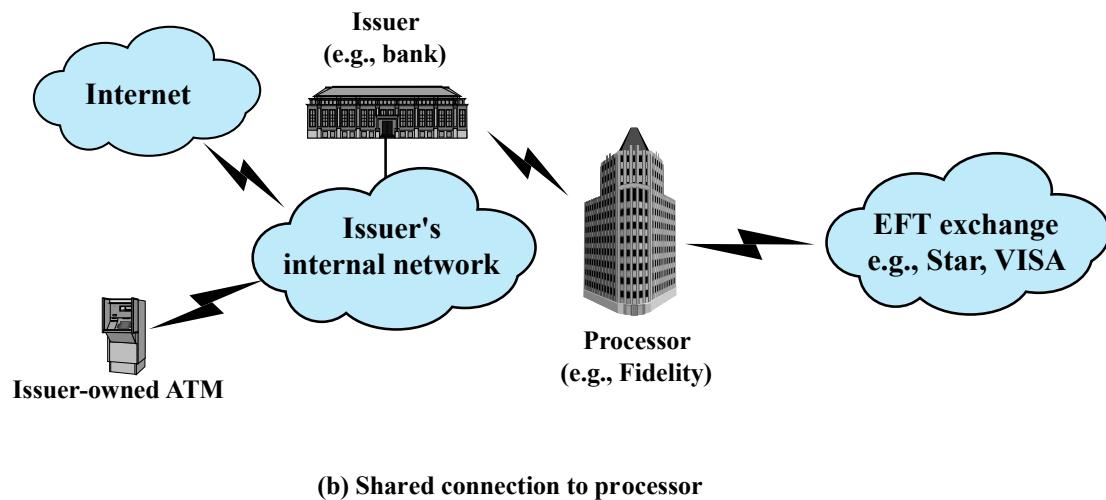
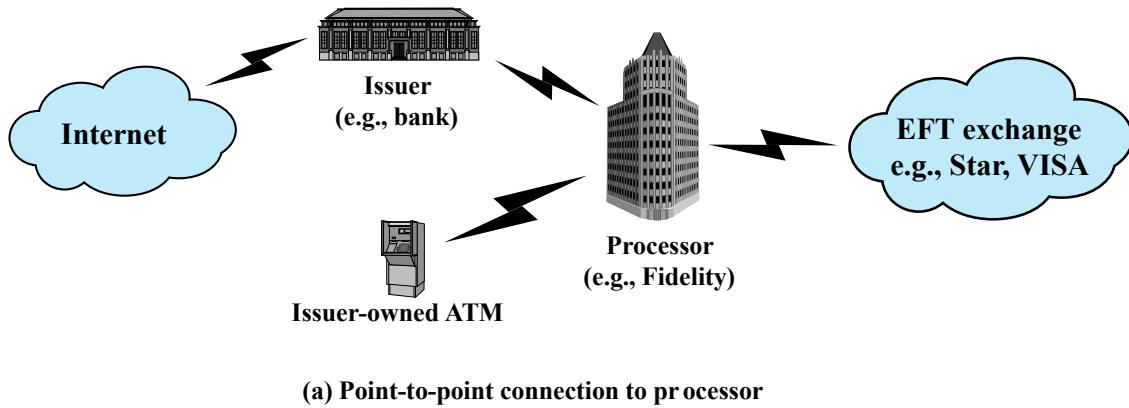


Figure 3.15 ATM Architectures. Most small to mid-sized issuers of debit cards contract processors to provide core data processing and electronic funds transfer (EFT) services. The bank's ATM machine may link directly to the processor or to the bank.

Summary

- Digital user authentication principles
 - A model for digital user authentication
 - Means of authentication
 - Risk assessment for user authentication
- Password-based authentication
 - The vulnerability of passwords
 - The use of hashed passwords
 - Password cracking of user-chosen passwords
 - Password file access control
 - Password selection strategies
- Token-based authentication
 - Memory cards
 - Smart cards
 - Electronic identity cards
- Biometric authentication
 - Physical characteristics used in biometric applications
 - Operation of a biometric authentication system
 - Biometric accuracy
- Remote user authentication
 - Password protocol
 - Token protocol
 - Static biometric protocol
 - Dynamic biometric protocol
- Security issues for user authentication

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 4

Access Control

Access Control Definitions

1/2

NISTIR 7298 defines access control as:

“the process of granting or denying specific requests to: (1) obtain and use information and related information processing services; and (2) enter specific physical facilities”

Access Control Definitions

2/2

RFC 4949 defines access control as:

“a process by which use of system resources is regulated according to a security policy and is permitted only by authorized entities (users, programs, processes, or other systems) according to that policy”

Table 4.1

Access Control Security Requirements (SP 800-171)

Basic Security Requirements	
1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
Derived Security Requirements	
3	Control the flow of CUI in accordance with approved authorizations.
4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
6	Use non-privileged accounts or roles when accessing nonsecurity functions.
7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
8	Limit unsuccessful logon attempts.
9	Provide privacy and security notices consistent with applicable CUI rules.
10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.
11	Terminate (automatically) a user session after a defined condition.
12	Monitor and control remote access sessions.
13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
14	Route remote access via managed access control points.
15	Authorize remote execution of privileged commands and remote access to security-relevant information.
16	Authorize wireless access prior to allowing such connections.
17	Protect wireless access using authentication and encryption.
18	Control connection of mobile devices.
19	Encrypt CUI on mobile devices.
20	Verify and control/limit connections to and use of external information systems.
21	Limit use of organizational portable storage devices on external information systems.
22	Control CUI posted or processed on publicly accessible information systems.

CUI = controlled unclassified information

(Table is on page 107 in the textbook)

Access Control Principles

- In a broad sense, all of computer security is concerned with access control
- RFC 4949 defines computer security as:

“measures that implement and assure security services in a computer system, particularly those that assure access control service”

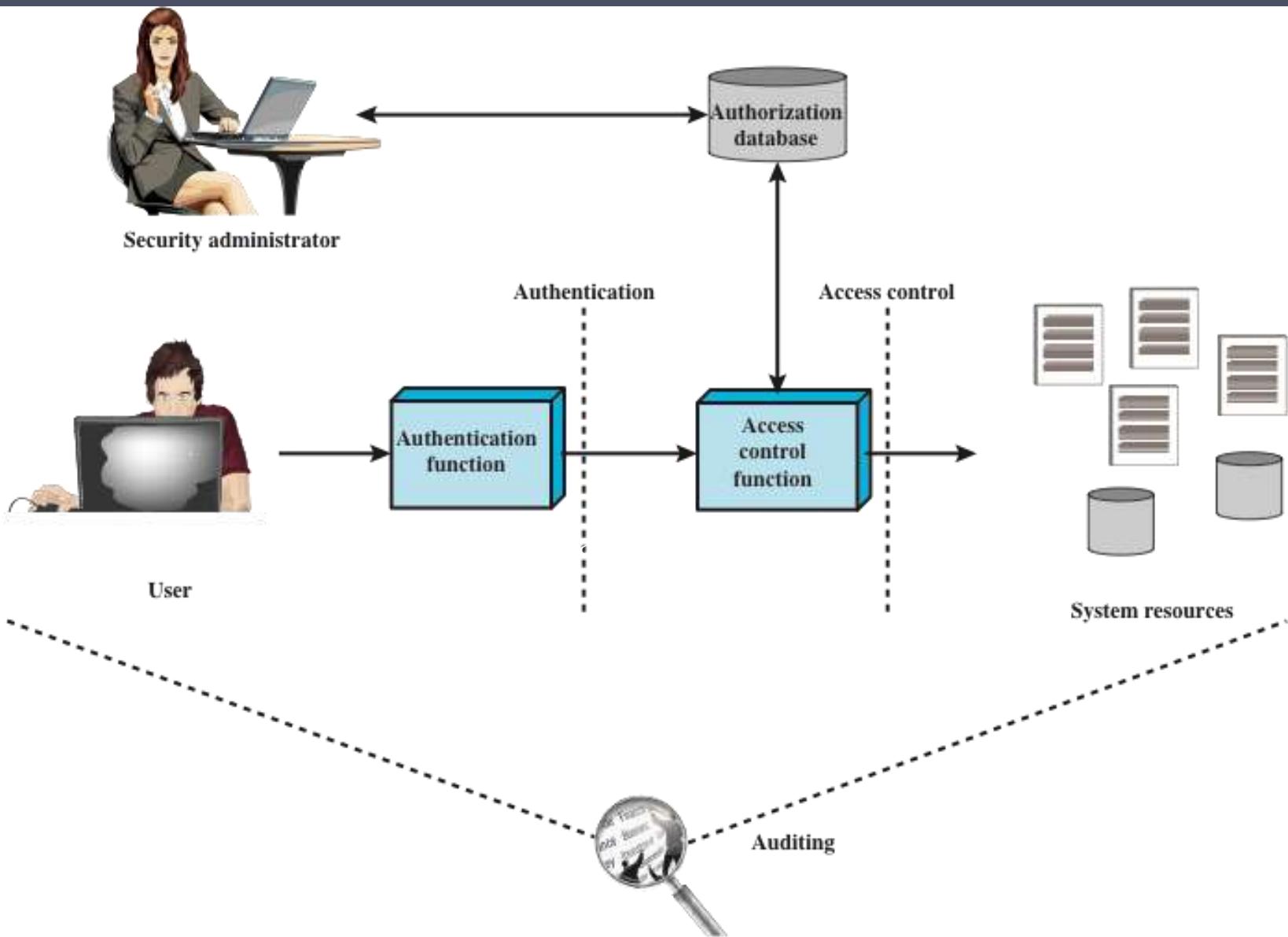


Figure 4.1 Relationship Among Access Control and Other Security Functions

Source: Based on [SAND94].

Access Control Policies

- Discretionary access control (DAC)
 - Controls access based on the identity of the requestor and on access rules (authorizations) stating what requestors are (or are not) allowed to do
- Mandatory access control (MAC)
 - Controls access based on comparing security labels with security clearances
- Role-based access control (RBAC)
 - Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles
- Attribute-based access control (ABAC)
 - Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

Subjects, Objects, and Access Rights

Subject

An entity capable of accessing objects

Three classes

- Owner
- Group
- World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

Could include:

- Read
- Write
- Execute
- Delete
- Create
- Search

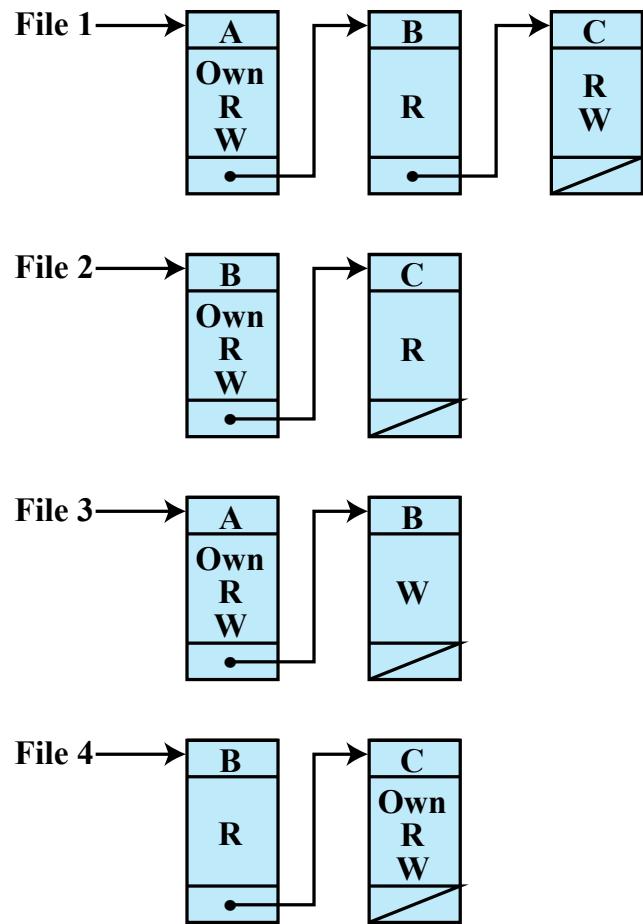
Discretionary Access Control (DAC)

- Scheme in which an entity may be granted access rights that permit the entity, by its own violation, to enable another entity to access some resource
- Often provided using an access matrix
 - One dimension consists of identified subjects that may attempt data access to the resources
 - The other dimension lists the objects that may be accessed
- Each entry in the matrix indicates the access rights of a particular subject for a particular object

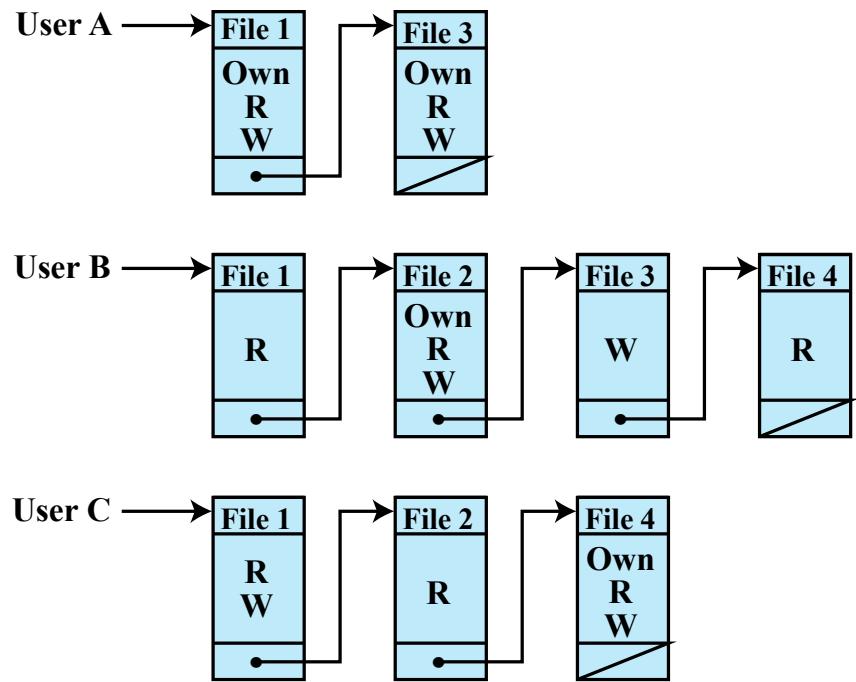
		OBJECTS				
		File 1	File 2	File 3	File 4	
SUBJECTS		User A	Own Read Write		Own Read Write	
		User B	Read	Own Read Write	Write	Read
		User C	Read Write	Read		Own Read Write

(a) Access matrix

Figure 4.2 Example of Access Control Structures



(b) Access control lists for files of part (a)



(c) Capability lists for files of part (a)

Figure 4.2 Example of Access Control Structures

Table 4.2
 Authorization
 Table
 for Files in
 Figure 4.2

Subject	Access Mode	Object
A	Own	File 1
A	Read	File 1
A	Write	File 1
A	Own	File 3
A	Read	File 3
A	Write	File 3
B	Read	File 1
B	Own	File 2
B	Read	File 2
B	Write	File 2
B	Write	File 3
B	Read	File 4
C	Read	File 1
C	Write	File 1
C	Read	File 2
C	Own	File 4
C	Read	File 4
C	Write	File 4

(Table is on page 113 in the textbook)

OBJECTS

		subjects			files		processes		disk drives	
		S ₁	S ₂	S ₃	F ₁	F ₂	P ₁	P ₂	D ₁	D ₂
SUBJECTS	S ₁	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
	S ₂		control		write *	execute			owner	seek *
	S ₃			control		write	stop			

* - copy flag set

Figure 4.3 Extended Access Control Matrix

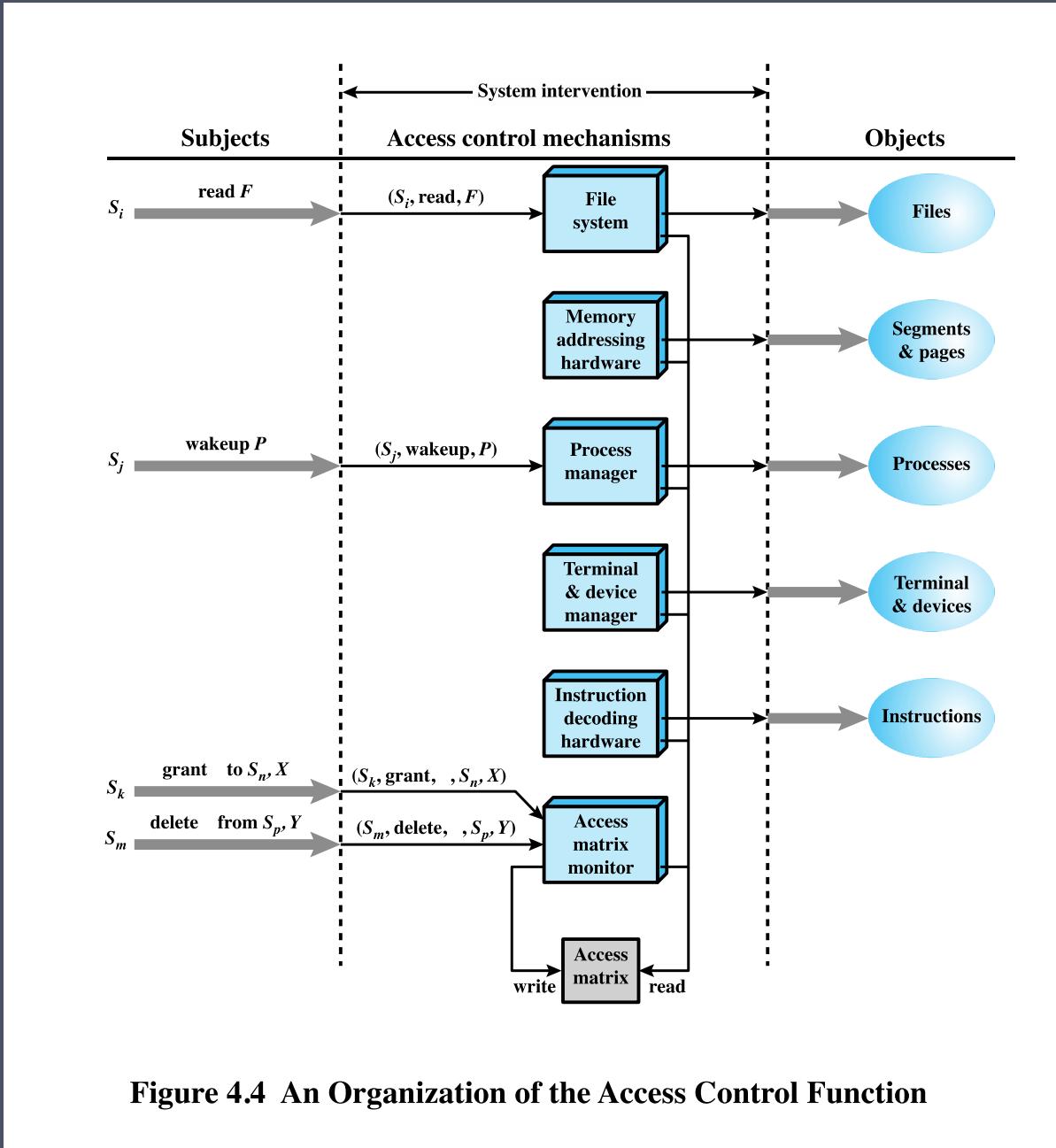


Figure 4.4 An Organization of the Access Control Function

Table 4.3

Access Control System Commands

Rule	Command (by S_o)	Authorization	Operation
R1	transfer $\begin{Bmatrix} a^* \\ a \end{Bmatrix}$ to S, X	' a^* ' in $A[S_o, X]$	store $\begin{Bmatrix} a^* \\ a \end{Bmatrix}$ in $A[S, X]$
R2	grant $\begin{Bmatrix} a^* \\ a \end{Bmatrix}$ to S, X	'owner' in $A[S_o, X]$	store $\begin{Bmatrix} a^* \\ a \end{Bmatrix}$ in $A[S, X]$
R3	delete a from S, X	'control' in $A[S_o, S]$ or 'owner' in $A[S_o, X]$	delete a from $A[S, X]$
R4	$w \leftarrow \mathbf{read} S, X$	'control' in $A[S_o, S]$ or 'owner' in $A[S_o, X]$	copy $A[S, X]$ into w
R5	create object X	None	add column for X to A ; store 'owner' in $A[S_o, X]$
R6	destroy object X	'owner' in $A[S_o, X]$	delete column for X from A
R7	create subject S	none	add row for S to A ; execute create object S ; store 'control' in $A[S, S]$
R8	destroy subject S	'owner' in $A[S_o, S]$	delete row for S from A ; execute destroy object S

(Table is on page 116 in the textbook)

Protection Domains

- Set of objects together with access rights to those objects
- More flexibility when associating capabilities with protection domains
- In terms of the access matrix, a row defines a protection domain
- User can spawn processes with a subset of the access rights of the user
- Association between a process and a domain can be static or dynamic
- In user mode certain areas of memory are protected from use and certain instructions may not be executed
- In kernel mode privileged instructions may be executed and protected areas of memory may be accessed

UNIX File Access Control

UNIX files are administered using inodes (index nodes)

- Control structures with key information needed for a particular file
- Several file names may be associated with a single inode
- An active inode is associated with exactly one file
- File attributes, permissions and control information are sorted in the inode
- On the disk there is an inode table, or inode list, that contains the inodes of all the files in the file system
- When a file is opened its inode is brought into main memory and stored in a memory resident inode table

Directories are structured in a hierarchical tree

- May contain files and/or other directories
- Contains file names plus pointers to associated inodes

UNIX

File Access Control

- Unique user identification number (user ID)
- Member of a primary group identified by a group ID
- Belongs to a specific group
- 12 protection bits
 - Specify read, write, and execute permission for the owner of the file, members of the group and all other users
- The owner ID, group ID, and protection bits are part of the file's inode

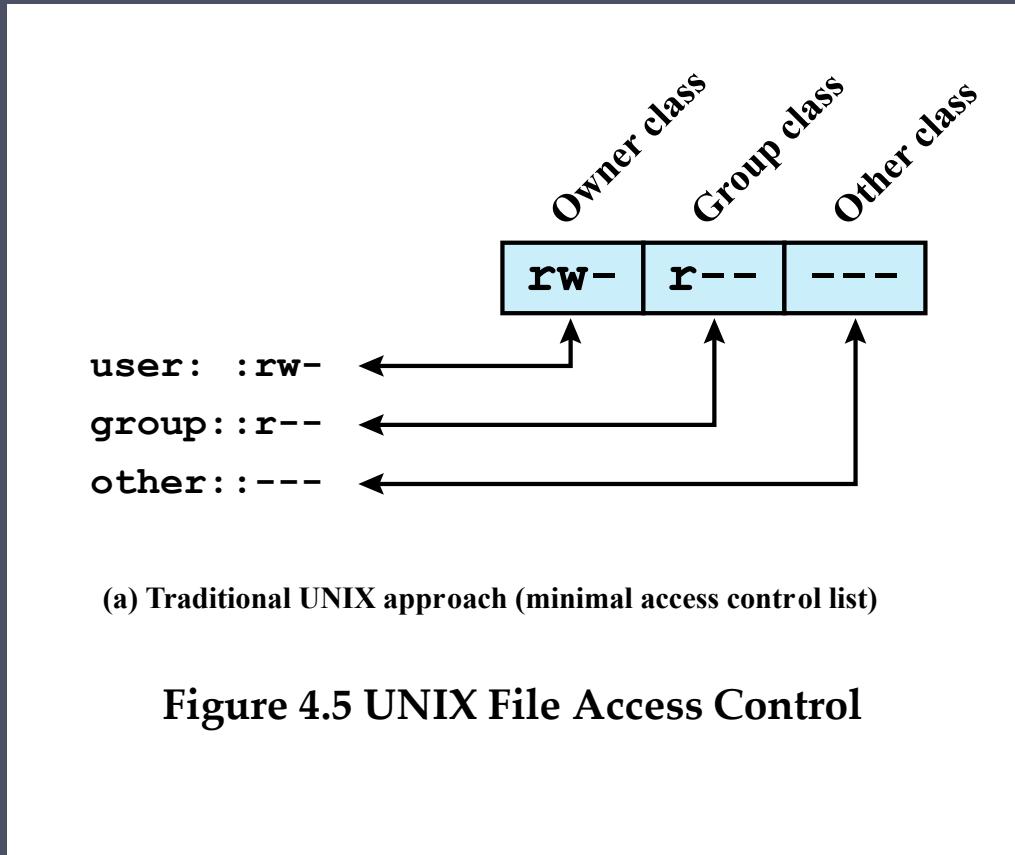


Figure 4.5 UNIX File Access Control

Traditional UNIX File Access Control

- “Set user ID”(SetUID)
- “Set group ID”(SetGID)
 - System temporarily uses rights of the file owner/group in addition to the real user’s rights when making access control decisions
 - Enables privileged programs to access files/resources not generally accessible
- Sticky bit
 - When applied to a directory it specifies that only the owner of any file in the directory can rename, move, or delete that file
- Superuser
 - Is exempt from usual access control restrictions
 - Has system-wide access

Access Control Lists (ACLs) in UNIX

Modern UNIX systems support ACLs

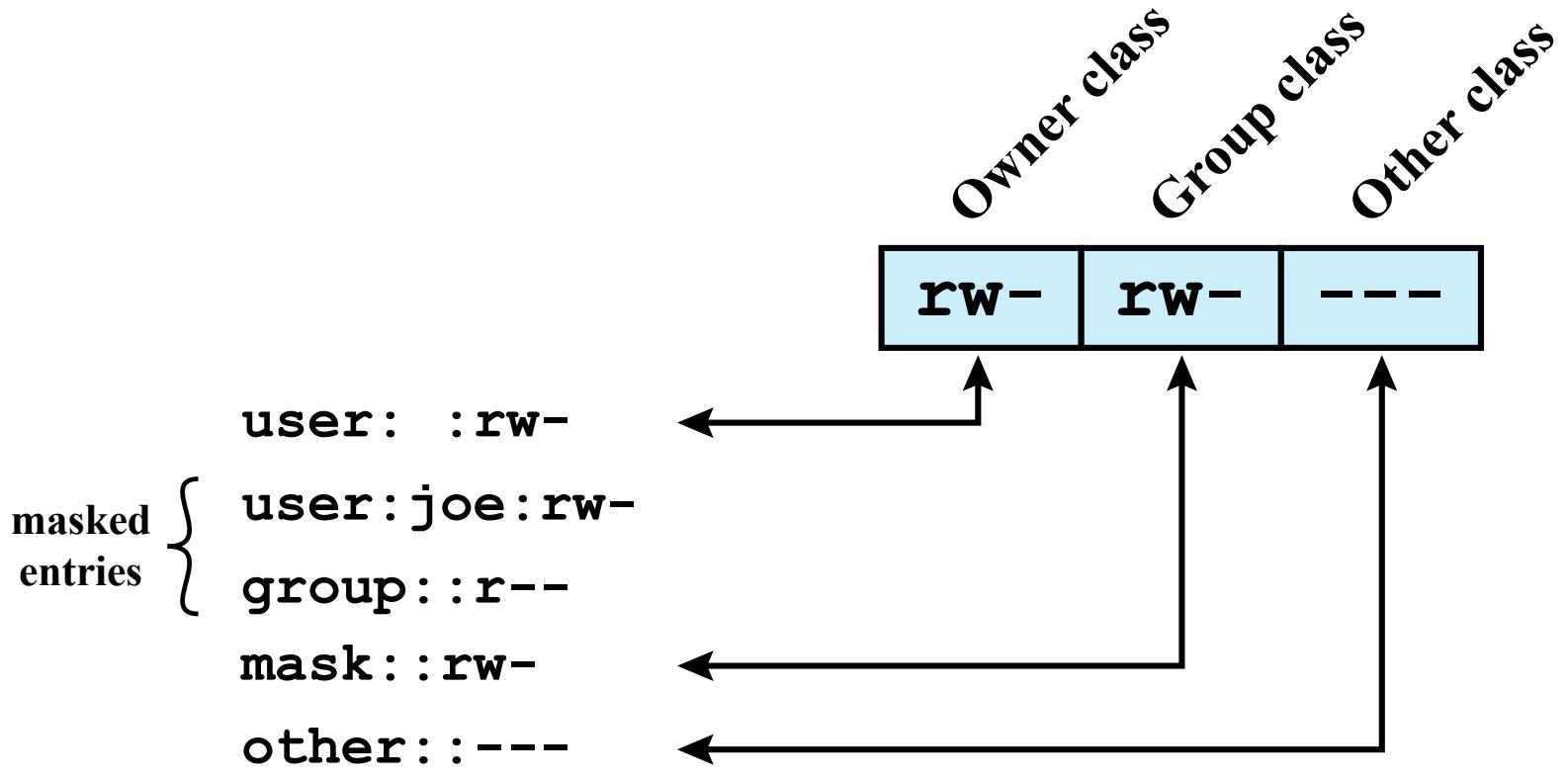
- FreeBSD, OpenBSD, Linux, Solaris

FreeBSD

- Setfacl command assigns a list of UNIX user IDs and groups
- Any number of users and groups can be associated with a file
- Read, write, execute protection bits
- A file does not need to have an ACL
- Includes an additional protection bit that indicates whether the file has an extended ACL

When a process requests access to a file system object two steps are performed:

- Step 1 selects the most appropriate ACL
- Step 2 checks if the matching entry contains sufficient permissions



(b) Extended access control list

Figure 4.5 UNIX File Access Control

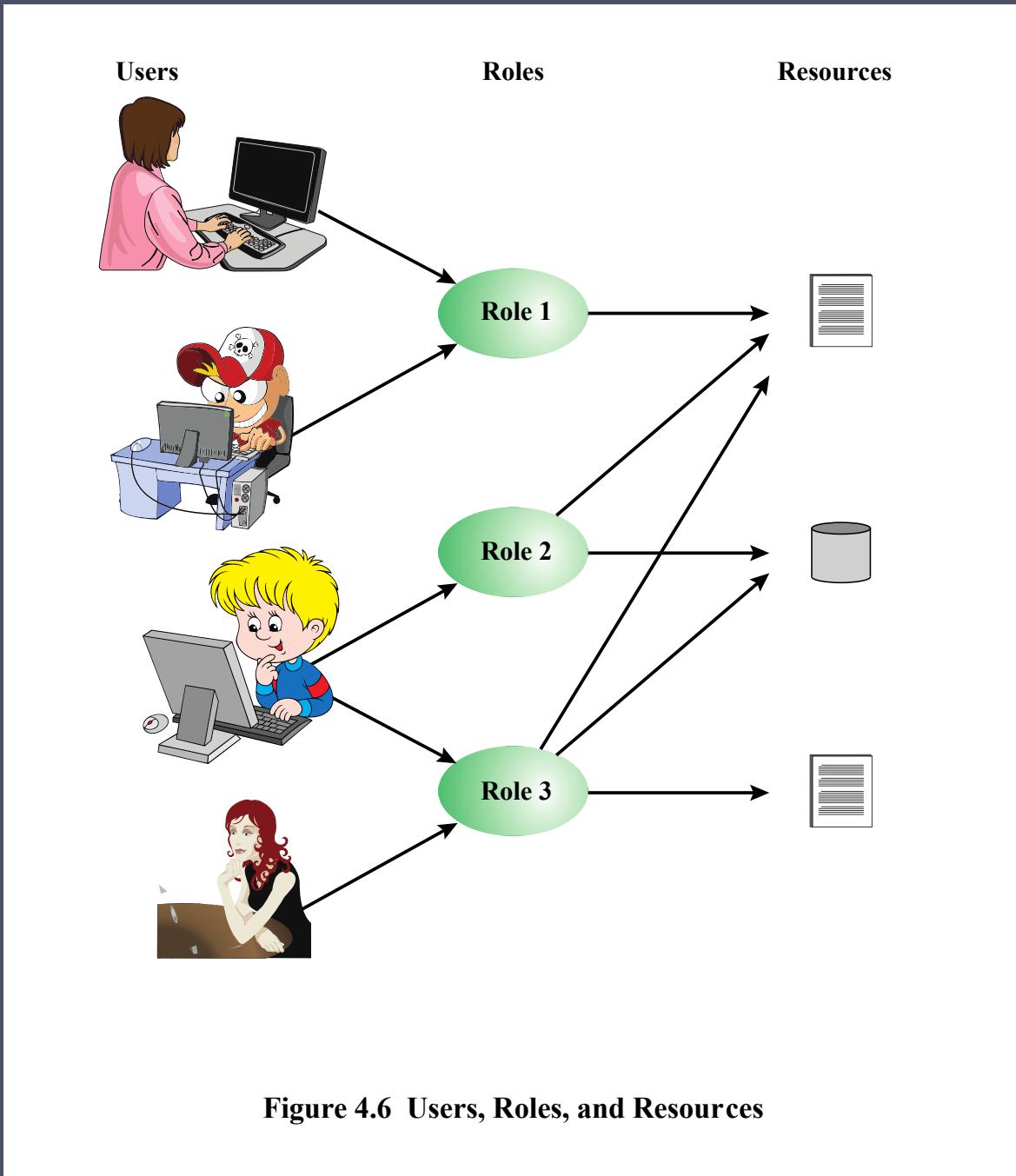
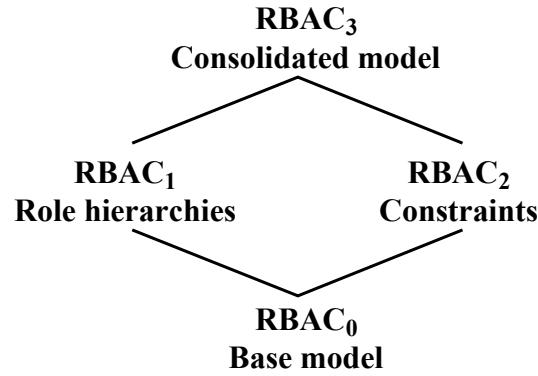


Figure 4.6 Users, Roles, and Resources

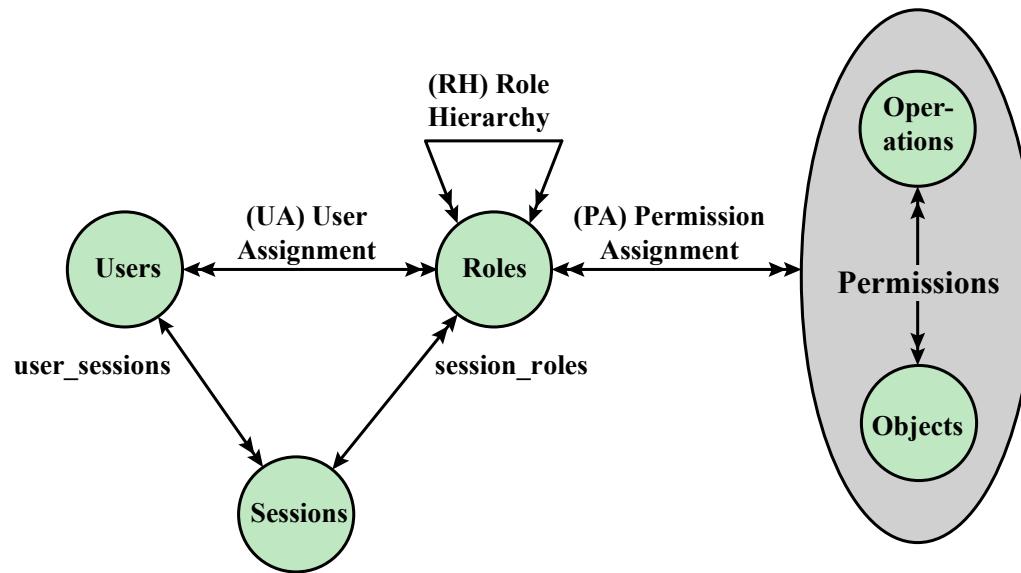
	R ₁	R ₂	• • •	R _n
U ₁	X			
U ₂	X			
U ₃		X		X
U ₄				X
U ₅				X
U ₆				X
•				
•				
•				
U _m	X			

OBJECTS									
	R ₁	R ₂	R _n	F ₁	F ₁	P ₁	P ₂	D ₁	D ₂
R ₁	control	owner	owner control	read *	read owner	wakeup	wakeup	seek	owner
R ₂		control		write *	execute			owner	seek *
•									
•									
•									
R _n			control		write	stop			

Figure 4.7 Access Control Matrix Representation of RBAC



(a) Relationship among RBAC models



(b) RBAC models

Figure 4.8 A Family of Role-Based Access Control Models.

Table 4.4

Scope RBAC Models

Models	Hierarchies	Constraints
RBAC ₀	No	No
RBAC ₁	Yes	No
RBAC ₂	No	Yes
RBAC ₃	Yes	Yes

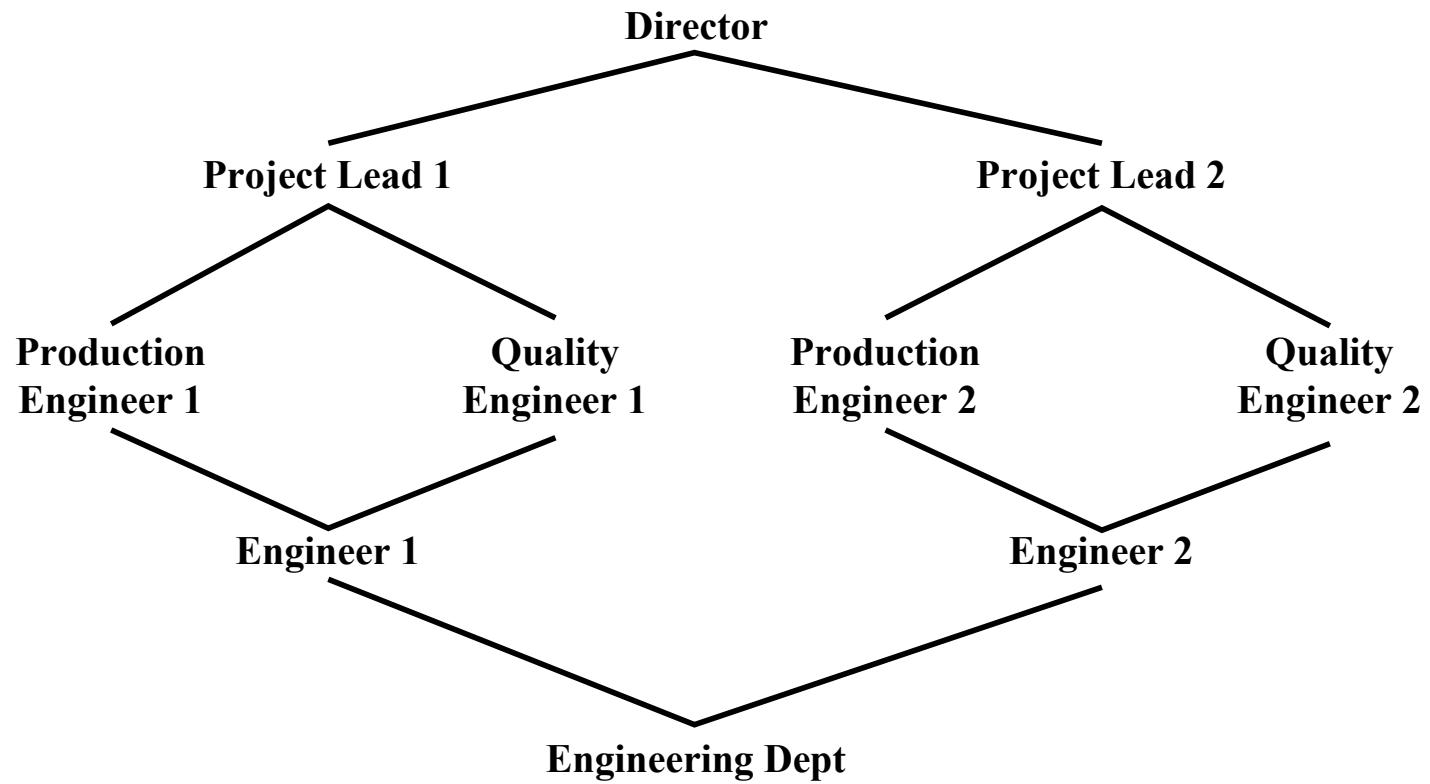


Figure 4.9 Example of Role Hierarchy

Constraints - RBAC

- Provide a means of adapting RBAC to the specifics of administrative and security policies of an organization
- A defined relationship among roles or a condition related to roles
- Types:

Mutually exclusive roles	Cardinality	Prerequisite roles
<ul style="list-style-type: none">• A user can only be assigned to one role in the set (either during a session or statically)• Any permission (access right) can be granted to only one role in the set	<ul style="list-style-type: none">• Setting a maximum number with respect to roles	<ul style="list-style-type: none">• Dictates that a user can only be assigned to a particular role if it is already assigned to some other specified role

Attribute-Based Access Control (ABAC)

Can define authorizations that express conditions on properties of both the resource and the subject

Strength is its flexibility and expressive power

Main obstacle to its adoption in real systems has been concern about the performance impact of evaluating predicates on both resource and user properties for each access

Web services have been pioneering technologies through the introduction of the eXtensible Access Control Markup Language (XAMCL)

There is considerable interest in applying the model to cloud services

ABAC Model: Attributes

Subject attributes

- A subject is an active entity that causes information to flow among objects or changes the system state
- Attributes define the identity and characteristics of the subject

Object attributes

- An object (or resource) is a passive information system-related entity containing or receiving information
- Objects have attributes that can be leverages to make access control decisions

Environment attributes

- Describe the operational, technical, and even situational environment or context in which the information access occurs
- These attributes have so far been largely ignored in most access control policies

ABAC

Distinguishable because it controls access to objects by evaluating rules against the attributes of entities, operations, and the environment relevant to a request

Relyes upon the evaluation of attributes of the subject, attributes of the object, and a formal relationship or access control rule defining the allowable operations for subject-object attribute combinations in a given environment

Systems are capable of enforcing DAC, RBAC, and MAC concepts

Allows an unlimited number of attributes to be combined to satisfy any access control rule

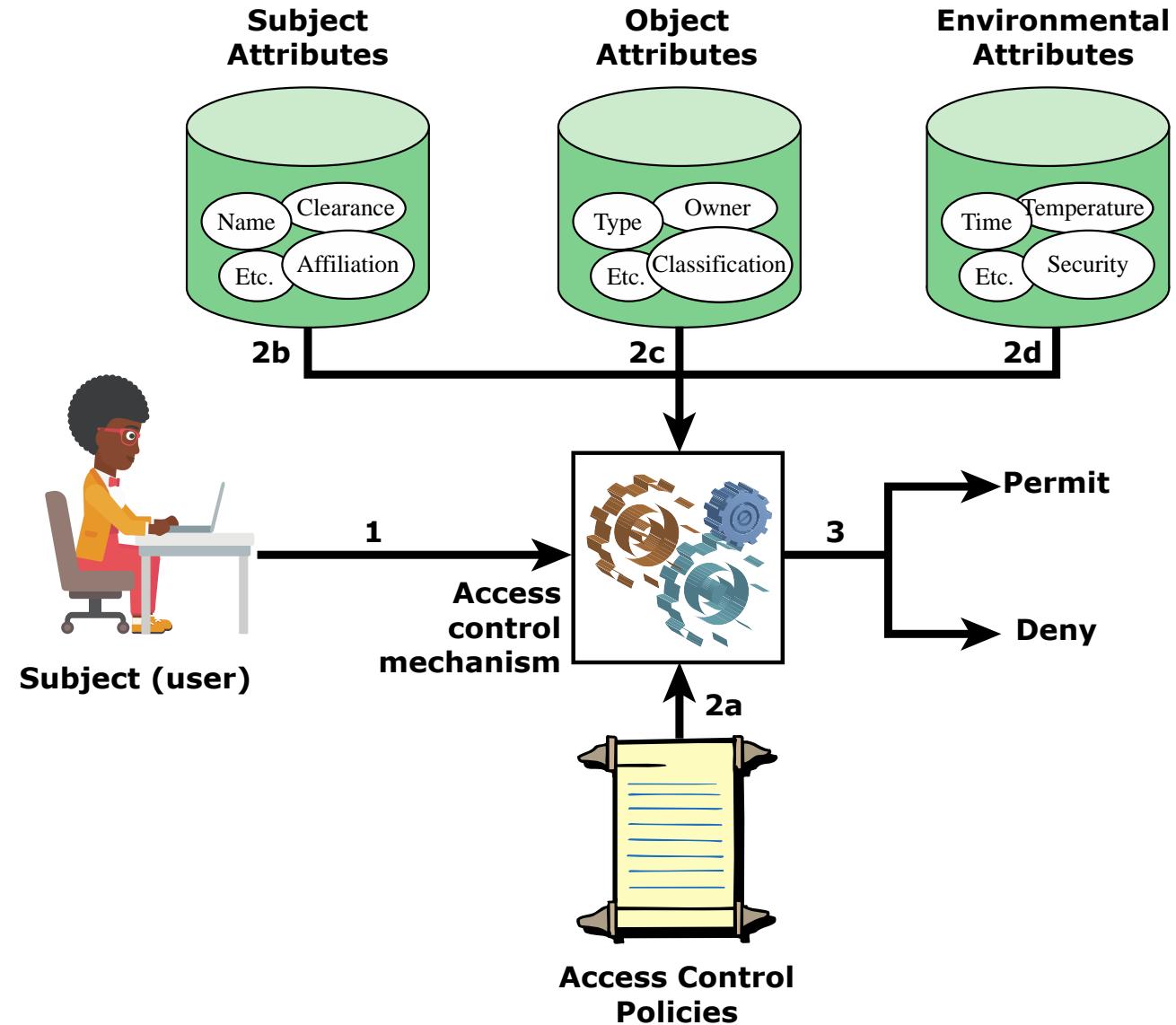
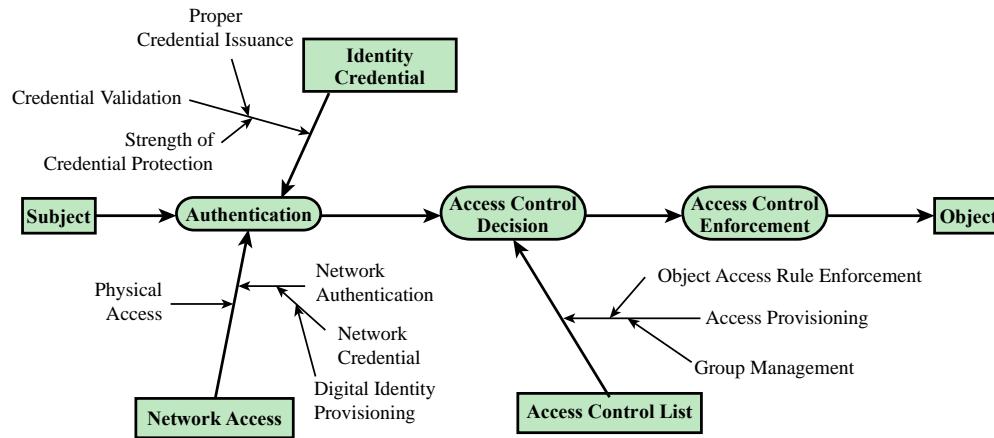
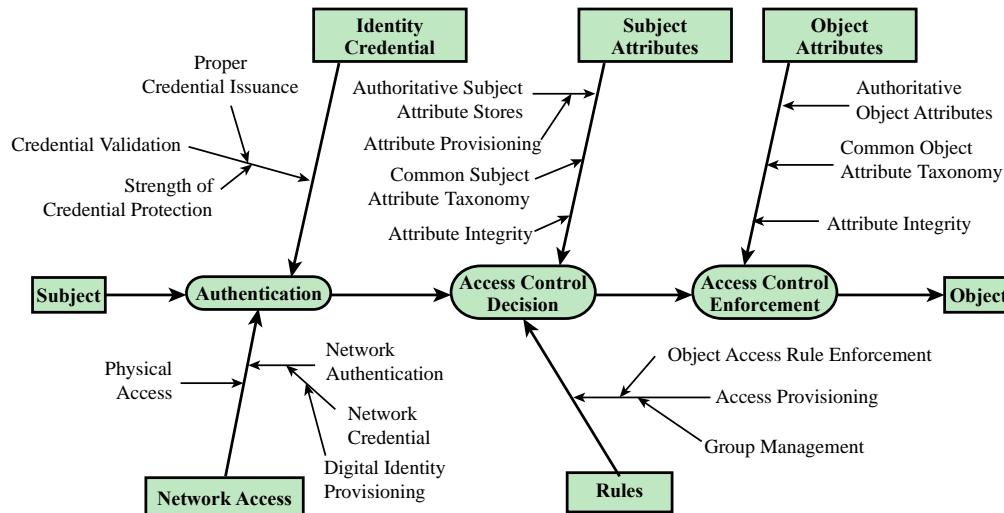


Figure 4.10 ABAC Scenario



(a) ACL Trust Chain



(b) ABAC Trust Chain

Figure 4.11 ACL and ABAC Trust Relationships

ABAC Policies

A policy is a set of rules and relationships that govern allowable behavior within an organization, based on the privileges of subjects and how resources or objects are to be protected under which environment conditions

Typically written from the perspective of the object that needs protecting and the privileges available to subjects

Privileges represent the authorized behavior of a subject and are defined by an authority and embodied in a policy

Other terms commonly used instead of privileges are: rights, authorizations, and entitlements

Identity, Credential, and Access Management (ICAM)

- A comprehensive approach to managing and implementing digital identities, credentials, and access control
- Developed by the U.S. government
- Designed to:
 - Create trusted digital identity representations of individuals and nonperson entities (NPEs)
 - Bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions
 - A credential is an object or data structure that authoritatively binds an identity to a token possessed and controlled by a subscriber
 - Use the credentials to provide authorized access to an agency's resources

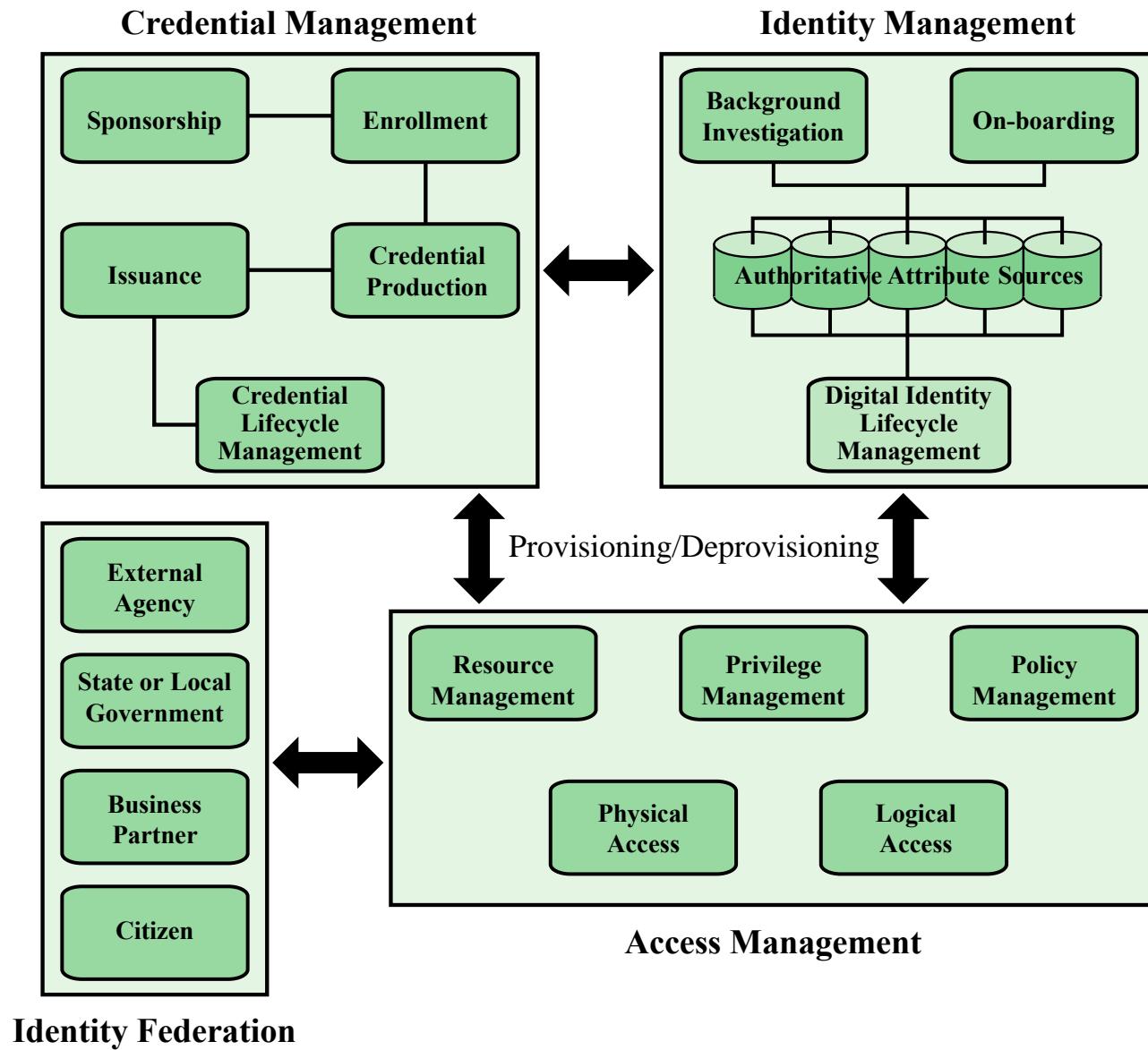
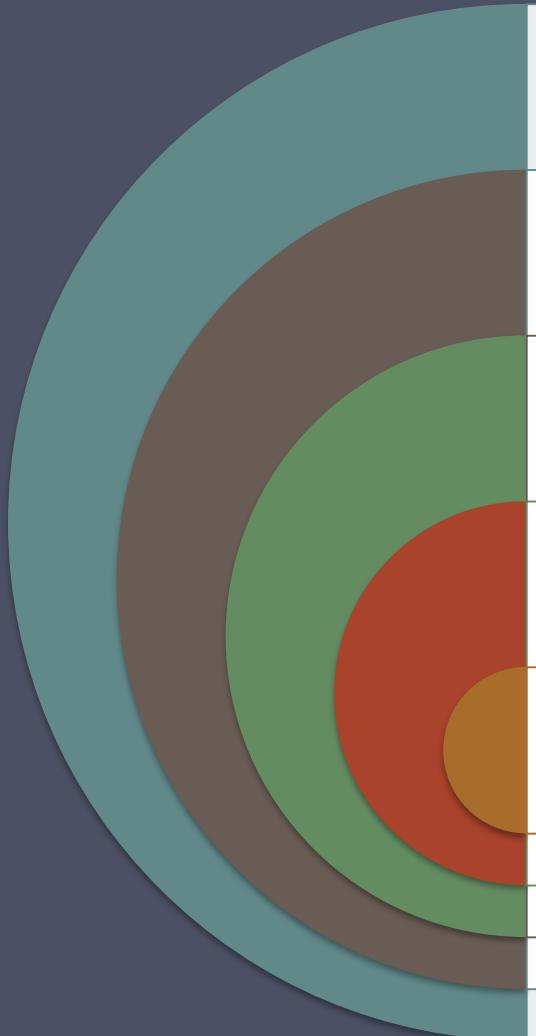


Figure 4.12 Identity, Credential, and Access Management (ICAM)

Identity Management



	<p>Concerned with assigning attributes to a digital identity and connecting that digital identity to an individual or NPE</p>
	<p>Goal is to establish a trustworthy digital identity that is independent of a specific application or context</p>
	<p>Most common approach to access control for applications and programs is to create a digital representation of an identity for the specific use of the application or program</p>
	<p>Maintenance and protection of the identity itself is treated as secondary to the mission associated with the application</p>
	<p>Final element is lifecycle management which includes:</p> <ul style="list-style-type: none">• Mechanisms, policies, and procedures for protecting personal identity information• Controlling access to identity data• Techniques for sharing authoritative identity data with applications that need it• Revocation of an enterprise identity

Credential Management

The management of the life cycle of the credential

Examples of credentials are smart cards, private/public cryptographic keys, and digital certificates

Encompasses five logical components:

An authorized individual sponsors an individual or entity for a credential to establish the need for the credential

The sponsored individual enrolls for the credential

- Process typically consists of identity proofing and the capture of biographic and biometric data
- This step may also involve incorporating authoritative attribute data, maintained by the identity management component

A credential is produced

- Depending on the credential type, production may involve encryption, the use of a digital signature, the production of a smart card or other functions

The credential is issued to the individual or NPE

A credential must be maintained over its life cycle

- Might include revocation, reissuance/replacement, reenrollment, expiration, personal identification number (PIN) reset, suspension, or reinstatement

Access Management

Deals with the management and control of the ways entities are granted access to resources

Covers both logical and physical access

May be internal to a system or an external element

Purpose is to ensure that the proper identity verification is made when an individual attempts to access a security sensitive building, computer systems, or data

Three support elements are needed for an enterprise-wide access control facility:

- Resource management
- Privilege management
- Policy management

Three support elements are needed for an enterprise-wide access control facility:

Resource management

- Concerned with defining rules for a resource that requires access control
- Rules would include credential requirements and what user attributes, resource attributes, and environmental conditions are required for access of a given resource for a given function

Privilege management

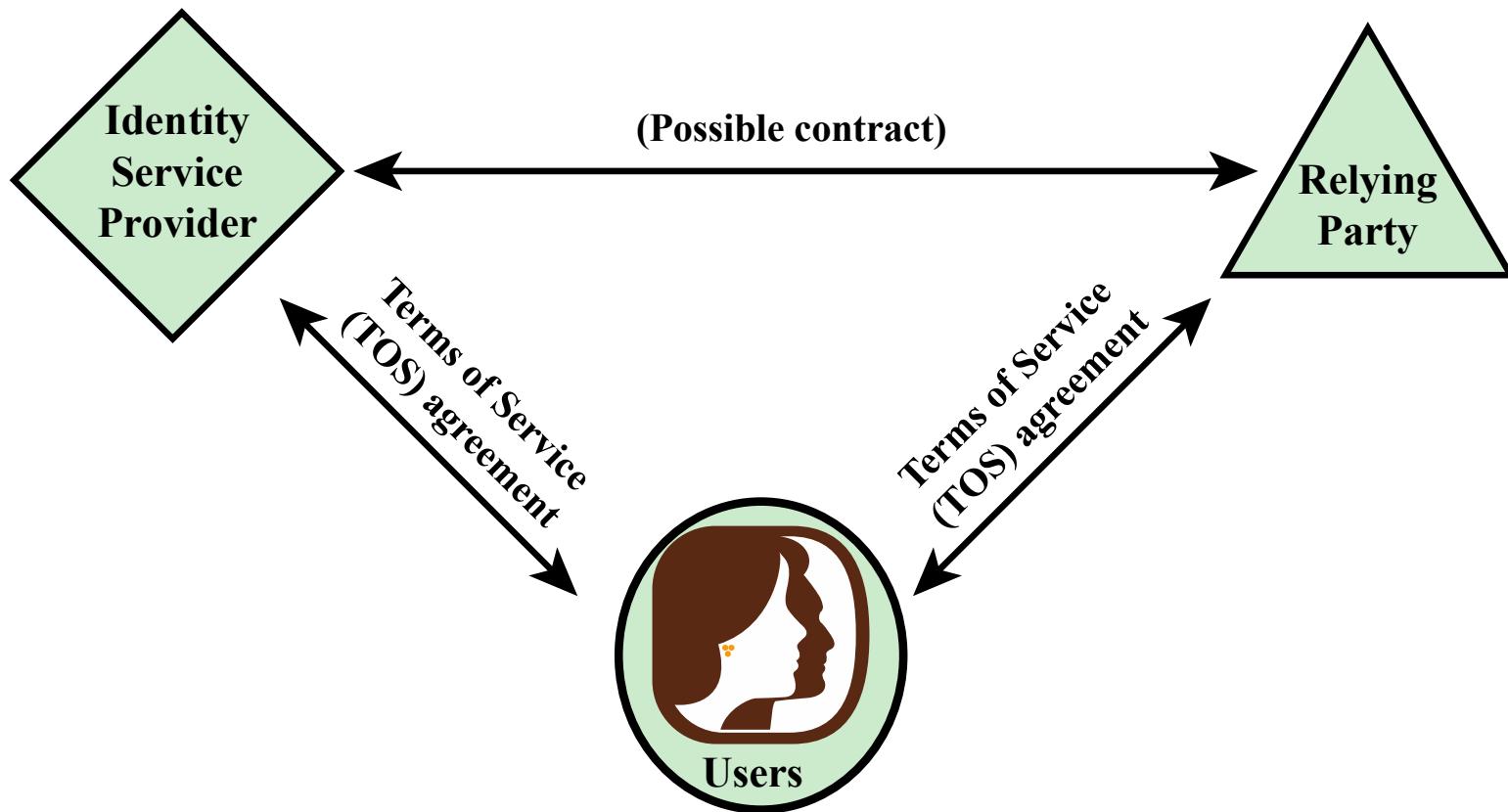
- Concerned with establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile
- These attributes represent features of an individual that can be used as the basis for determining access decisions to both physical and logical resources
- Privileges are considered attributes that can be linked to a digital identity

Policy management

- Governs what is allowable and unallowable in an access transaction

Identity Federation

- Term used to describe the technology, standards, policies, and processes that allow an organization to trust digital identities, identity attributes, and credentials created and issued by another organization
- Addresses two questions:
 - How do you trust identities of individuals from external organizations who need access to your systems
 - How do you vouch for identities of individuals in your organization when they need to collaborate with external organizations



(a) Traditional triangle of parties involved in an exchange of identity information

Figure 4.13 Identity Information Exchange Approaches

Open Identity Trust Framework

OpenID

- An open standard that allows users to be authenticated by certain cooperating sites using a third party service

OIDF

- OpenID Foundation is an international nonprofit organization of individuals and companies committed to enabling, promoting, and protecting OpenID technologies

ICF

- Information Card Foundation is a nonprofit community of companies and individuals working together to evolve the Information Card ecosystem

OITF

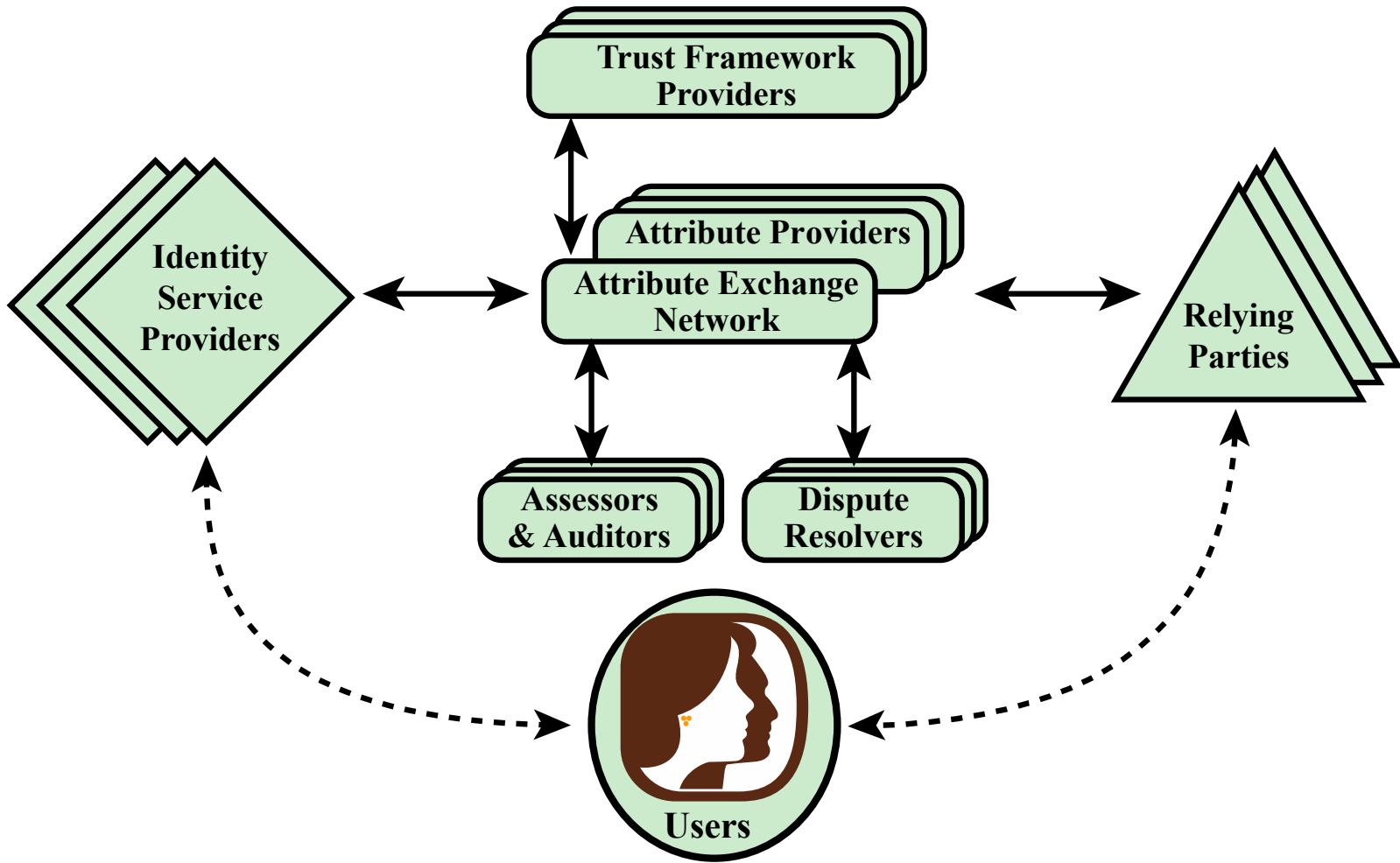
- Open Identity Trust Framework is a standardized, open specification of a trust framework for identity and attribute exchange, developed jointly by OIDF and ICF

OIX

- Open Identity Exchange Corporation is an independent, neutral, international provider of certification trust frameworks conforming to the OITF model

AXN

- Attribute Exchange Network is an online Internet-scale gateway for identity service providers and relying parties to efficiently access user asserted, permissioned, and verified online identity attributes in high volumes at affordable costs



(B) Identity attribute exchange elements

Figure 4.13 Identity Information Exchange Approaches

Table 4.5
Functions and Roles for Banking Example

(a) Functions and Official Positions		
Role	Function	Official Position
A	financial analyst	Clerk
B	financial analyst	Group Manager
C	financial analyst	Head of Division
D	financial analyst	Junior
E	financial analyst	Senior
F	financial analyst	Specialist
G	financial analyst	Assistant
...
X	share technician	Clerk
Y	support e-commerce	Junior
Z	office banking	Head of Division

Table 4.5
Functions and Roles for Banking Example

(b) Permission Assignments

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	1, 2, 3, 4, 7
	derivatives trading	1, 2, 3, 7, 10, 12, 14
	interest instruments	1, 4, 8, 12, 14, 16
	private consumer instruments	1, 2, 4, 7
...

(c) PA with Inheritance

Role	Application	Access Right
A	money market instruments	1, 2, 3, 4
	derivatives trading	1, 2, 3, 7, 10, 12
	interest instruments	1, 4, 8, 12, 14, 16
B	money market instruments	7
	derivatives trading	14
	private consumer instruments	1, 2, 4, 7
...

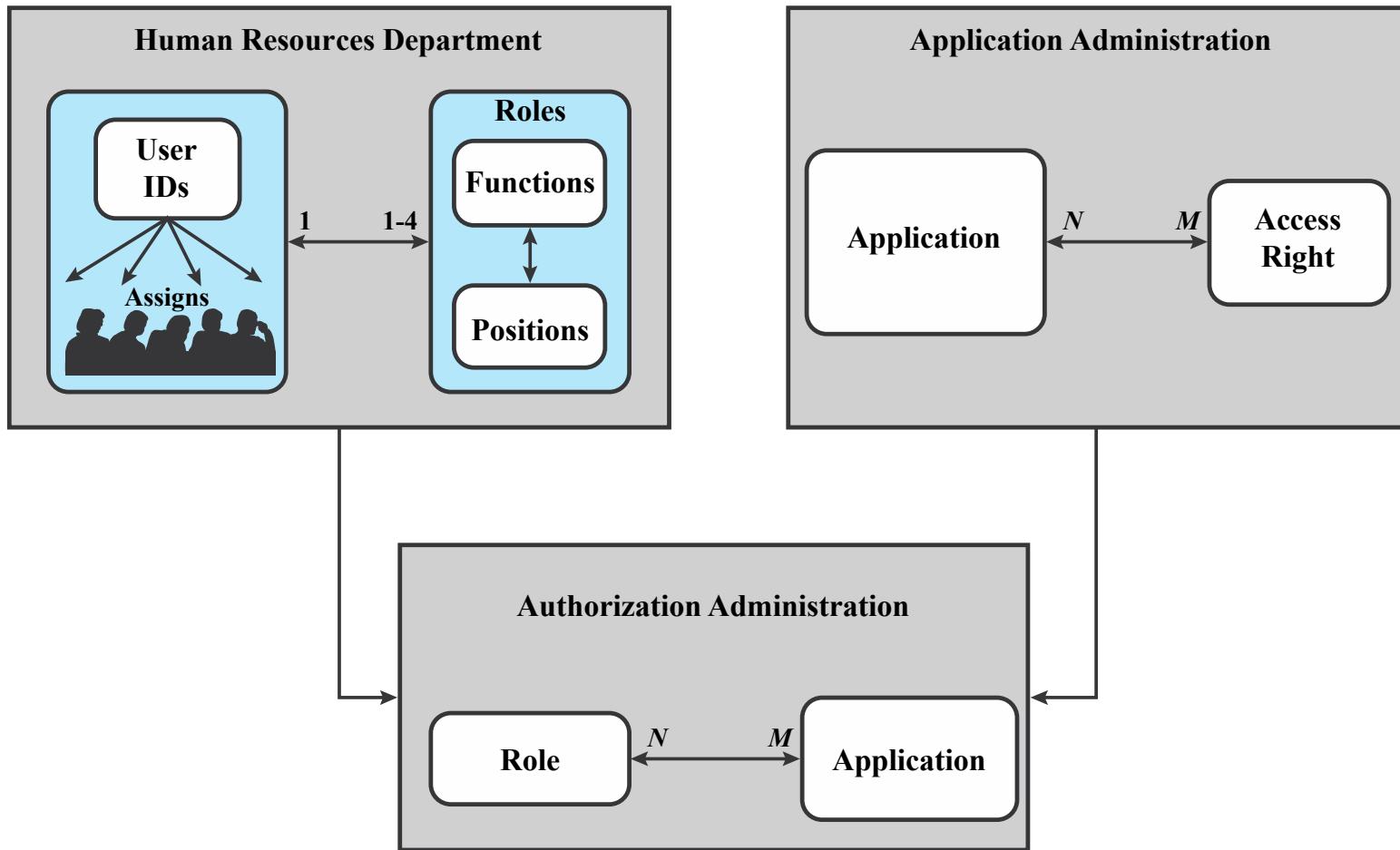


Figure 4.14 Example of Access Control Administration

Summary

- Access control principles
 - Access control context
 - Access control policies
- Subjects, objects, and access rights
- Discretionary access control
 - Access control model
 - Protection domains
- UNIX file access control
 - Traditional UNIX file access control
 - Access control lists in UNIX
- Role-based access control
 - RBAC reference models
- Attribute-based access control
 - Attributes
 - ABAC logical architecture
 - ABAC policies
- Identity, credential, and access management
 - Identity management
 - Credential management
 - Access management
 - Identity federation
- Trust frameworks
 - Traditional identity exchange approach
 - Open identity trust framework
- Bank RBAC system

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 5

Database and Data Center Security

Database Security

The increasing reliance on cloud technology to host part or all of the corporate database

Most enterprise environments consist of a heterogeneous mixture of database platforms, enterprise platforms, and OS platforms, creating an additional complexity hurdle for security personnel

There is a dramatic imbalance between the complexity of modern database management systems (DBMS) and the security technique used to protect these critical systems

Reasons database security has not kept pace with the increased reliance on databases are:

The typical organization lacks full-time database security personnel

Databases have a sophisticated interaction protocol, Structured Query Language (SQL), which is complex

Effective database security requires a strategy based on a full understanding of the security vulnerabilities of SQL

Databases

- Structured collection of data stored for use by one or more applications
- Contains the relationships between data items and groups of data items
- Can sometimes contain sensitive data that needs to be secured

Query language

- Provides a uniform interface to the database for users and applications

Database management system (DBMS)

- Suite of programs for constructing and maintaining the database
- Offers ad hoc query facilities to multiple users and applications

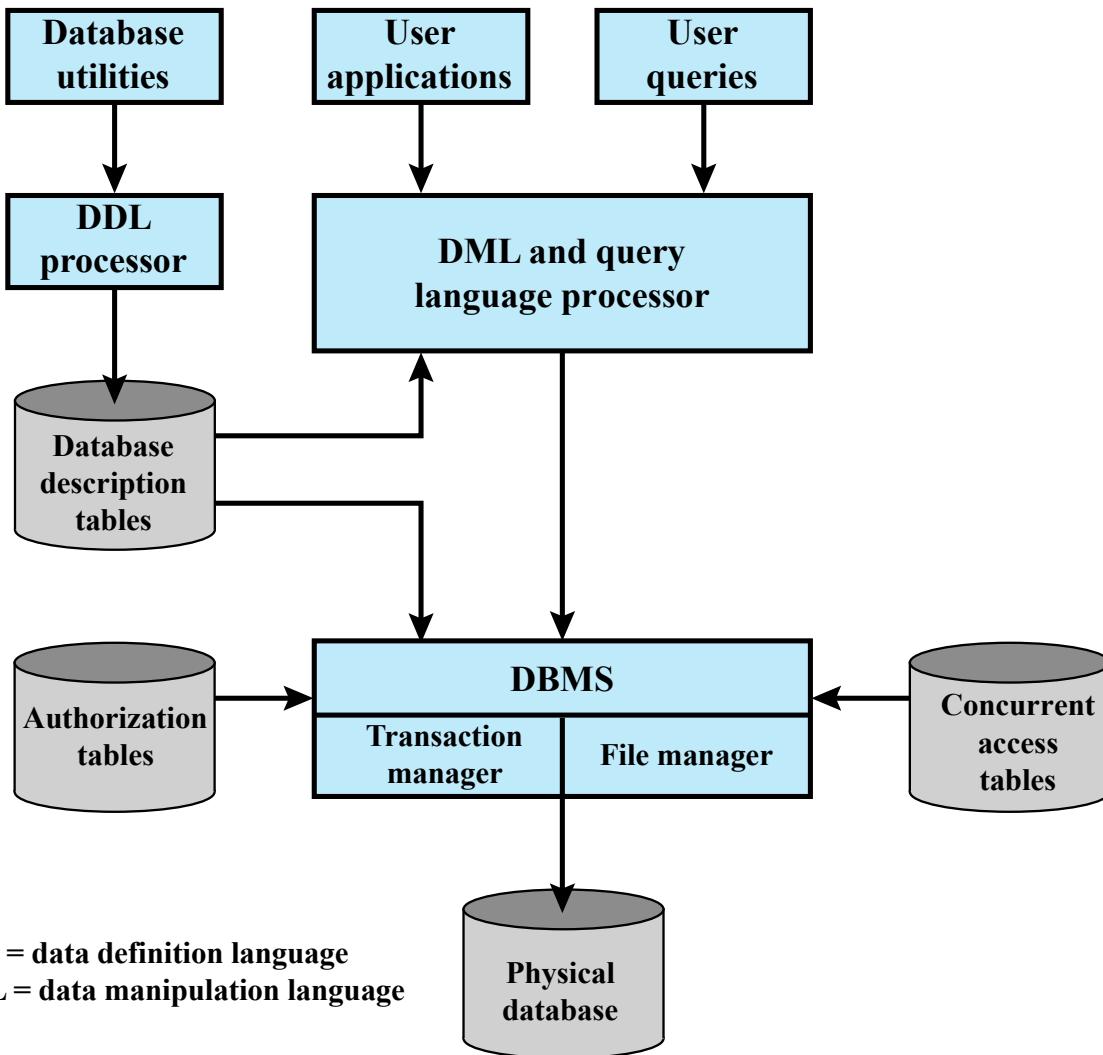
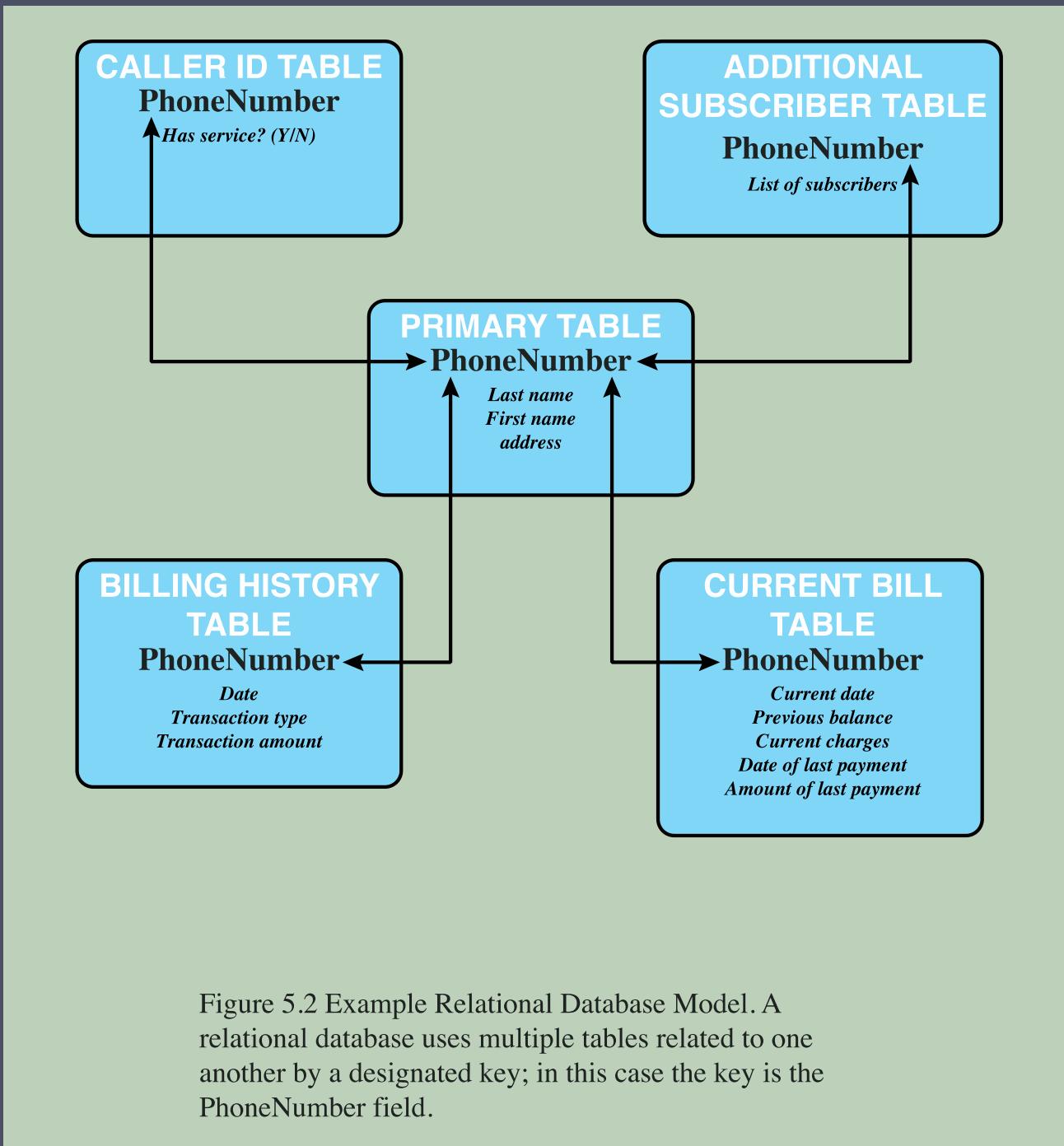


Figure 5.1 DBMS Architecture

Relational Databases

- Table of data consisting of rows and columns
 - Each column holds a particular type of data
 - Each row contains a specific value for each column
 - Ideally has one column where all values are unique, forming an identifier/key for that row
- Enables the creation of multiple tables linked together by a unique identifier that is present in all tables
- Use a relational query language to access the database
 - Allows the user to request data that fit a given set of criteria



Relational Database Elements

- Relation
 - Table/file
- Tuple
 - Row/record
- Attribute
 - Column/field

Primary key

- Uniquely identifies a row
- Consists of one or more column names

Foreign key

- Links one table to attributes in another

View/virtual table

- Result of a query that returns selected rows and columns from one or more tables
- Views are often used for security purposes

Table 5.1

Basic Terminology for Relational Databases

Formal Name	Common Name	Also Known As
Relation	Table	File
Tuple	Row	Record
Attribute	Column	Field

		Attributes								
		A_1	•	•	•	A_j	•	•	•	A_M
Records	1	x_{11}	•	•	•	x_{1j}	•	•	•	x_{1M}
	•	•				•			•	
	•	•				•			•	
	•	•				•			•	
	i	x_{i1}	•	•	•	x_{ij}	•	•	•	x_{iM}
	•	•				•			•	
	•	•				•			•	
	•	•				•			•	
	N	x_{N1}	•	•	•	x_{Nj}	•	•	•	x_{NM}

Figure 5.3 Abstract Model of a Relational Database

Department Table

Did	Dname	Dacctno
4	human resources	528221
8	education	202035
9	accounts	709257
13	public relations	755827
15	services	223945

primary key

Employee Table

Ename	Did	Salarycode	Eid	Ephone
Robin	15	23	2345	6127092485
Neil	13	12	5088	6127092246
Jasmine	4	26	7712	6127099348
Cody	15	22	9664	6127093148
Holly	8	23	3054	6127092729
Robin	8	24	2976	6127091945
Smith	9	21	4490	6127099380

foreign key

primary key

(a) Two tables in a relational database

Dname	Ename	Eid	Ephone
human resources	Jasmine	7712	6127099348
education	Holly	3054	6127092729
education	Robin	2976	6127091945
accounts	Smith	4490	6127099380
public relations	Neil	5088	6127092246
services	Robin	2345	6127092485
services	Cody	9664	6127093148

(b) A view derived from the database

Figure 5.4 Relational Database Example

Structured Query Language (SQL)

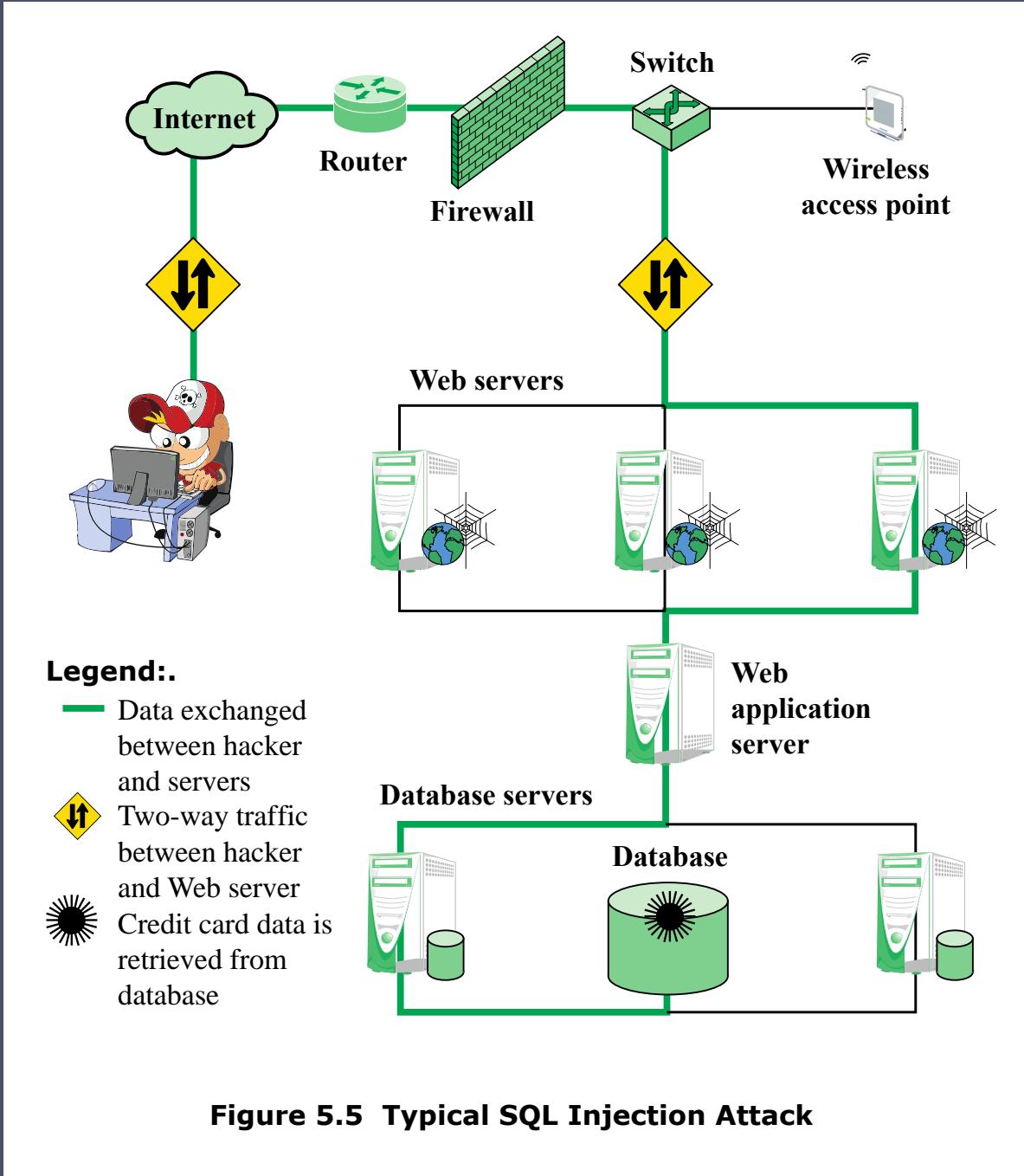
- Standardized language to define schema, manipulate, and query data in a relational database
- Several similar versions of ANSI/ISO standard
- All follow the same basic syntax and semantics

SQL statements can be used to:

- Create tables
- Insert and delete data in tables
- Create views
- Retrieve data with query statements

SQL Injection Attacks (SQLi)

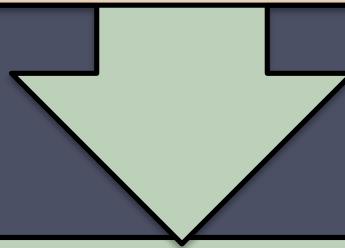
- One of the most prevalent and dangerous network-based security threats
- Designed to exploit the nature of Web application pages
- Sends malicious SQL commands to the database server
 - Most common attack goal is bulk extraction of data
 - Depending on the environment SQL injection can also be exploited to:
 - Modify or delete data
 - Execute arbitrary operating system commands
 - Launch denial-of-service (DoS) attacks



Injection Technique

The SQLi attack typically works by prematurely terminating a text string and appending a new command

Because the inserted command may have additional strings appended to it before it is executed the attacker terminates the injected string with a comment mark “- -”



Subsequent text is ignored at execution time

SQLi Attack Avenues

User input

- Attackers inject SQL commands by providing suitable crafted user input

Server variables

- Attackers can forge the values that are placed in HTTP and network headers and exploit this vulnerability by placing data directly into the headers

Second-order injection

- A malicious user could rely on data already present in the system or database to trigger an SQL injection attack, so when the attack occurs, the input that modifies the query to cause an attack does not come from the user, but from within the system itself

Cookies

- An attacker could alter cookies such that when the application server builds an SQL query based on the cookie's content, the structure and function of the query is modified

Physical user input

- Applying user input that constructs an attack outside the realm of web requests

Inband Attacks

- Uses the same communication channel for injecting SQL code and retrieving results
- The retrieved data are presented directly in application Web page
- Include:

Tautology

This form of attack injects code in one or more conditional statements so that they always evaluate to true

End-of-line comment

After injecting code into a particular field, legitimate code that follows are nullified through usage of end of line comments

Piggybacked queries

The attacker adds additional queries beyond the intended query, piggy-backing the attack on top of a legitimate request

Inferential Attack

- There is no actual transfer of data, but the attacker is able to reconstruct the information by sending particular requests and observing the resulting behavior of the Website/database server
- Include:
 - Illegal/logically incorrect queries
 - This attack lets an attacker gather important information about the type and structure of the backend database of a Web application
 - The attack is considered a preliminary, information-gathering step for other attacks
 - Blind SQL injection
 - Allows attackers to infer the data present in a database system even when the system is sufficiently secure to not display any erroneous information back to the attacker

Out-of-Band Attack

- Data are retrieved using a different channel
- This can be used when there are limitations on information retrieval, but outbound connectivity from the database server is lax

SQLi Countermeasures

- Three types:

- Manual defensive coding practices
- Parameterized query insertion
- SQL DOM

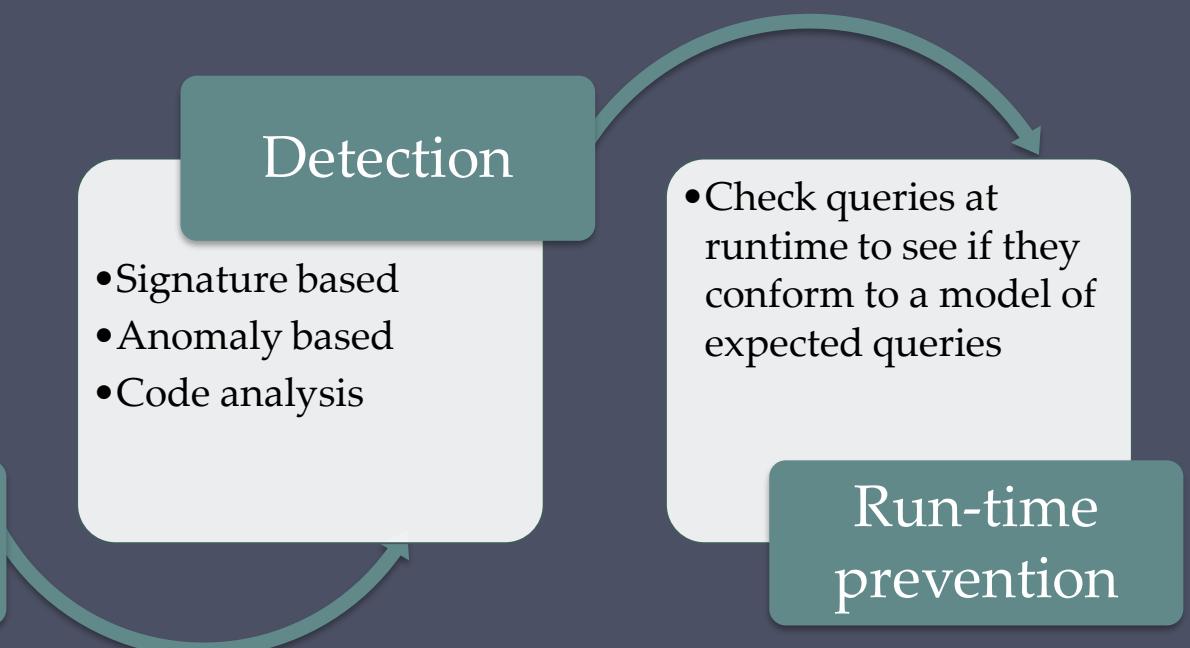
Defensive coding

Detection

- Signature based
- Anomaly based
- Code analysis

- Check queries at runtime to see if they conform to a model of expected queries

Run-time prevention



Database Access Control

Database access control system determines:

If the user has access to the entire database or just portions of it

What access rights the user has (create, insert, delete, update, read, write)

Can support a range of administrative policies

Centralized administration

- Small number of privileged users may grant and revoke access rights

Ownership-based administration

- The creator of a table may grant and revoke access rights to the table

Decentralized administration

- The owner of the table may grant and revoke authorization rights to other users, allowing them to grant and revoke access rights to the table

SQL Access Controls

- Two commands for managing access rights:
 - Grant
 - Used to grant one or more access rights or can be used to assign a user to a role
 - Revoke
 - Revokes the access rights
- Typical access rights are:
 - Select
 - Insert
 - Update
 - Delete
 - References

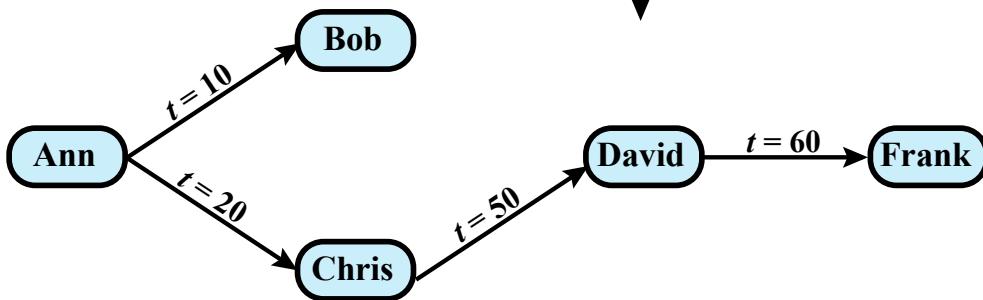
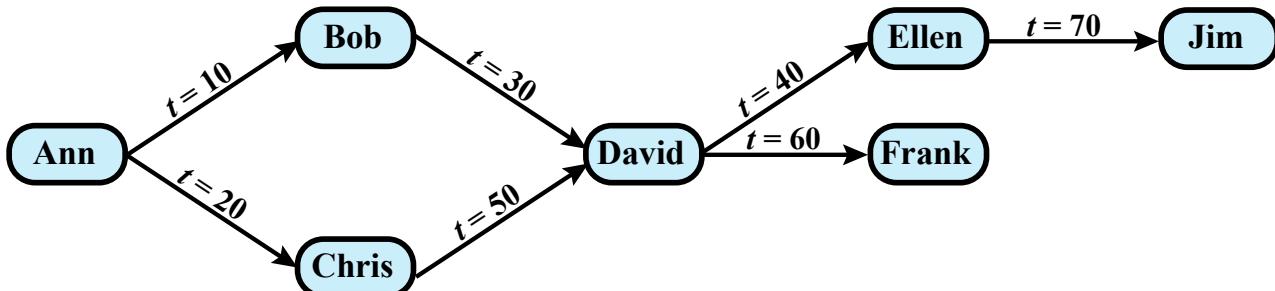


Figure 5.6 Bob Revokes Privilege from David

Role-Based Access Control (RBAC)

- Role-based access control eases administrative burden and improves security
- A database RBAC needs to provide the following capabilities:
 - Create and delete roles
 - Define permissions for a role
 - Assign and cancel assignment of users to roles
- Categories of database users:

Application owner

- An end user who owns database objects as part of an application

End user

- An end user who operates on database objects via a particular application but does not own any of the database objects

Administrator

- User who has administrative responsibility for part or all of the database

Table 5.2

Fixed Roles in Microsoft SQL Server

(Table is on page 165 in
the textbook)

Role	Permissions
Fixed Server Roles	
sysadmin	Can perform any activity in SQL Server and have complete control over all database functions
serveradmin	Can set server-wide configuration options, shut down the server
setupadmin	Can manage linked servers and startup procedures
securityadmin	Can manage logins and CREATE DATABASE permissions, also read error logs and change passwords
processadmin	Can manage processes running in SQL Server
dbcreator	Can create, alter, and drop databases
diskadmin	Can manage disk files
bulkadmin	Can execute BULK INSERT statements
Fixed Database Roles	
db_owner	Has all permissions in the database
db_accessadmin	Can add or remove user IDs
db_datareader	Can select all data from any user table in the database
db_datawriter	Can modify any data in any user table in the database
db_ddladmin	Can issue all Data Definition Language (DDL) statements
db_securityadmin	Can manage all permissions, object ownerships, roles and role memberships
db_backupoperator	Can issue DBCC, CHECKPOINT, and BACKUP statements
db_denydatareader	Can deny permission to select data in the database
db_denydatawriter	Can deny permission to change data in the database

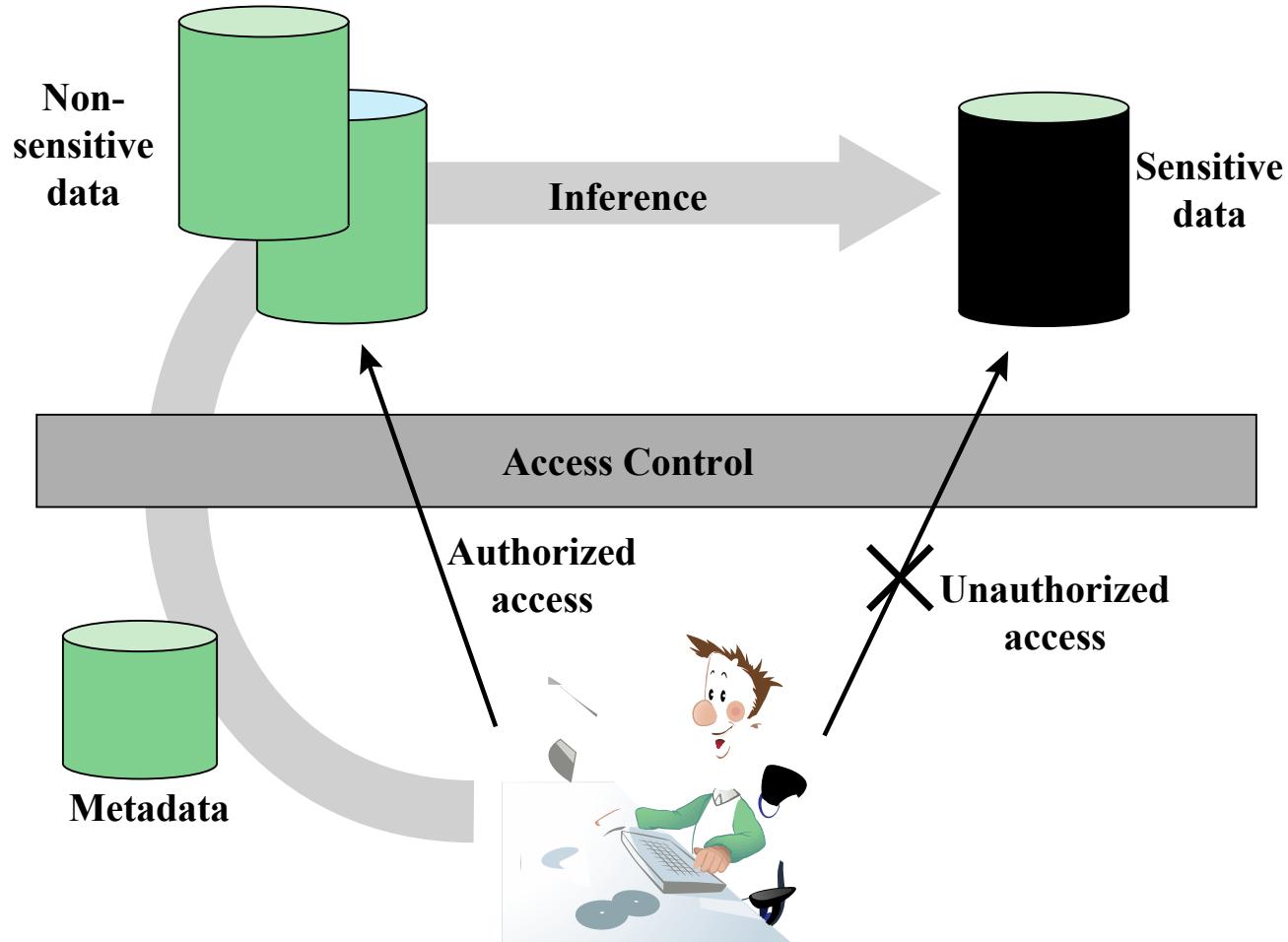


Figure 5.7 Indirect Information Access Via Inference Channel

Item	Availability	Cost (\$)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware
Cake pan	online only	12.99	housewares
Shower/tub cleaner	in-store/online	11.99	housewares
Rolling pin	in-store/online	10.99	housewares

(a) Inventory table

Availability	Cost (\$)
in-store/online	7.99
online only	5.49
in-store/online	104.99

Item	Department
Shelf support	hardware
Lid support	hardware
Decorative chain	hardware

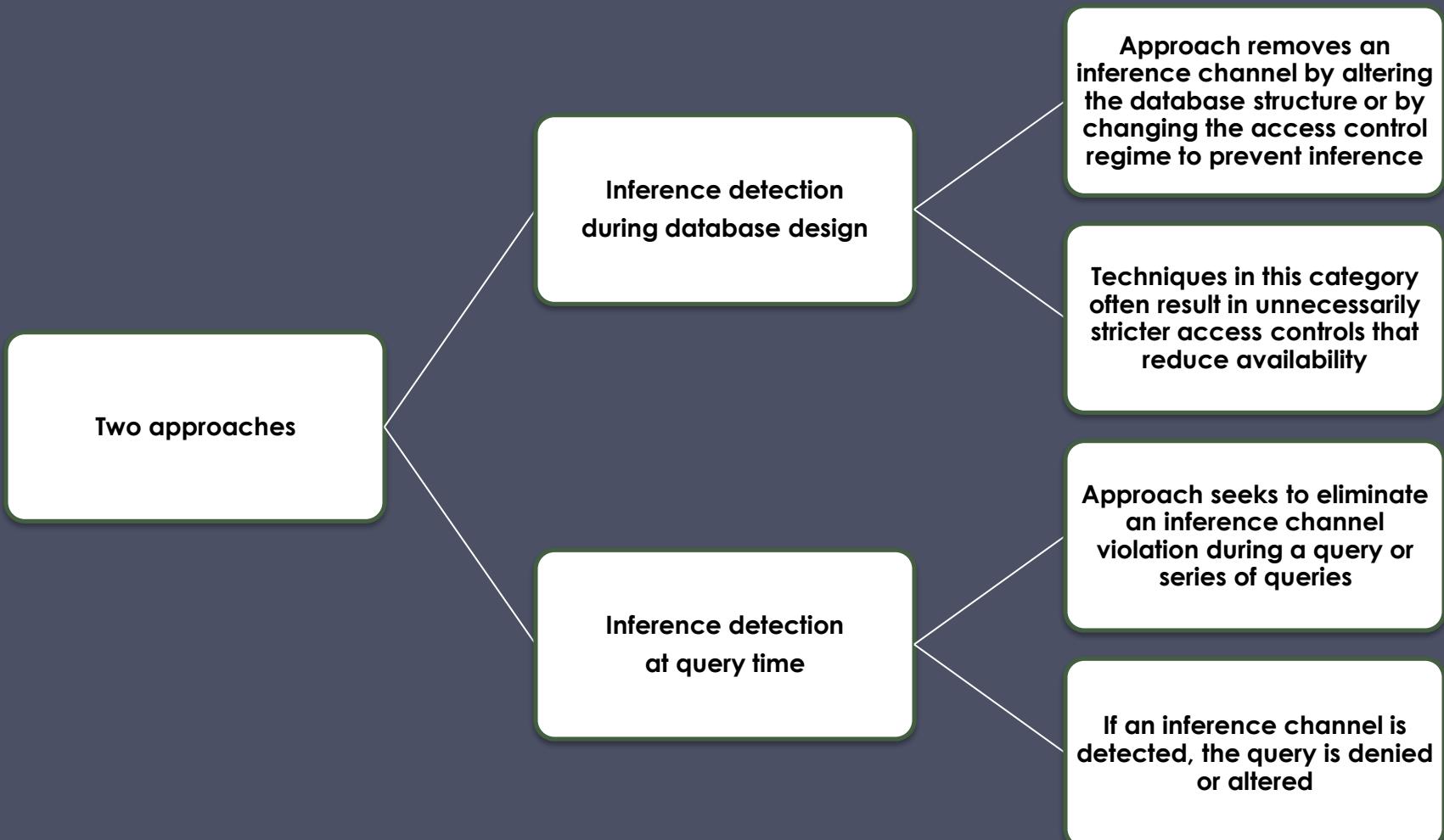
(b) Two views

Item	Availability	Cost (\$)	Department
Shelf support	in-store/online	7.99	hardware
Lid support	online only	5.49	hardware
Decorative chain	in-store/online	104.99	hardware

(c) Table derived from combining query answers

Figure 5.8 Inference Example

Inference Detection



- Some inference detection algorithm is needed for either of these approaches
- Progress has been made in devising specific inference detection techniques for multilevel secure databases and statistical databases

Database Encryption

- The database is typically the most valuable information resource for any organization
 - Protected by multiple layers of security
 - Firewalls, authentication, general access control systems, DB access control systems, database encryption
 - Encryption becomes the last line of defense in database security
 - Can be applied to the entire database, at the record level, the attribute level, or level of the individual field
- Disadvantages to encryption:
 - Key management
 - Authorized users must have access to the decryption key for the data for which they have access
 - Inflexibility
 - When part or all of the database is encrypted it becomes more difficult to perform record searching

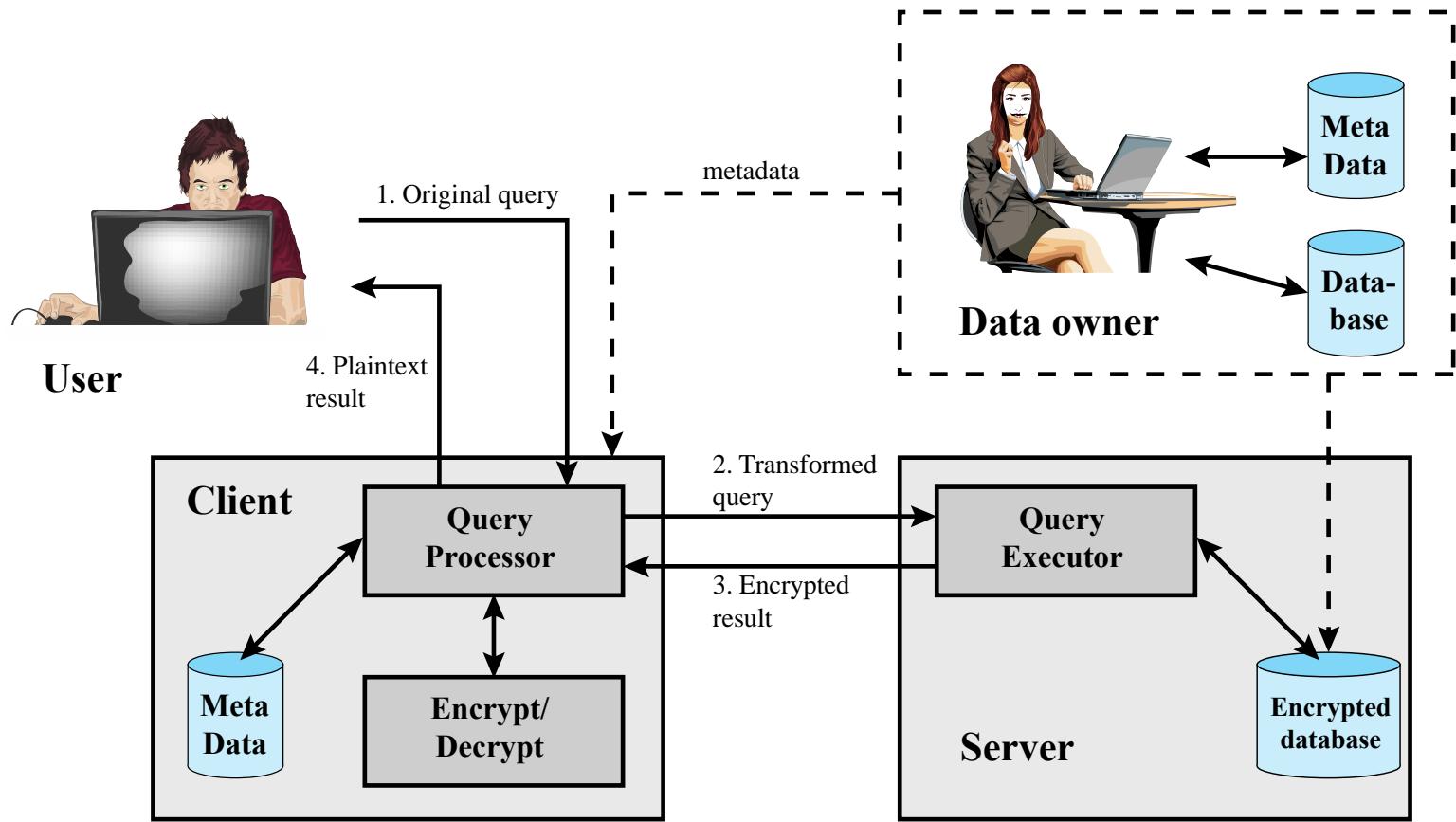


Figure 5.9 A Database Encryption Scheme

$E(k, B_1)$	I_{11}	\dots	I_{Ij}	\dots	I_{IM}
\cdot	\cdot		\cdot		\cdot
\cdot	\cdot		\cdot		\cdot
\cdot	\cdot		\cdot		\cdot
$E(k, B_i)$	I_{i1}	\dots	I_{ij}	\dots	I_{iM}
\cdot	\cdot		\cdot		\cdot
\cdot	\cdot		\cdot		\cdot
\cdot	\cdot		\cdot		\cdot
$E(k, B_N)$	I_{N1}	\dots	I_{Nj}	\dots	I_{NM}

$$B_i = (x_{i1} \parallel x_{i2} \parallel \dots \parallel x_{iM})$$

Figure 5.10 Encryption Scheme for Database of Figure 5.3

Table 5.3 Encrypted Database Example

(a) Employee Table

eid	ename	salary	addr	did
23	Tom	70K	Maple	45
860	Mary	60K	Main	83
320	John	50K	River	50
875	Jerry	55K	Hopewell	92

(b) Encrypted Employee Table with Indexes

E(k, B)	I(eid)	I(ename)	I(salary)	I(addr)	I(did)
1100110011001011...	1	10	3	7	4
0111000111001010...	5	7	2	7	8
1100010010001101...	2	5	1	9	5
0011010011111101...	5	5	2	4	9

Data Center Security

- Data center:
 - An enterprise facility that houses a large number of servers, storage devices, and network switches and equipment
 - The number of servers and storage devices can run into the tens of thousands in one facility
 - Generally includes redundant or backup power supplies, redundant network connections, environmental controls, and various security devices
 - Can occupy one room of a building, one or more floors, or an entire building
- Examples of uses include:
 - Cloud service providers
 - Search engines
 - Large scientific research facilities
 - IT facilities for large enterprises

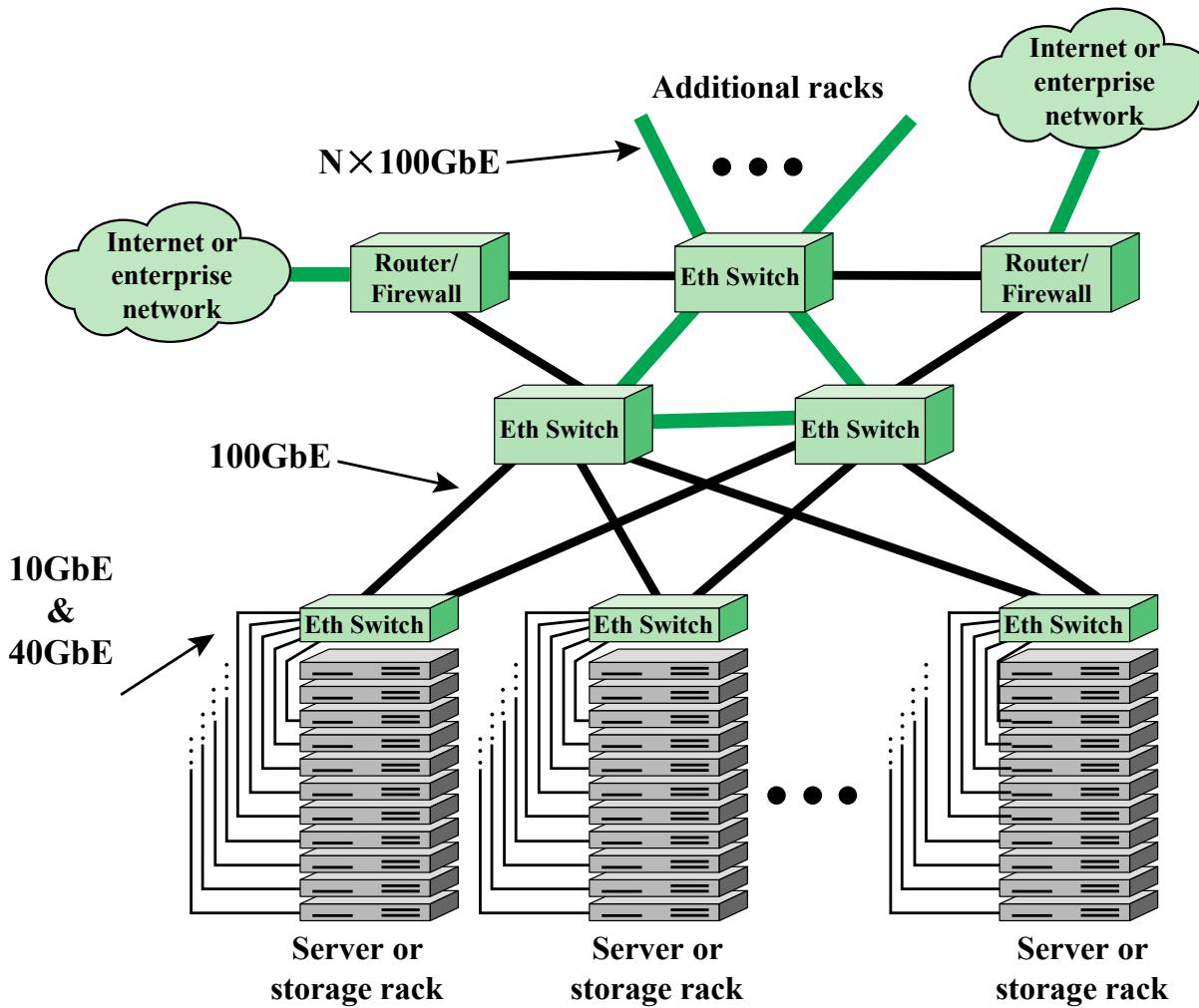


Figure 5.11 Key Data Center Elements

Data Security	Encryption, Password policy, secure IDs, Data Protection (ISO 27002), Data masking, Data retention, etc.
Network Security	Firewalls, Anti-virus, Intrusion detection/prevention, authentication, etc.
Physical Security	Surveillance, Mantraps, Two/three factor authentication, Security zones, ISO 27001/27002, etc.
Site Security	Setbacks, Redundant utilities Landscaping, Buffer zones, Crash barriers, Entry points, etc.

Figure 5.12 Data Center Security Model

TIA-492

- The Telecommunications Industry Association (TIA)
- TIA-492 (*Telecommunications Infrastructure Standard for Data Centers*) specifies the minimum requirements for telecommunications infrastructure of data centers
- Includes topics such as:
 - Network architecture
 - Electrical design
 - File storage, backup, and archiving
 - System redundancy
 - Network access control and security
 - Database management
 - Web hosting
 - Application hosting
 - Content distribution
 - Environmental control
 - Protection against physical hazards
 - Power management

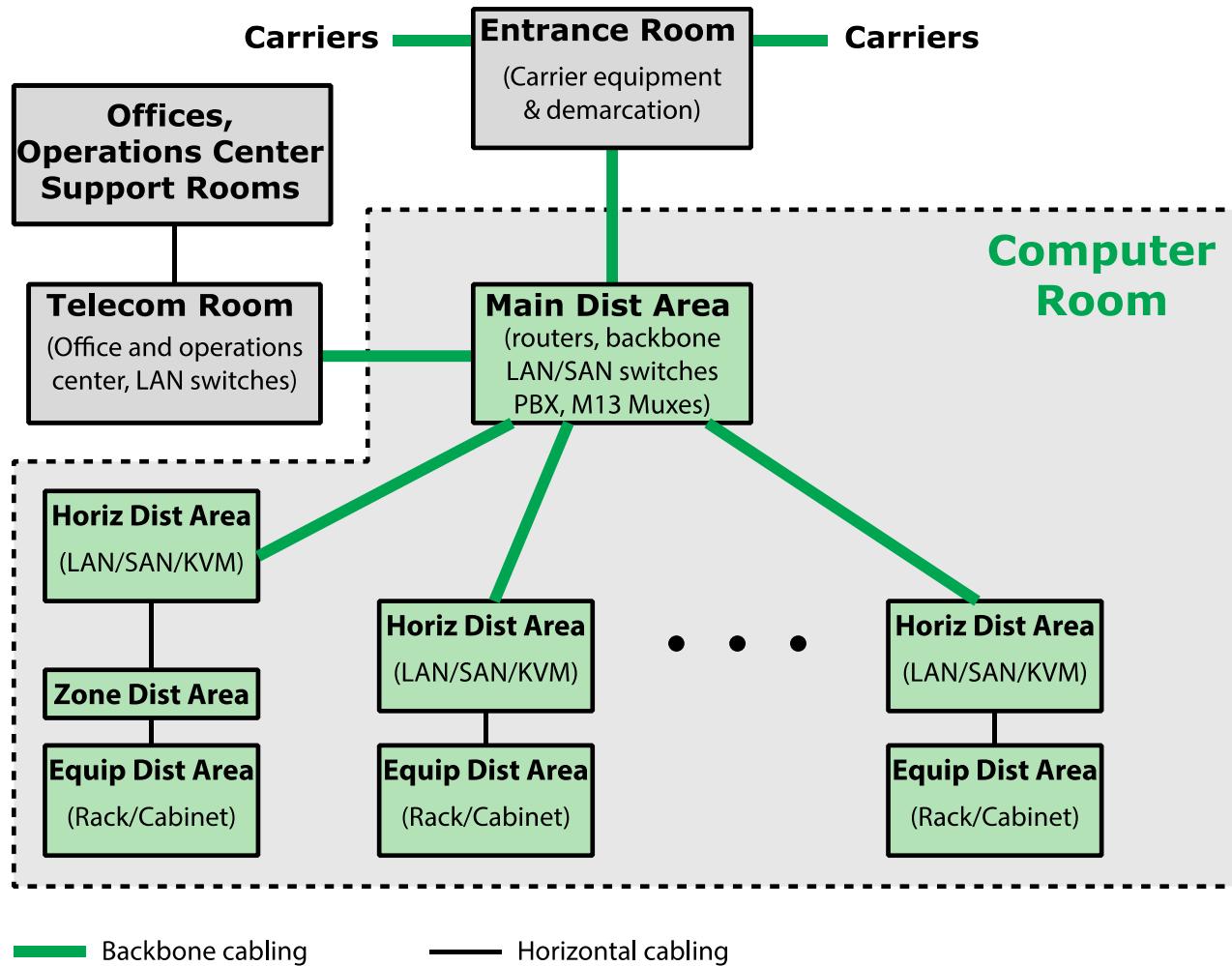


Figure 5.13 TIA-942 Compliant Data Center Showing Key Functional Areas

Table 5.4
**Data Center
Tiers
Defined in
TIA-942**

Tier	System design	Availability /Annual Downtime
1	<ul style="list-style-type: none"> Susceptible to disruptions from both planned and unplanned activity Single path for power and cooling distribution, no redundant components May or may not have raised floor, UPS, or generator Takes 3 months to implement Must be shut down completely to perform preventive maintenance 	99.671%/ 28.8 hours
2	<ul style="list-style-type: none"> Less susceptible to disruptions from both planned and unplanned activity Single path for power and cooling distribution, includes redundant components Includes raised floor, UPS, and generator Takes 3 to 6 months to implement Maintenance of power path and other parts of the infrastructure require a processing shutdown 	99.741%/ 22.0 hours
3	<ul style="list-style-type: none"> Enables planned activity without disrupting computer hardware operation but unplanned events will still cause disruption Multiple power and cooling distribution paths but with only one path active, includes redundant components Takes 15 to 20 months to implement Includes raised floor and sufficient capacity and distribution to carry load on one path while performing maintenance on the other 	99.982%/ 1.6 hours
4	<ul style="list-style-type: none"> Planned activity does not disrupt critical load and data center can sustain at least one worst-case unplanned event with no critical load impact Multiple active power and cooling distribution paths, includes redundant components Takes 15 to 20 months to implement 	99.995%/ 0.4 hours

(Table is on page 177 in textbook)

Summary

- The need for database security
- Database management systems
- Relational databases
 - Elements of a relational database system
 - Structured Query Language
- SQL injection attacks
 - A typical SQLi attack
 - The injection technique
 - SQLi attack avenues and types
 - SQLi countermeasures
- Database access control
 - SQL-based access definition
 - Cascading authorizations
 - Role-based access control
- Inference
- Database encryption
- Data center security
 - Data center elements
 - Data center security considerations
 - TIA-492

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 6

Malicious Software

Malware

NIST 800-83 defines malware as:

“a program that is inserted into a system,
usually covertly, with the intent of
compromising the confidentiality, integrity, or
availability of the victim’s data, applications, or
operating system or otherwise annoying or
disrupting the victim.”

Classification of Malware

Classified into two broad categories:

Based first on how it spreads or propagates to reach the desired targets

Then on the actions or payloads it performs once a target is reached

Also classified by:

Those that need a host program (parasitic code such as viruses)

Those that are independent, self-contained programs (worms, trojans, and bots)

Malware that does not replicate (trojans and spam e-mail)

Malware that does replicate (viruses and worms)

Types of Malicious Software (Malware)

Propagation mechanisms include:

- Infection of existing content by viruses that is subsequently spread to other systems
- Exploit of software vulnerabilities by worms or drive-by-downloads to allow the malware to replicate
- Social engineering attacks that convince users to bypass security mechanisms to install Trojans or to respond to phishing attacks



Payload actions performed by malware once it reaches a target system can include:

- Corruption of system or data files
- Theft of service/make the system a zombie agent of attack as part of a botnet
- Theft of information from the system/keylogging
- Stealth/hiding its presence on the system

Viruses

- Piece of software that infects programs
 - Modifies them to include a copy of the virus
 - Replicates and goes on to infect other content
 - Easily spread through network environments
- When attached to an executable program a virus can do anything that the program is permitted to do
 - Executes secretly when the host program is run
- Specific to operating system and hardware
 - Takes advantage of their details and weaknesses

Virus Components

Infection mechanism

- Means by which a virus spreads or propagates
- Also referred to as the *infection vector*

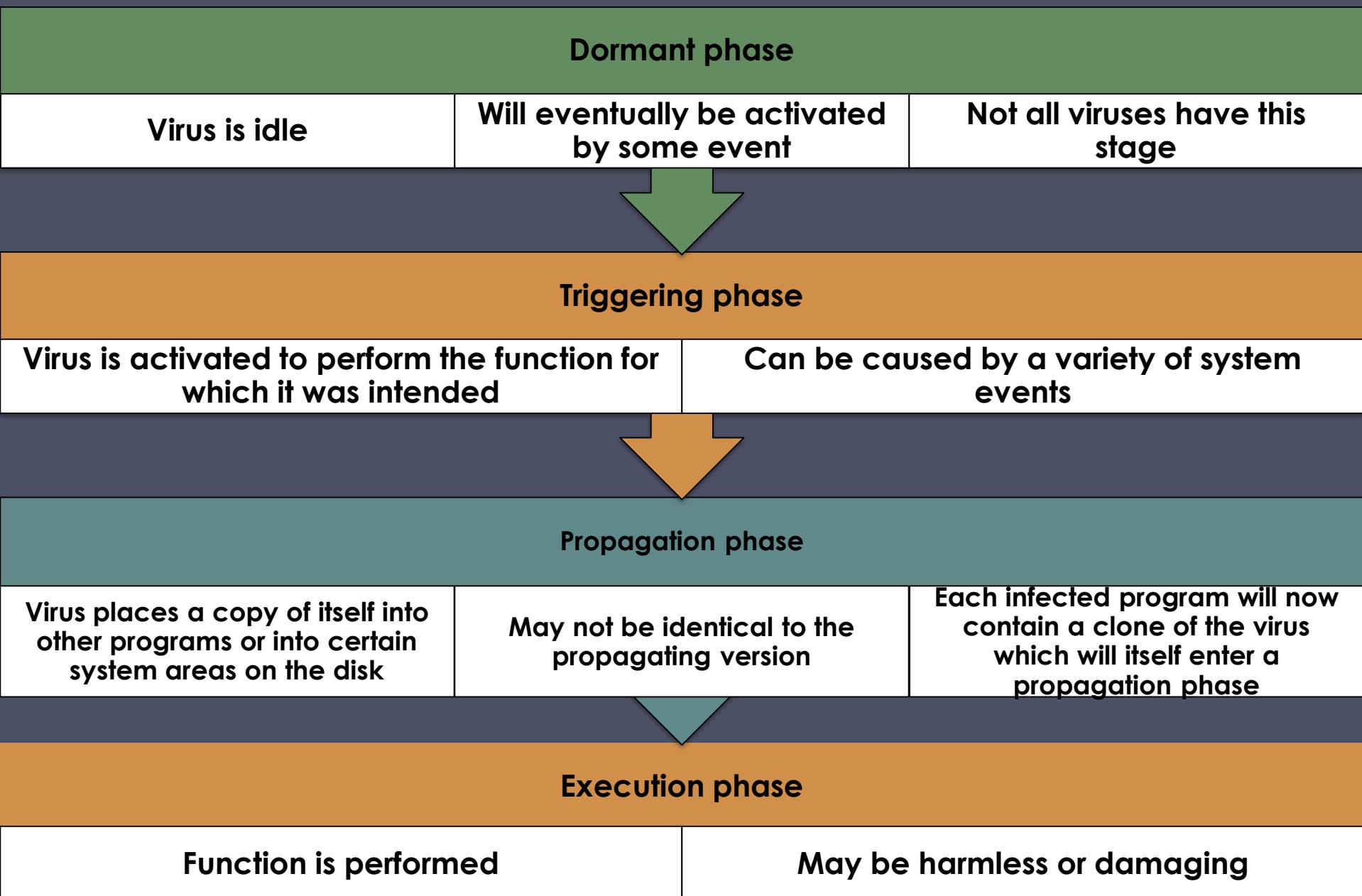
Trigger

- Event or condition that determines when the payload is activated or delivered
- Sometimes known as a *logic bomb*

Payload

- What the virus does (besides spreading)
- May involve damage or benign but noticeable activity

Virus Phases



Worms

- Program that actively seeks out more machines to infect and each infected machine serves as an automated launching pad for attacks on other machines
- Exploits software vulnerabilities in client or server programs
- Can use network connections to spread from system to system
- Spreads through shared media (USB drives, CD, DVD data disks)
- E-mail worms spread in macro or script code included in attachments and instant messenger file transfers
- Upon activation the worm may replicate and propagate again
- Usually carries some form of payload
- First known implementation was done in Xerox Palo Alto Labs in the early 1980s

Worm Replication

Electronic mail or instant messenger facility

- Worm e-mails a copy of itself to other systems
- Sends itself as an attachment via an instant message service

File sharing

- Creates a copy of itself or infects a file as a virus on removable media

Remote execution capability

- Worm executes a copy of itself on another system

Remote file access or transfer capability

- Worm uses a remote file access or transfer service to copy itself from one system to the other

Remote login capability

- Worm logs onto a remote system as a user and then uses commands to copy itself from one system to the other

Recent Worm Attacks

Melissa	1998	E-mail worm First to include virus, worm and Trojan in one package
Code Red	July 2001	Exploited Microsoft IIS bug Probes random IP addresses Consumes significant Internet capacity when active
Code Red II	August 2001	Also targeted Microsoft IIS Installs a backdoor for access
Nimda	September 2001	Had worm, virus and mobile code characteristics Spread using e-mail, Windows shares, Web servers, Web clients, backdoors
SQL Slammer	Early 2003	Exploited a buffer overflow vulnerability in SQL server compact and spread rapidly
Sobig.F	Late 2003	Exploited open proxy servers to turn infected machines into spam engines
Mydoom	2004	Mass-mailing e-mail worm Installed a backdoor in infected machines
Warezov	2006	Creates executables in system directories Sends itself as an e-mail attachment Can disable security related products
Conficker (Downadup)	November 2008	Exploits a Windows buffer overflow vulnerability Most widespread infection since SQL Slammer
Stuxnet	2010	Restricted rate of spread to reduce chance of detection Targeted industrial control systems

WannaCry

Ransomware attack in May 2017 that spread extremely fast over a period of hours to days, infecting hundreds of thousands of systems belonging to both public and private organizations in more than 150 countries

It spread as a worm by aggressively scanning both local and random remote networks, attempting to exploit a vulnerability in the Server Message Block protocol file sharing service on unpatched Windows systems

This rapid spread was only slowed by the accidental activation of a "kill-switch" domain by a UK security researcher

Once installed on infected systems, it also encrypted files, demanding a ransom payment to recover them

Worm Technology

Multiplatform

Metamorphic

Multi-exploit

Polymorphic

Ultrafast
spreading

Mobile Code

- NIST SP 800-28 defines mobile code as

“programs that can be shipped unchanged to a heterogeneous collection of platforms and executed with identical semantics”
- Transmitted from a remote system to a local system and then executed on the local system
- Often acts as a mechanism for a virus, worm, or Trojan horse
- Takes advantage of vulnerabilities to perform its own exploits
- Popular vehicles include:
 - Java applets
 - ActiveX
 - JavaScript
 - VBScript
- Most common ways of using mobile code for malicious operations on local system are:
 - Cross-site scripting
 - Interactive and dynamic Web sites
 - E-mail attachments
 - Downloads from untrusted sites or of untrusted software

Mobile Phone Worms

- First discovery was Cabir worm in 2004
- Then Lasco and CommWarrior in 2005
- Communicate through Bluetooth wireless connections or MMS
- Target is the smartphone
- Can completely disable the phone, delete data on the phone, or force the device to send costly messages
- CommWarrior replicates by means of Bluetooth to other phones, sends itself as an MMS file to contacts and as an auto reply to incoming text messages

Drive-By-Downloads

Exploits browser and plugin vulnerabilities so when the user views a webpage controlled by the attacker, it contains code that exploits the bug to download and install malware on the system without the user's knowledge or consent

In most cases the malware does not actively propagate as a worm does

Spreads when users visit the malicious Web page

Watering-Hole Attacks

- A variant of drive-by-download used in highly targeted attacks
- The attacker researches their intended victims to identify websites they are likely to visit, then scans these sites to identify those with vulnerabilities that allow their compromise
- They then wait for one of their intended victims to visit one of the compromised sites
- Attack code may even be written so that it will only infect systems belonging to the target organization and take no action for other visitors to the site
- This greatly increases the likelihood of the site compromise remaining undetected

Malvertising

Places malware on websites without actually compromising them

The attacker pays for advertisements that are highly likely to be placed on their intended target websites and incorporate malware in them

Using these malicious ads, attackers can infect visitors to sites displaying them

The malware code may be dynamically generated to either reduce the chance of detection or to only infect specific systems

Has grown rapidly in recent years because they are easy to place on desired websites with few questions asked and are hard to track

Attackers can place these ads for as little as a few hours, when they expect their intended victims could be browsing the targeted websites, greatly reducing their visibility

Clickjacking

- Also known as a user-interface (UI) redress attack
- Using a similar technique, keystrokes can also be hijacked
 - A user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker
- Vulnerability used by an attacker to collect an infected user's clicks
 - The attacker can force the user to do a variety of things from adjusting the user's computer settings to unwittingly sending the user to Web sites that might have malicious code
 - By taking advantage of Adobe Flash or JavaScript an attacker could even place a button under or over a legitimate button making it difficult for users to detect
 - A typical attack uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page
 - The attacker is hijacking clicks meant for one page and routing them to another page

Social Engineering

- “Tricking” users to assist in the compromise of their own systems

Spam

Unsolicited bulk e-mail

Significant carrier of malware

Used for phishing attacks

Trojan horse

Program or utility containing harmful hidden code

Used to accomplish functions that the attacker could not accomplish directly

Mobile phone Trojans

First appeared in 2004 (Skuller)

Target is the smartphone

Payload

System Corruption

Chernobyl virus

- First seen in 1998
- Example of a destructive parasitic memory-resident Windows 95 and 98 virus
- Infects executable files when they are opened and when a trigger date is reached, the virus deletes data on the infected system by overwriting the first megabyte of the hard drive with zeroes, resulting in massive corruption of the entire file system

Klez

- Mass mailing worm infecting Windows 95 to XP systems
- First seen in October 2001
- Spreads by e-mailing copies of itself to addresses found in the address book and in files on the system
- It can stop and delete some anti-virus programs running on the system
- On trigger date causes files on the hard drive to become empty

Ransomware

- Encrypts the user's data and demands payment in order to access the key needed to recover the information
- PC Cyborg Trojan (1989)
- Mid-2006 a number of worms and Trojans appeared that used public-key cryptography with increasingly larger key sizes to encrypt data
- The user needed to pay a ransom, or to make a purchase from certain sites, in order to receive the key to decrypt this data

Ransomware

- WannaCry

- Infected a large number of systems in many countries in May 2017
- When installed on infected systems, it encrypted a large number of files and then demanded a ransom payment in Bitcoins to recover them
- Recovery of this information was generally only possible if the organization had good backups and an appropriate incident response and disaster recovery plan
- Targets widened beyond personal computer systems to include mobile devices and Linux servers
- Tactics such as threatening to publish sensitive personal information, or to permanently destroy the encryption key after a short period of time, are sometimes used to increase the pressure on the victim to pay up

Payload System Corruption

- Real-world damage
 - Causes damage to physical equipment
 - Chernobyl virus rewrites BIOS code
 - Stuxnet worm
 - Targets specific industrial control system software
 - There are concerns about using sophisticated targeted malware for industrial sabotage
- Logic bomb
 - Code embedded in the malware that is set to “explode” when certain conditions are met

Payload – Attack Agents Bots

- Takes over another Internet attached computer and uses that computer to launch or manage attacks
- *Botnet* - collection of bots capable of acting in a coordinated manner
- Uses:
 - Distributed denial-of-service (DDoS) attacks
 - Spamming
 - Sniffing traffic
 - Keylogging
 - Spreading new malware
 - Installing advertisement add-ons and browser helper objects (BHOs)
 - Attacking IRC chat networks
 - Manipulating online polls/games

Remote Control Facility

- Distinguishes a bot from a worm
 - Worm propagates itself and activates itself
 - Bot is initially controlled from some central facility
- Typical means of implementing the remote control facility is on an IRC server
 - Bots join a specific channel on this server and treat incoming messages as commands
 - More recent botnets use covert communication channels via protocols such as HTTP
 - Distributed control mechanisms use peer-to-peer protocols to avoid a single point of failure

Payload – Information Theft Keyloggers and Spyware

Keylogger

- Captures keystrokes to allow attacker to monitor sensitive information
- Typically uses some form of filtering mechanism that only returns information close to keywords (“login”, “password”)

Spyware

- Subverts the compromised machine to allow monitoring of a wide range of activity on the system
 - Monitoring history and content of browsing activity
 - Redirecting certain Web page requests to fake sites
 - Dynamically modifying data exchanged between the browser and certain Web sites of interest

Payload – Information Theft

Phishing

- Exploits social engineering to leverage the user's trust by masquerading as communication from a trusted source
 - Include a URL in a spam e-mail that links to a fake Web site that mimics the login page of a banking, gaming, or similar site
 - Suggests that urgent action is required by the user to authenticate their account
 - Attacker exploits the account using the captured credentials
- Spear-phishing
 - Recipients are carefully researched by the attacker
 - E-mail is crafted to specifically suit its recipient, often quoting a range of information to convince them of its authenticity

Payload – Stealthing Backdoor

- Also known as a *trapdoor*
- Secret entry point into a program allowing the attacker to gain access and bypass the security access procedures
- *Maintenance hook* is a backdoor used by Programmers to debug and test programs
- Difficult to implement operating system controls for backdoors in applications

Payload - Stealthing Rootkit

- Set of hidden programs installed on a system to maintain covert access to that system
- Hides by subverting the mechanisms that monitor and report on the processes, files, and registries on a computer
- Gives administrator (or root) privileges to attacker
 - Can add or change programs and files, monitor processes, send and receive network traffic, and get backdoor access on demand

Rootkit Classification Characteristics

Persistent

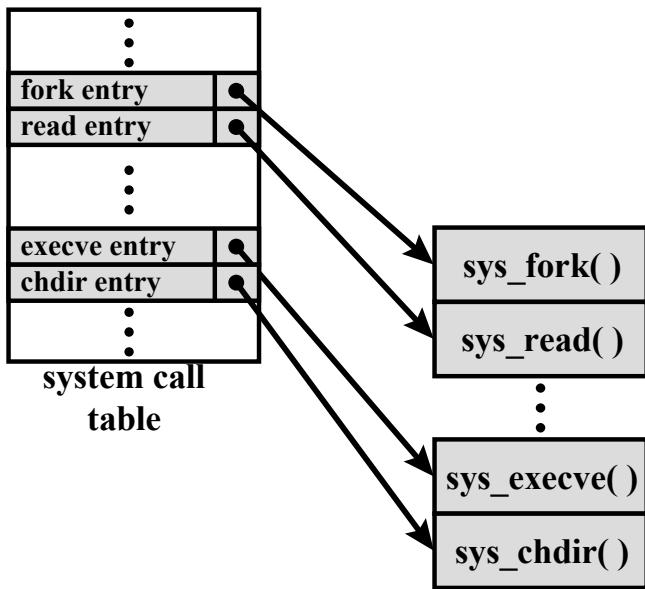
Memory
based

User mode

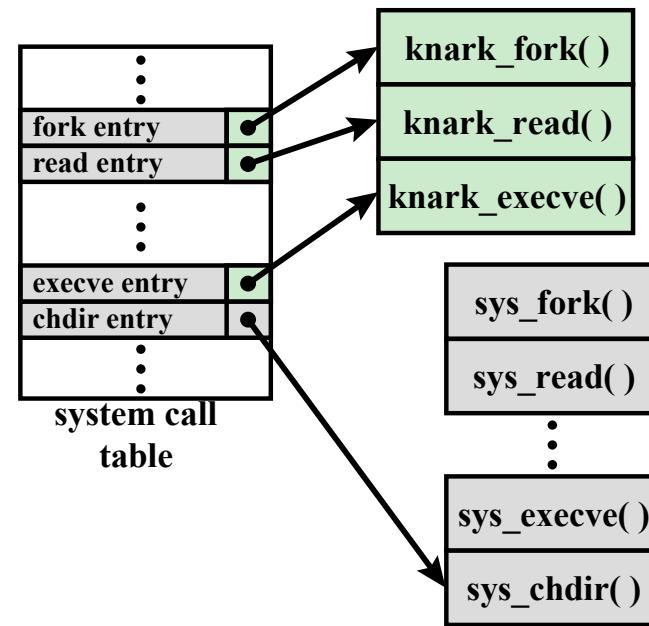
Kernel mode

Virtual
machine
based

External mode



(a) Normal kernel memory layout



(b) After nkark install

Figure 6.3 System Call Table Modification by Rootkit

Malware Countermeasure Approaches

- Ideal solution to the threat of malware is prevention

Four main elements of prevention:

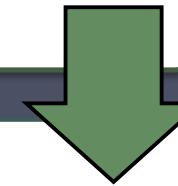
- Policy
- Awareness
- Vulnerability mitigation
- Threat mitigation

- If prevention fails, technical mechanisms can be used to support the following threat mitigation options:
 - Detection
 - Identification
 - Removal

Generations of Anti-Virus Software

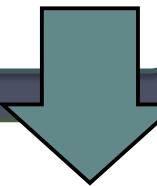
First generation: simple scanners

- Requires a malware signature to identify the malware
- Limited to the detection of known malware



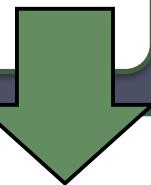
Second generation: heuristic scanners

- Uses heuristic rules to search for probable malware instances
- Another approach is integrity checking



Third generation: activity traps

- Memory-resident programs that identify malware by its actions rather than its structure in an infected program



Fourth generation: full-featured protection

- Packages consisting of a variety of anti-virus techniques used in conjunction
- Include scanning and activity trap components and access control capability

Sandbox Analysis

- Running potentially malicious code in an emulated sandbox or on a virtual machine
- Allows the code to execute in a controlled environment where its behavior can be closely monitored without threatening the security of a real system
- Running potentially malicious software in such environments enables the detection of complex encrypted, polymorphic, or metamorphic malware
- The most difficult design issue with sandbox analysis is to determine how long to run each interpretation

Host-Based Behavior-Blocking Software

- Integrates with the operating system of a host computer and monitors program behavior in real time for malicious action
 - Blocks potentially malicious actions before they have a chance to affect the system
 - Blocks software in real time so it has an advantage over anti-virus detection techniques such as fingerprinting or heuristics

Limitations

- Because malicious code must run on the target machine before all its behaviors can be identified, it can cause harm before it has been detected and blocked

Perimeter Scanning Approaches

- Anti-virus software typically included in e-mail and Web proxy services running on an organization's firewall and IDS
- May also be included in the traffic analysis component of an IDS
- May include intrusion prevention measures, blocking the flow of any suspicious traffic
- Approach is limited to scanning malware

Ingress monitors

Located at the border between the enterprise network and the Internet

Egress monitors

Located at the egress point of individual LANs as well as at the border between the enterprise network and the Internet

One technique is to look for incoming traffic to unused local IP addresses

Monitors outgoing traffic for signs of scanning or other suspicious behavior

Two types of monitoring software

Summary

- Types of malicious software (malware)
 - Broad classification of malware
 - Attack kits
 - Attack sources
- Advanced persistent threat
- Propagation-vulnerability exploit-worms
 - Target discovery
 - Worm propagation model
 - The Morris Worm
 - Brief history of worm attacks
 - State of worm technology
 - Mobile code
 - Mobile phone worms
 - Client-side vulnerabilities
 - Drive-by-downloads
 - Clickjacking
- Payload-stealththing-backdoors, rootkits
 - Backdoor
 - Rootkit
 - Kernel mode rootkits
 - Virtual machine and other external rootkits
- Propagation-social engineering-span E-mail, Trojans
 - Spam E-mail
 - Trojan horses
 - Mobile phone Trojans
- Payload-system corruption
 - Data destruction
 - Real-world damage
 - Logic bomb
- Payload-attack agent-zombie, bots
 - Uses of bots
 - Remote control facility
- Payload-information theft-keyloggers, phishing, spyware
 - Credential theft, keyloggers, and spyware
 - Phishing and identity theft
 - Reconnaissance, espionage, and data exfiltration
- Countermeasures
 - Malware countermeasure approaches
 - Host-based scanners
 - Signature-based anti-virus
 - Perimeter scanning approaches
 - Distributed intelligence gathering approaches

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 8

Intrusion Detection

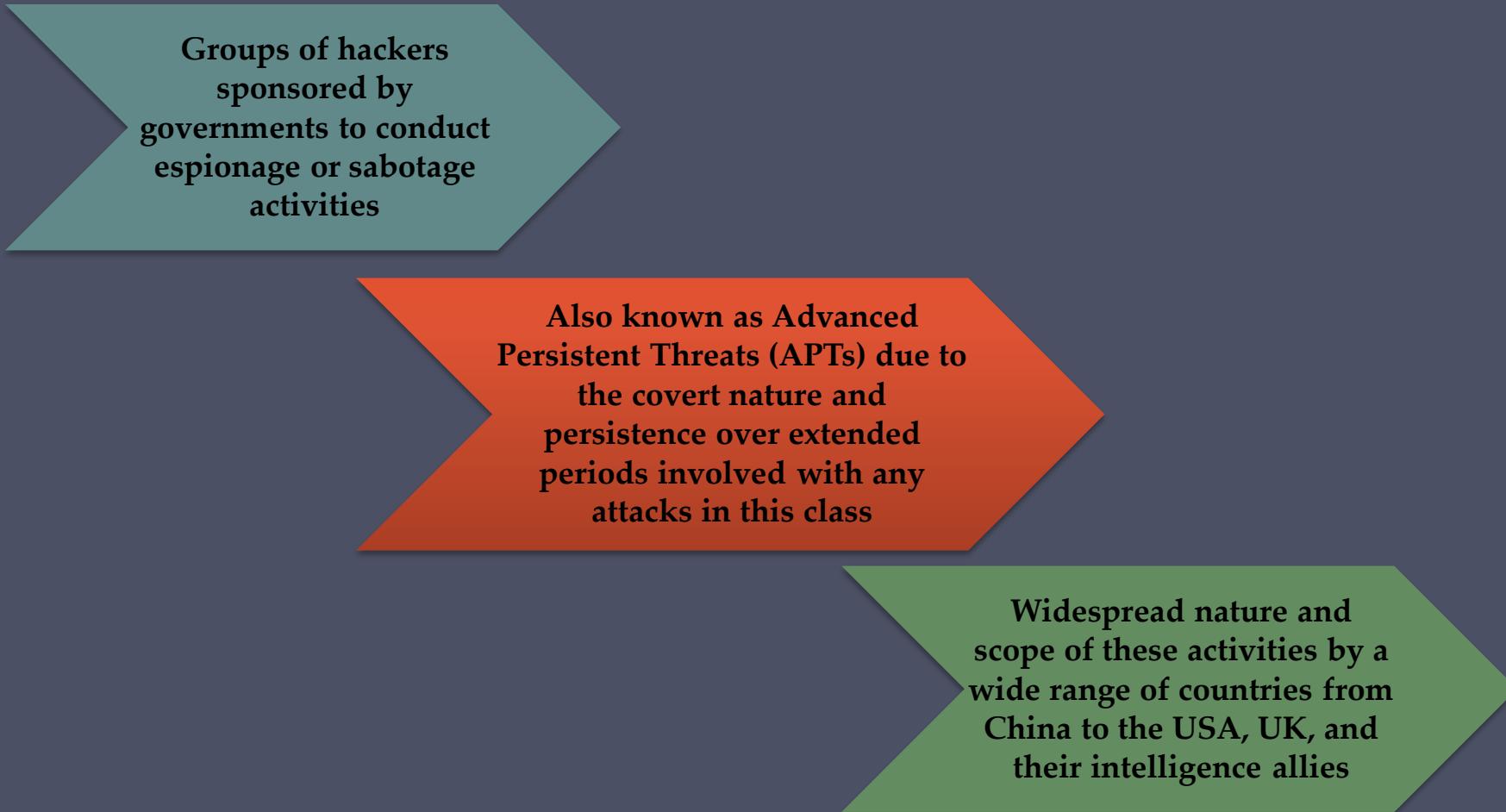
Classes of Intruders – Cyber Criminals

- Individuals or members of an organized crime group with a goal of financial reward
- Their activities may include:
 - Identity theft
 - Theft of financial credentials
 - Corporate espionage
 - Data theft
 - Data ransoming
- Typically they are young, often Eastern European, Russian, or southeast Asian hackers, who do business on the Web
- They meet in underground forums to trade tips and data and coordinate attacks

Classes of Intruders – Activists

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also known as hacktivists
 - Skill level is often quite low
- Aim of their attacks is often to promote and publicize their cause typically through:
 - Website defacement
 - Denial of service attacks
 - Theft and distribution of data that results in negative publicity or compromise of their targets

Classes of Intruders – State-Sponsored Organizations



Groups of hackers sponsored by governments to conduct espionage or sabotage activities

Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class

Widespread nature and scope of these activities by a wide range of countries from China to the USA, UK, and their intelligence allies

Classes of Intruders – Others

- Hackers with motivations other than those previously listed
- Include classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation
- Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class
- Given the wide availability of attack toolkits, there is a pool of “hobby hackers” using them to explore system and network security

Intruder Skill Levels – Apprentice

- Hackers with minimal technical skill who primarily use existing attack toolkits
- They likely comprise the largest number of attackers, including many criminal and activist attackers
- Given their use of existing known tools, these attackers are the easiest to defend against
- Also known as “script-kiddies” due to their use of existing scripts (tools)

Intruder Skill Levels – Journeymen

- Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities
- They may be able to locate new vulnerabilities to exploit that are similar to some already known
- Hackers with such skills are likely found in all intruder classes
- Adapt tools for use by others

Intruder Skill Levels – Master

- Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities
- Write new powerful attack toolkits
- Some of the better known classical hackers are of this level
- Some are employed by state-sponsored organizations
- Defending against these attacks is of the highest difficulty

Examples of Intrusion

- Remote root compromise
- Web server defacement
- Guessing/cracking passwords
- Copying databases containing credit card numbers
- Viewing sensitive data without authorization
- Running a packet sniffer
- Distributing pirated software
- Using an unsecured modem to access internal network
- Impersonating an executive to get information
- Using an unattended workstation

Intruder Behavior

Target acquisition
and information
gathering

Initial access

Privilege
escalation

Information
gathering or
system exploit

Maintaining
access

Covering tracks

(a) Target Acquisition and Information Gathering

- Explore corporate website for information on corporate structure, personnel, key systems, as well as details of specific web server and OS used.
- Gather information on target network using DNS lookup tools such as dig, host, and others; and query WHOIS database.
- Map network for accessible services using tools such as NMAP.
- Send query email to customer service contact, review response for information on mail client, server, and OS used, and also details of person responding.
- Identify potentially vulnerable services, eg vulnerable web CMS.

(b) Initial Access

- Brute force (guess) a user's web content management system (CMS) password.
- Exploit vulnerability in web CMS plugin to gain system access.
- Send spear-phishing email with link to web browser exploit to key people.

(c) Privilege Escalation

- Scan system for applications with local exploit.
- Exploit any vulnerable application to gain elevated privileges.
- Install sniffers to capture administrator passwords.
- Use captured administrator password to access privileged information.

(d) Information Gathering or System Exploit

- Scan files for desired information.
- Transfer large numbers of documents to external repository.
- Use guessed or captured passwords to access other servers on network.

(e) Maintaining Access

- Install remote administration tool or rootkit with backdoor for later access.
- Use administrator password to later access network.
- Modify or disable anti-virus or IDS programs running on system.

(f) Covering Tracks

- Use rootkit to hide files installed on system.
- Edit logfiles to remove entries generated during the intrusion.

Table 8.1

Examples of Intruder Behavior

(Table can be found on pages 255-256 in the textbook.)

Definitions

- Security Intrusion:

Unauthorized act of bypassing the security mechanisms of a system

- Intrusion Detection:

A hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions

Intrusion Detection System (IDS)

- Host-based IDS (HIDS)
 - Monitors the characteristics of a single host for suspicious activity
- Network-based IDS (NIDS)
 - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity
- Distributed or hybrid IDS
 - Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity

Comprises three logical components:

- **Sensors - collect data**
- **Analyzers - determine if intrusion has occurred**
- **User interface - view output or control system behavior**

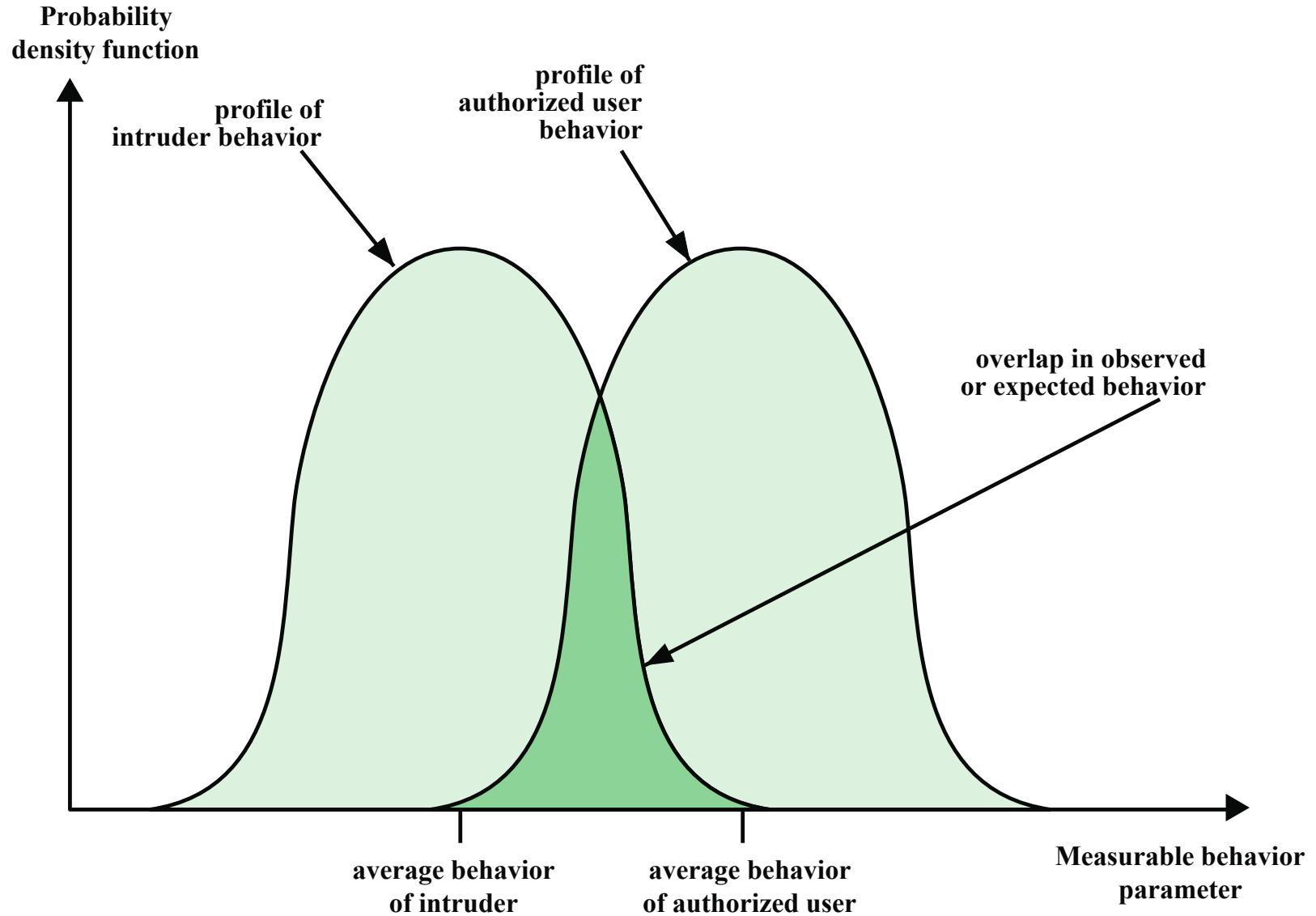


Figure 8.1 Profiles of Behavior of Intruders and Authorized Users

IDS Requirements

Run continually

Be fault tolerant

Resist subversion

Impose a minimal overhead on system

Configured according to system security policies

Adapt to changes in systems and users

Scale to monitor large numbers of systems

Provide graceful degradation of service

Allow dynamic reconfiguration

Analysis Approaches

Anomaly detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Signature/Heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

Anomaly Detection

A variety of classification approaches are used:

Statistical	Knowledge based	Machine-learning
<ul style="list-style-type: none">• Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics	<ul style="list-style-type: none">• Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior	<ul style="list-style-type: none">• Approaches automatically determine a suitable classification model from the training data using data mining techniques

Signature or Heuristic Detection

Signature approaches

Match a large collection of known patterns of malicious data against data stored on a system or in transit over a network

The signatures need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data

Widely used in anti-virus products, network traffic scanning proxies, and in NIDS

Rule-based heuristic identification

Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage

Typically rules used are specific

SNORT is an example of a rule-based NIDS

Host-Based Intrusion Detection (HIDS)

- Adds a specialized layer of security software to vulnerable or sensitive systems
- Can use either anomaly or signature and heuristic approaches
- Monitors activity to detect suspicious behavior
 - Primary purpose is to detect intrusions, log suspicious events, and send alerts
 - Can detect both external and internal intrusions

Data Sources and Sensors



A fundamental component of intrusion detection is the sensor that collects data

Common data sources include:

- System call traces
- Audit (log file) records
- File integrity checksums
- Registry access

Table 8.2

Linux System Calls and Windows DLLs Monitored

(a) Ubuntu Linux System Calls

```
accept, access, acct, adjtime, aiocancel, aioread, aiowait, aiowrite, alarm, async_daemon,  
auditsys, bind, chdir, chmod, chown, chroot, close, connect, creat, dup, dup2, execv, execve,  
exit, exportfs, fchdir, fchmod, fchown, fchroot, fcntl, flock, fork, fpathconf, fstat, fstat,  
fstatfs, fsync, ftime, ftruncate, getdents, getdirent, getdomainname, getopt, getdtsize,  
getfh, getgid, getgroups, gethostid, gethostname, getitimer, getmsg, getpagesize,  
getpeername, getpgrp, getpid, getpriority, getrlimit, getrusage, getsockname, getsockopt,  
gettimeofday, getuid, gtty, ioctl, kill, killpg, link, listen, lseek, lstat, madvise, mctl, mincore,  
mkdir, mknod, mmap, mount, mount, mprotect, mpxchan, msgsyst, msync, munmap,  
nfs_mount, nfssvc, nice, open, pathconf, pause, pcfs_mount, phys, pipe, poll, profil, ptrace,  
putmsg, quota, quotactl, read, readlink, ready, reboot, recv, recvfrom, recvmsg, rename,  
resuba, rfssys, rmdir, sbreak, sbrk, select, semsys, send, sendmsg, sendto, setdomainname,  
setsockopt, setgroup, sethostid, sethostname, setitimer, setpgid, setpgrp, setpgrp,  
setpriority, setquota, setregid, setreuid, setrlimit, setsid, setsockopt, gettimeofday, setuid,  
shmsys, shutdown, sigblock, sigpause, sigpending, sigsetmask, sigstack, sigsys, sigvec,  
socket, socketaddr, socketpair, sstk, stat, stat, statfs, stime, stty, swapon, symlink, sync,  
sysconf, time, times, truncate, umask, umount, uname, unlink, unmount, ust, utime, utimes,  
vadvise, vfork, vhangup, vlimit, vpixsys, vread, vtimes, vtrace, vwrite, wait, wait3, wait4,  
write, writev
```

(b) Key Windows DLLs and Executables

```
comctl32  
kernel32  
msvcpp  
msvcrt  
mswsock  
ntdll  
ntoskrnl  
user32  
ws2_32
```

(Table can be found on page 264 in the textbook)

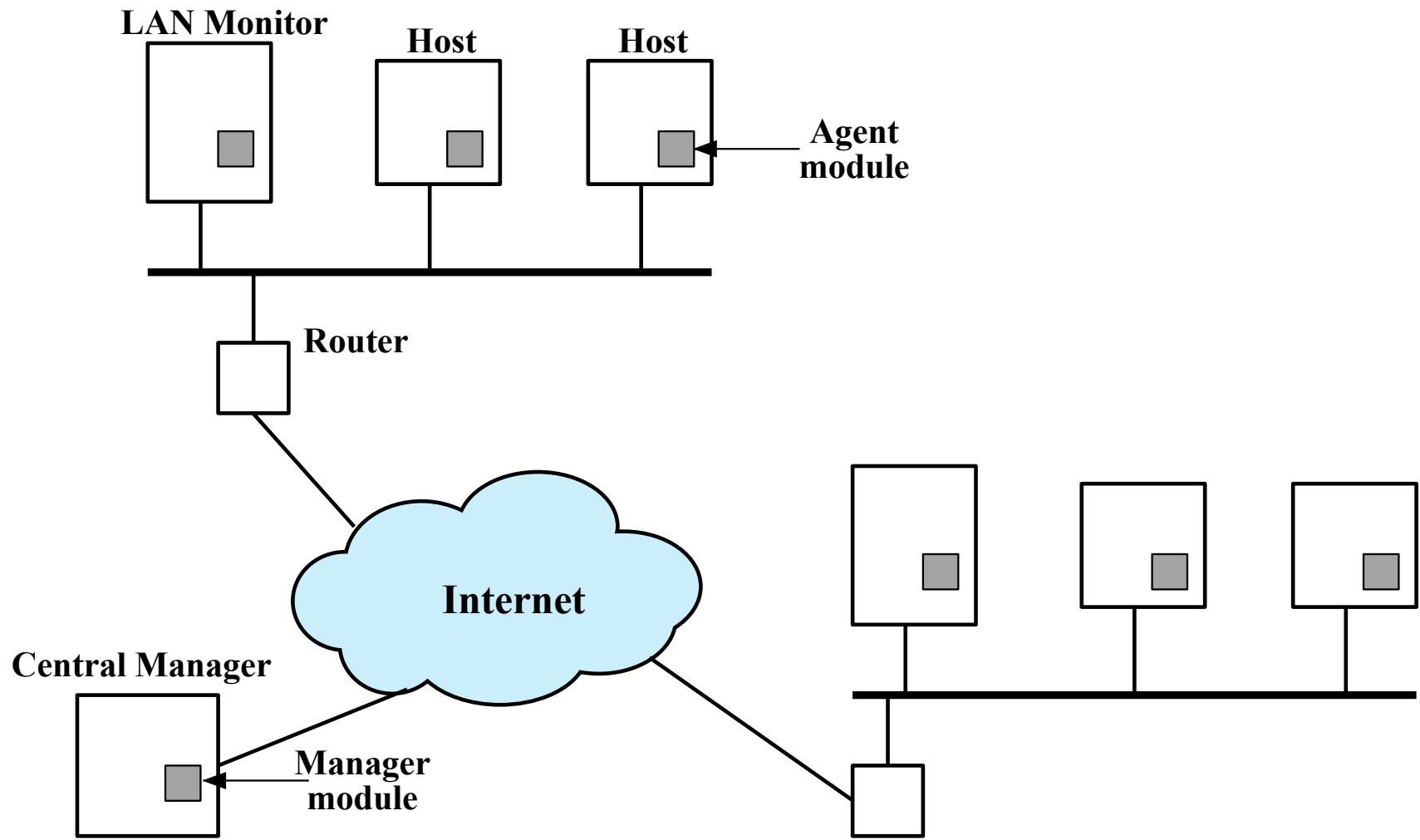


Figure 8.2 Architecture for Distributed Intrusion Detection

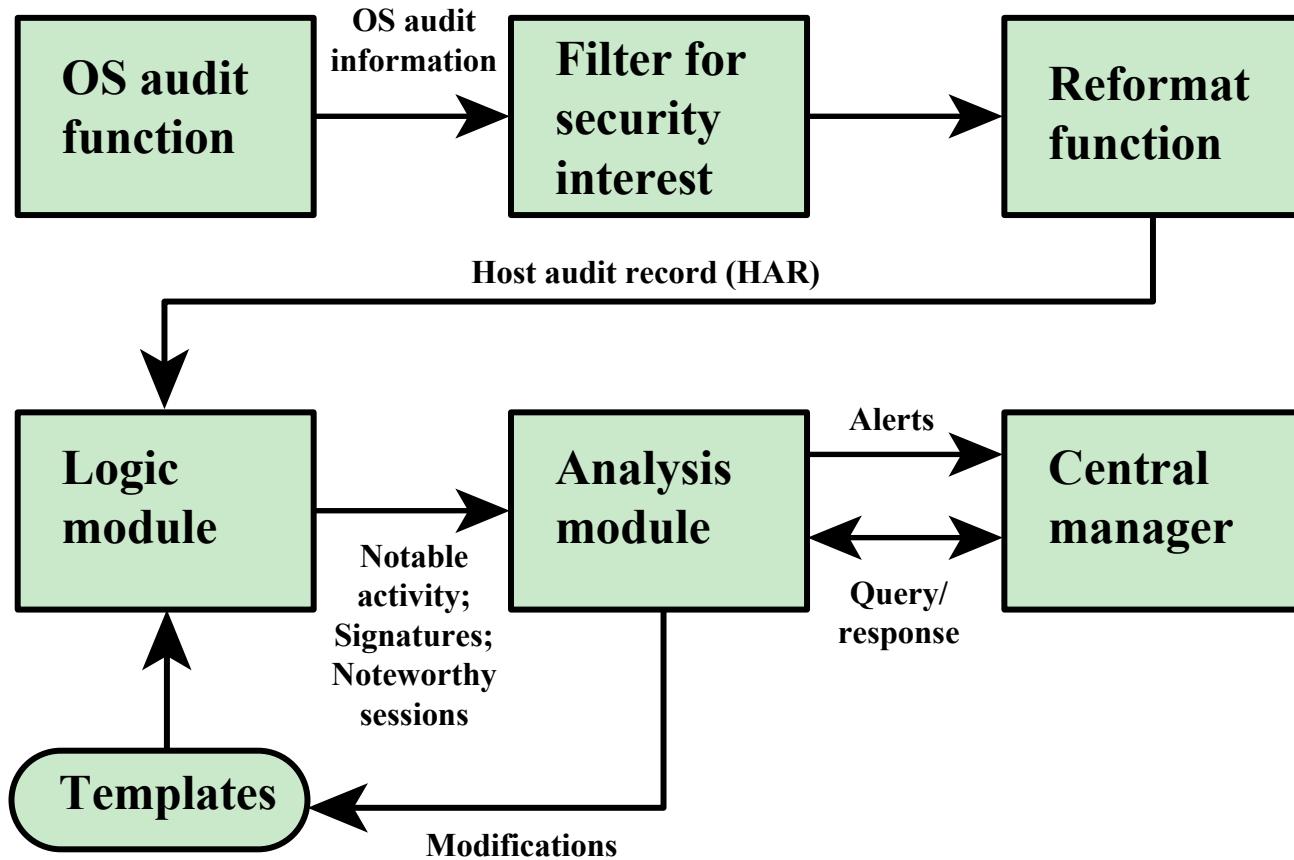


Figure 8.3 Agent Architecture

Network-Based IDS (NIDS)

Monitors traffic at selected points on a network

Examines traffic packet by packet in real or close to real time

May examine network, transport, and/or application-level protocol activity

Comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface

Analysis of traffic patterns may be done at the sensor, the management server or a combination of the two

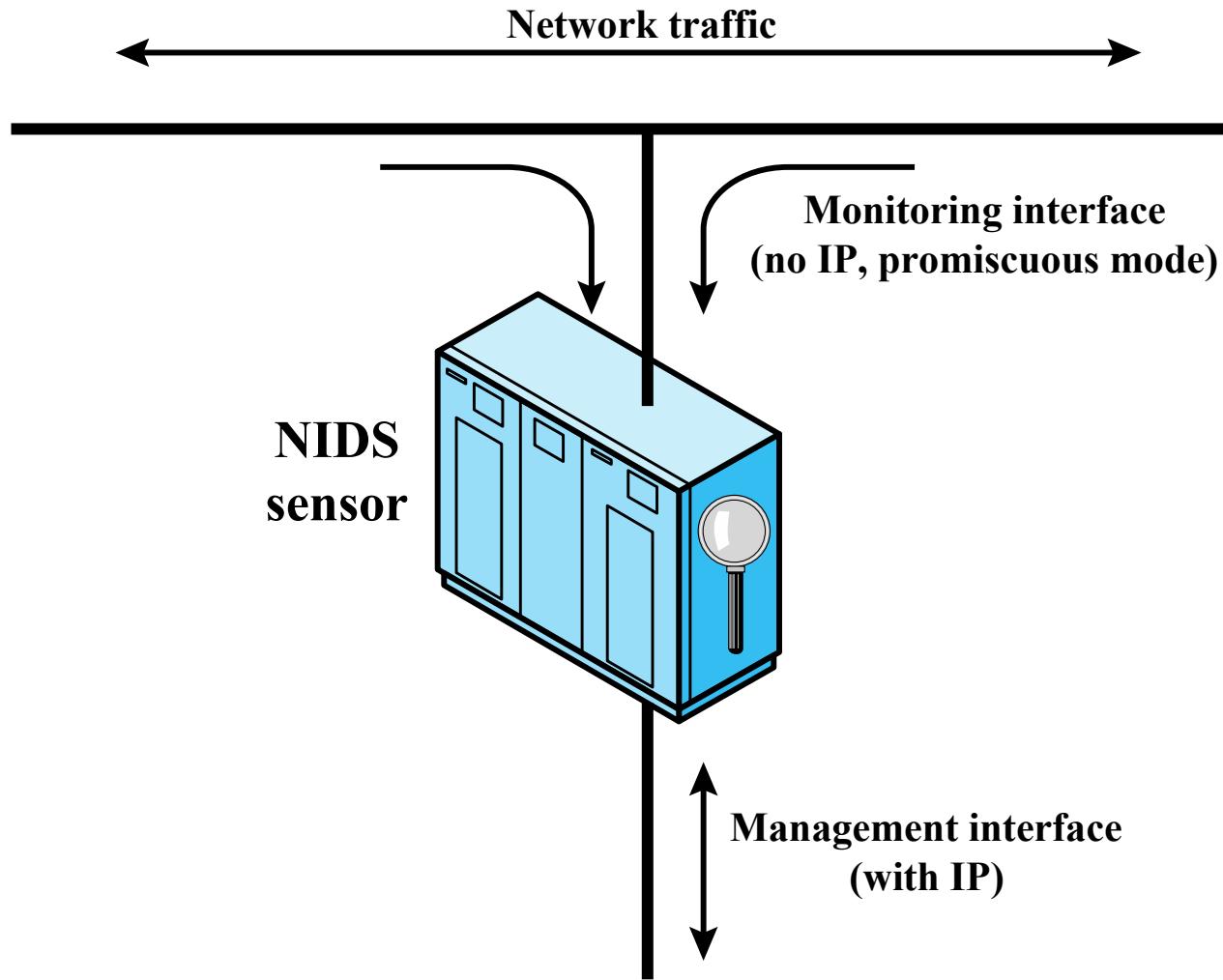


Figure 8.4 Passive NIDS Sensor

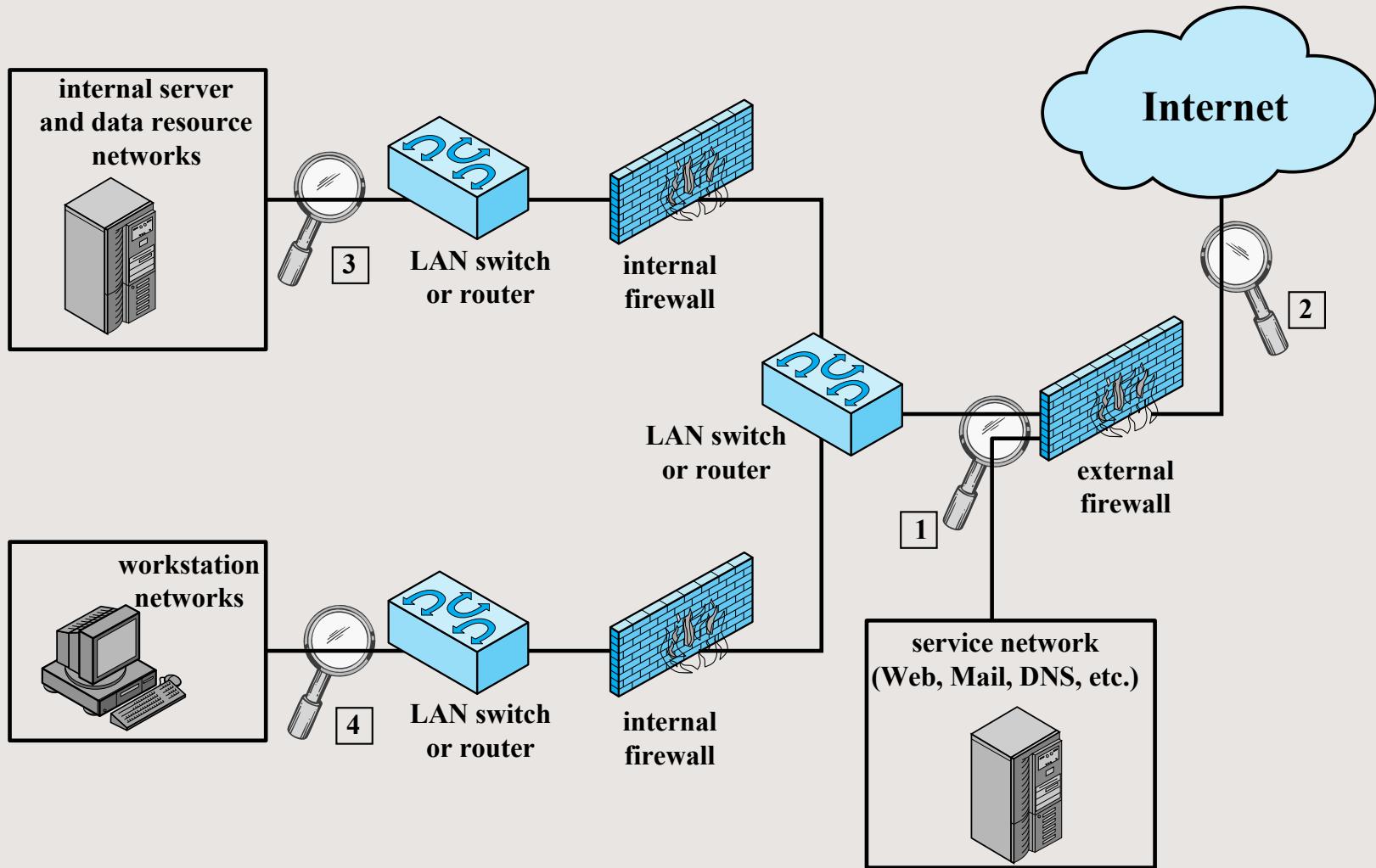


Figure 8.5 Example of NIDS Sensor Deployment

Intrusion Detection Techniques

Attacks suitable for
Signature detection

- Application layer reconnaissance and attacks
- Transport layer reconnaissance and attacks
- Network layer reconnaissance and attacks
- Unexpected application services
- Policy violations

Attacks suitable for
Anomaly detection

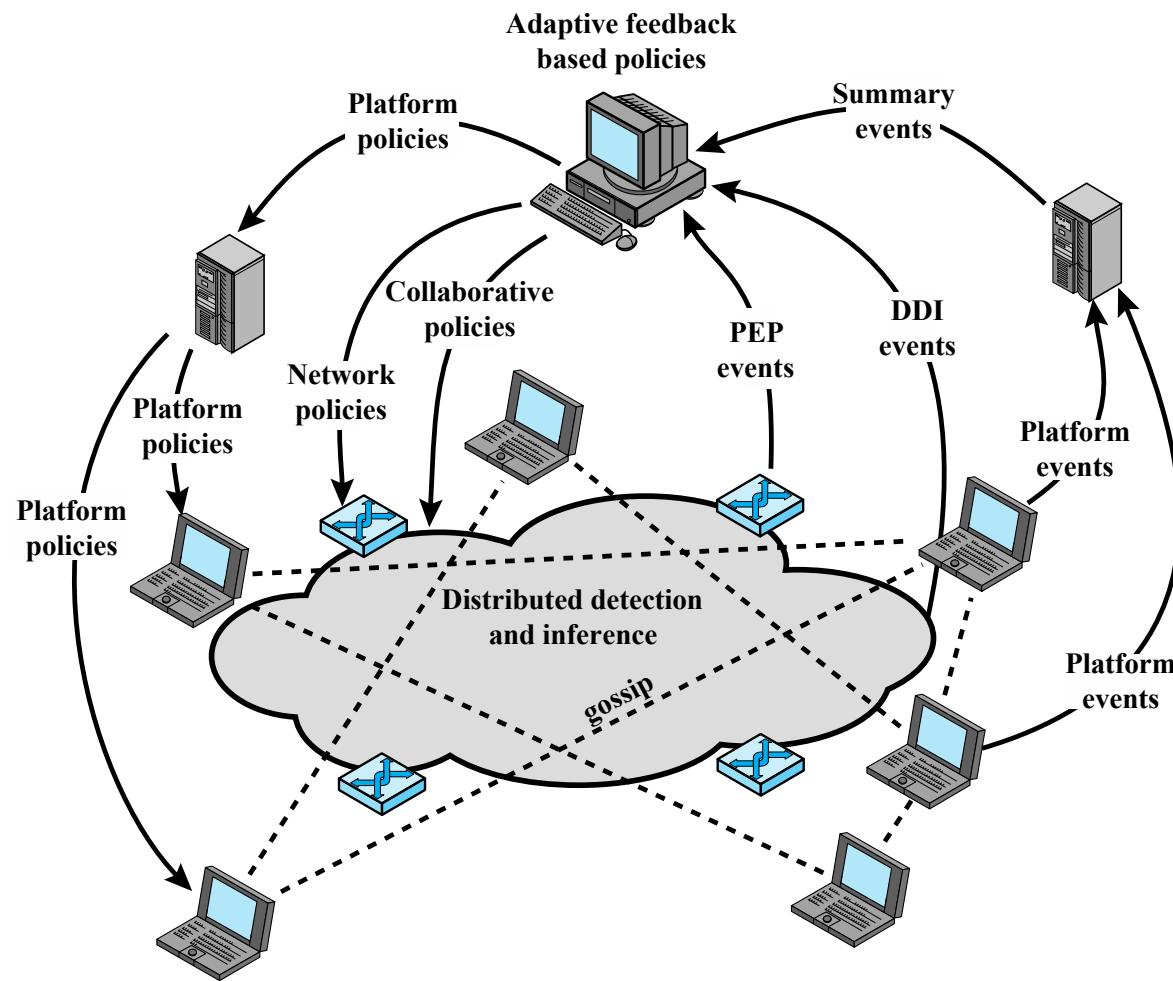
- Denial-of-service (DoS) attacks
- Scanning
- Worms

Stateful Protocol Analysis (SPA)

- Subset of anomaly detection that compares observed network traffic against predetermined universal vendor supplied profiles of benign protocol traffic
 - This distinguishes it from anomaly techniques trained with organization specific traffic protocols
- Understands and tracks network, transport, and application protocol states to ensure they progress as expected
- A key disadvantage is the high resource use it requires

Logging of Alerts

- Typical information logged by a NIDS sensor includes:
 - Timestamp
 - Connection or session ID
 - Event or alert type
 - Rating
 - Network, transport, and application layer protocols
 - Source and destination IP addresses
 - Source and destination TCP or UDP ports, or ICMP types and codes
 - Number of bytes transmitted over the connection
 - Decoded payload data, such as application requests and responses
 - State-related information



PEP = policy enforcement point
DDI = distributed detection and inference

Figure 8.6 Overall Architecture of an Autonomic Enterprise Security System

IETF Intrusion Detection Working Group

- Purpose is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to management systems that may need to interact with them
- The working group issued the following RFCs in 2007:

Intrusion Detection Message Exchange Requirements (RFC 4766)

- Document defines requirements for the Intrusion Detection Message Exchange Format (IDMEF)
- Also specifies requirements for a communication protocol for communicating IDMEF

The Intrusion Detection Message Exchange Format (RFC 4765)

- Document describes a data model to represent information exported by intrusion detection systems and explains the rationale for using this model
- An implementation of the data model in the Extensible Markup Language (XML) is presented, and XML Document Type Definition is developed, and examples are provided

The Intrusion Detection Exchange Protocol (RFC 4767)

- Document describes the Intrusion Detection Exchange Protocol (IDXP), an application level protocol for exchanging data between intrusion detection entities
- IDXP supports mutual authentication, integrity, and confidentiality over a connection oriented protocol

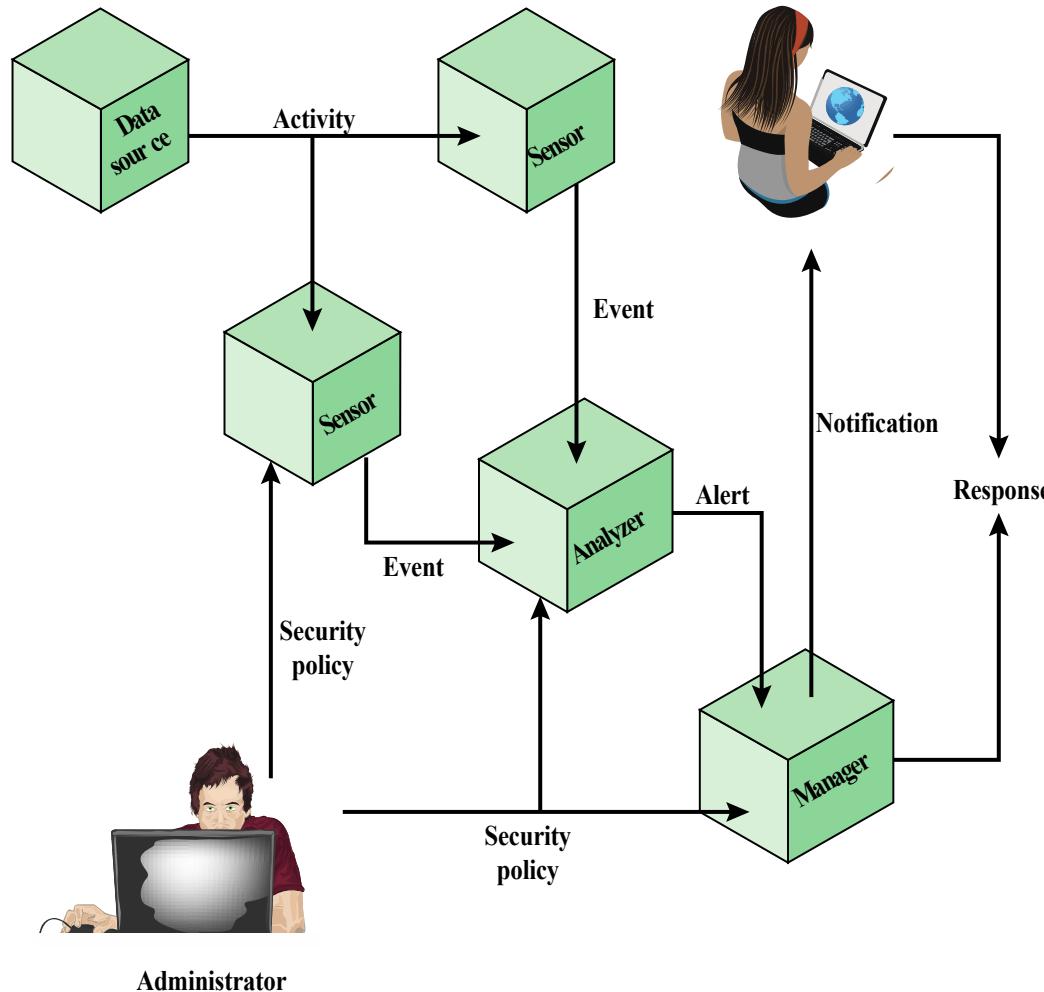


Figure 8.7 Model For Intrusion Detection Message Exchange

Honeypots

- Decoy systems designed to:
 - Lure a potential attacker away from critical systems
 - Collect information about the attacker's activity
 - Encourage the attacker to stay on the system long enough for administrators to respond
- Systems are filled with fabricated information that a legitimate user of the system wouldn't access
- Resources that have no production value
 - Therefore incoming communication is most likely a probe, scan, or attack
 - Initiated outbound communication suggests that the system has probably been compromised

Honeypot Classifications

- Low interaction honeypot
 - Consists of a software package that emulates particular IT services or systems well enough to provide a realistic initial interaction, but does not execute a full version of those services or systems
 - Provides a less realistic target
 - Often sufficient for use as a component of a distributed IDS to warn of imminent attack
- High interaction honeypot
 - A real system, with a full operating system, services and applications, which are instrumented and deployed where they can be accessed by attackers
 - Is a more realistic target that may occupy an attacker for an extended period
 - However, it requires significantly more resources
 - If compromised could be used to initiate attacks on other systems

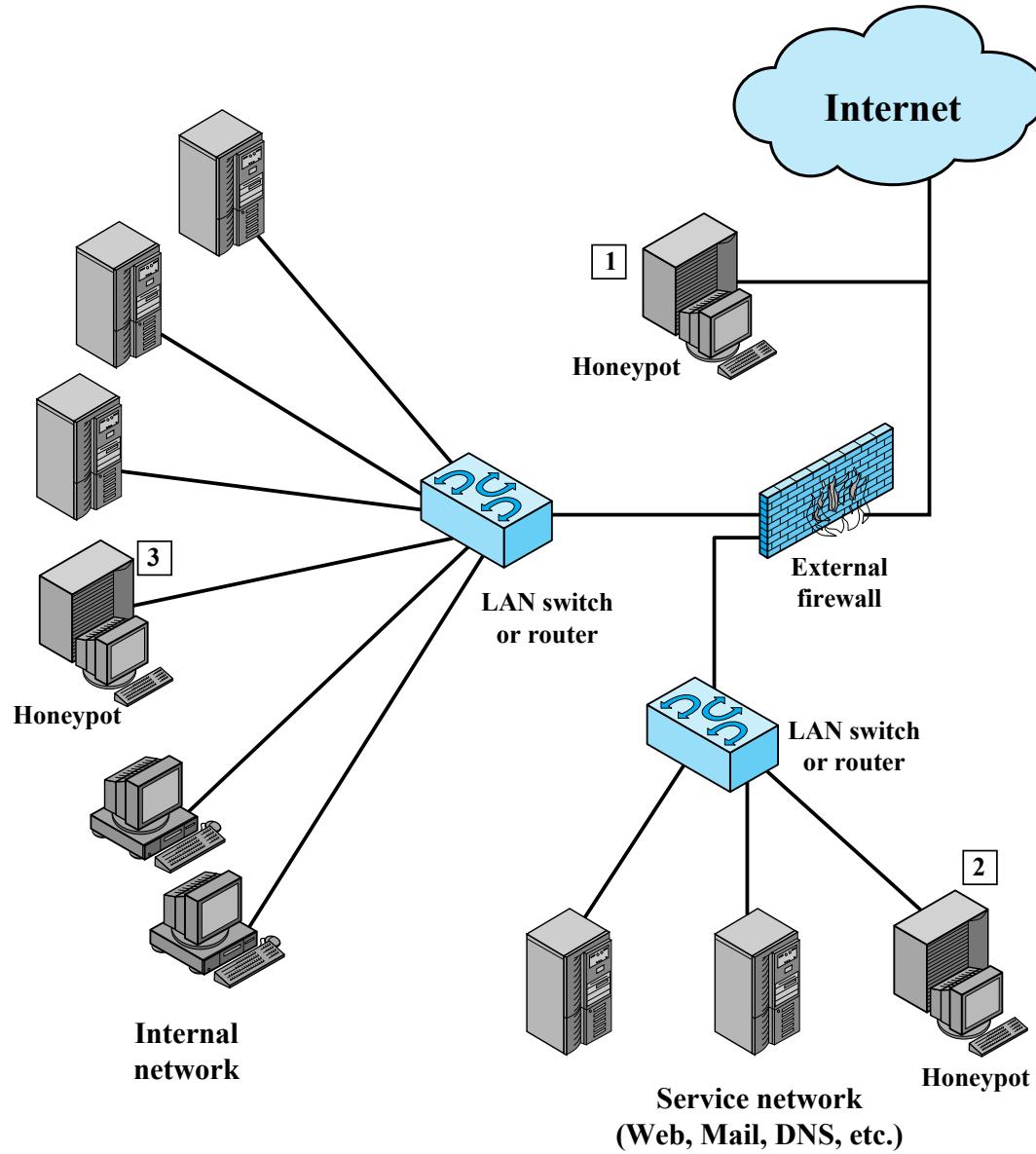


Figure 8.8 Example of Honeypot Deployment

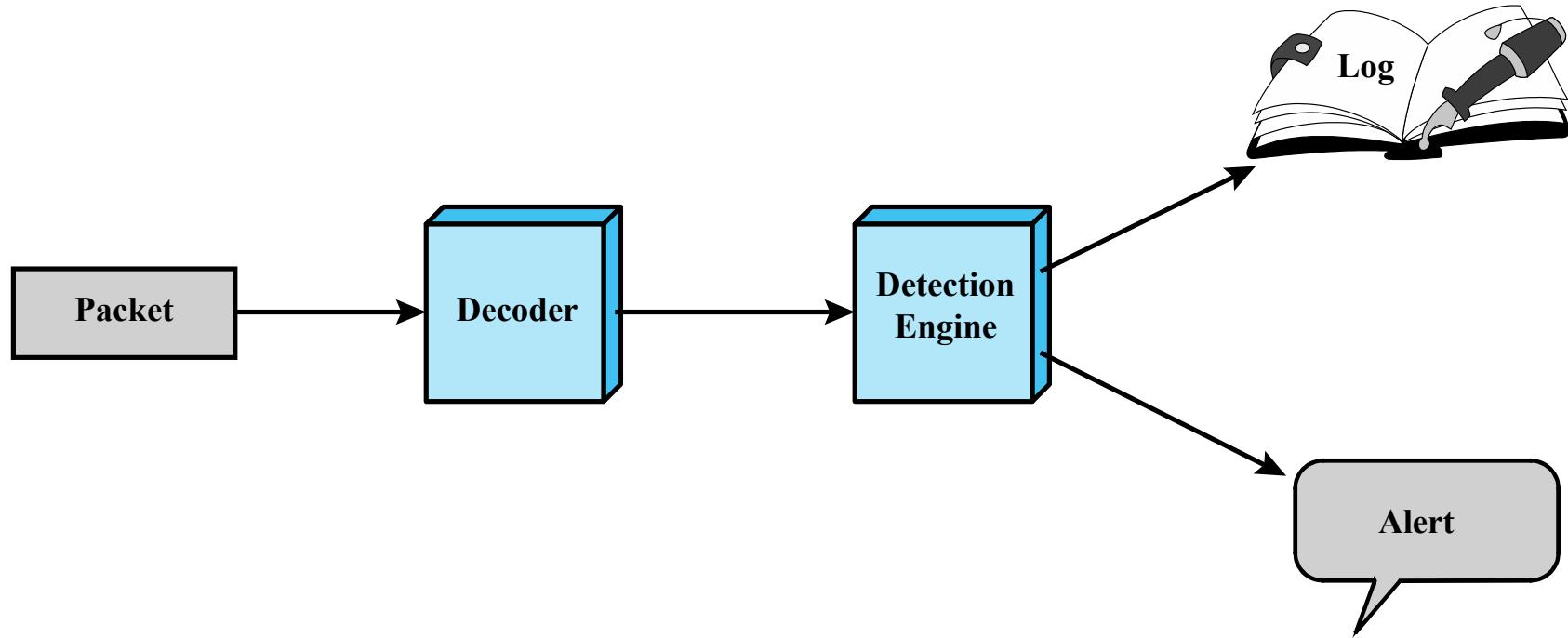


Figure 8.9 Snort Architecture

Action	Protocol	Source IP address	Source Port	Direction	Dest IP address	Dest Port
--------	----------	-------------------	-------------	-----------	-----------------	-----------

(a) Rule Header

Option Keyword	Option Arguments	• • •
----------------	------------------	-------

(b) Options

Figure 8.10 Snort Rule Formats

Table 8.3

Snort Rule Actions

Action	Description
alert	Generate an alert using the selected alert method, and then log the packet.
log	Log the packet.
pass	Ignore the packet.
activate	Alert and then turn on another dynamic rule.
dynamic	Remain idle until activated by an activate rule , then act as a log rule.
drop	Make iptables drop the packet and log the packet.
reject	Make iptables drop the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
sdrop	Make iptables drop the packet but does not log it.

meta-data	
msg	Defines the message to be sent when a packet generates an event.
reference	Defines a link to an external attack identification system, which provides additional information.
classtype Indicates what type of attack the packet attempted.	
payload	
content	Enables Snort to perform a case-sensitive search for specific content (text and/or binary) in the packet payload.
depth	Specifies how far into a packet Snort should search for the specified pattern. Depth modifies the previous content keyword in the rule.
offset	Specifies where to start searching for a pattern within a packet. Offset modifies the previous content keyword in the rule.
nocase	Snort should look for the specific pattern, ignoring case. Nocase modifies the previous content keyword in the rule.
non-payload	
ttl	Check the IP time-to-live value. This option was intended for use in the detection of traceroute attempts.
id	Check the IP ID field for a specific value. Some tools (exploits, scanners and other odd programs) set this field specifically for various purposes, for example, the value 31337 is very popular with some hackers.
dsize	Test the packet payload size. This may be used to check for abnormally sized packets. In many cases, it is useful for detecting buffer overflows.
flags	Test the TCP flags for specified settings.
seq	Look for a specific TCP header sequence number.
icmp-id	Check for a specific ICMP ID value. This is useful because some covert channel programs use static ICMP fields when they communicate. This option was developed to detect the stacheldraht DDoS agent.
post-detection	
logto	Log packets matching the rule to the specified filename.
session	Extract user data from TCP Sessions. There are many cases where seeing what users are typing in telnet, rlogin, ftp, or even web sessions is very useful.

Table 8.4

Examples of Snort Rule Options

(Table can be found on page 283 in textbook.)

Summary

- Intruders
 - Intruder behavior
- Intrusion detection
 - Basic principles
 - The base-rate fallacy
 - Requirements
- Analysis approaches
 - Anomaly detection
 - Signature or heuristic detection
- Distributed or hybrid intrusion detection
- Intrusion detection exchange format
- Honeypots
- Host-based intrusion detection
 - Data sources and sensors
 - Anomaly HIDS
 - Signature or heuristic HIDS
 - Distributed HIDS
- Network-based intrusion detection
 - Types of network sensors
 - NIDS sensor deployment
 - Intrusion detection techniques
 - Logging of alerts
- Example system:
Snort
 - Snort architecture
 - Snort rules

Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 9

Firewalls and Intrusion Prevention Systems

The Need For Firewalls

- Internet connectivity is essential
 - However it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
 - Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defense
 - Single choke point to impose security and auditing
 - Insulates the internal systems from external networks

Firewall Characteristics

Design goals

All traffic from inside to outside, and vice versa, must pass through the firewall

Only authorized traffic as defined by the local security policy will be allowed to pass

The firewall itself is immune to penetration

Firewall Access Policy

- A critical component in the planning and implementation of a firewall is specifying a suitable access policy
 - This lists the types of traffic authorized to pass through the firewall
 - Includes address ranges, protocols, applications and content types
- This policy should be developed from the organization's information security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support
 - Then refined to detail the filter elements which can then be implemented within an appropriate firewall topology

Firewall Filter Characteristics

- Characteristics that a firewall access policy could use to filter traffic include:

IP address and protocol values

This type of filtering is used by packet filter and stateful inspection firewalls

Typically used to limit access to specific services

Application protocol

This type of filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols

User identity

Typically for inside users who identify themselves using some form of secure authentication technology

Network activity

Controls access based on considerations such as the time or request, rate of requests, or other activity patterns

Firewall Capabilities And Limits

Capabilities:

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as the platform for IPSec

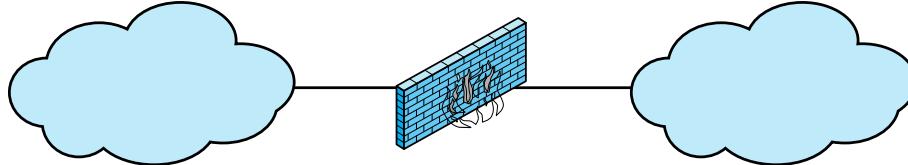
Limitations:

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organization
- Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

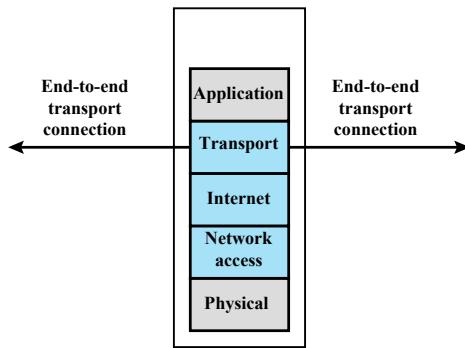
Internal (protected) network
(e.g. enterprise network)

Firewall

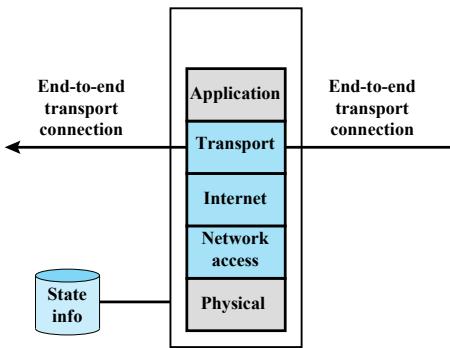
External (untrusted) network
(e.g. Internet)



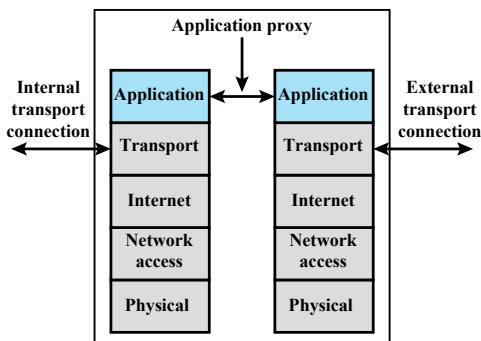
(a) General model



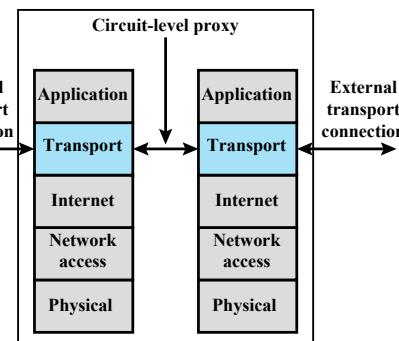
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

Figure 9.1 Types of Firewalls

Packet Filtering Firewall

- Applies rules to each incoming and outgoing IP packet
 - Typically a list of rules based on matches in the IP or TCP header
 - Forwards or discards the packet based on rules match

Filtering rules are based on information contained in a network packet

- Source IP address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- Interface

- Two default policies:
 - Discard - prohibit unless expressly permitted
 - More conservative, controlled, visible to users
 - Forward - permit unless expressly prohibited
 - Easier to manage and use but less secure

Table 9.1

Packet-Filtering Examples

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet Filter

Advantages And Weaknesses

- Advantages
 - Simplicity
 - Typically transparent to users and are very fast
- Weaknesses
 - Cannot prevent attacks that employ application specific vulnerabilities or functions
 - Limited logging functionality
 - Do not support advanced user authentication
 - Vulnerable to attacks on TCP/IP protocol bugs
 - Improper configuration can lead to breaches

Stateful Inspection Firewall

Tightens rules for TCP traffic by creating a directory of outbound TCP connections

- There is an entry for each currently established connection
- Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory

Reviews packet information but also records information about TCP connections

- Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
- Inspects data for protocols like FTP, IM and SIPS commands

Table 9.2

Example Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway

- Also called an application proxy
- Acts as a relay of application-level traffic
 - User contacts gateway using a TCP/IP application
 - User is authenticated
 - Gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application
 - May restrict application features supported
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection

Circuit-Level Gateway

Circuit level proxy

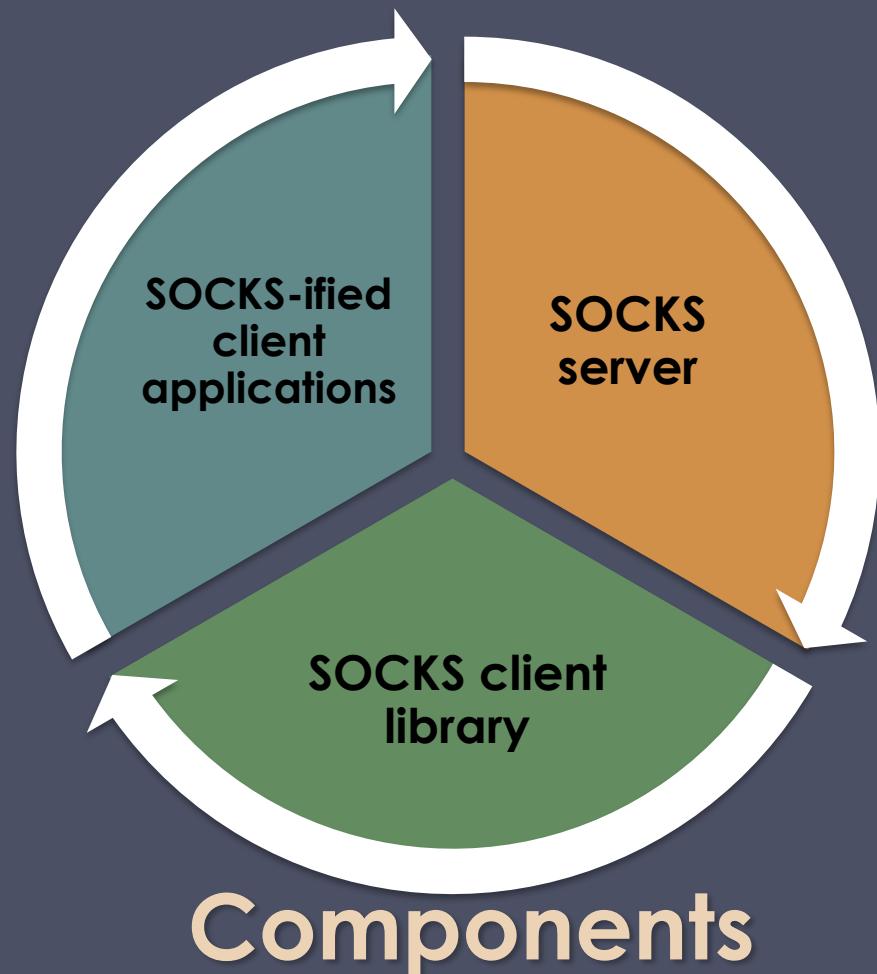
- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
- Relays TCP segments from one connection to the other without examining contents
- Security function consists of determining which connections will be allowed

Typically used when inside users are trusted

- May use application-level gateway inbound and circuit-level gateway outbound
- Lower overheads

SOCKS Circuit-Level Gateway

- SOCKS v5 defined in RFC1928
- Designed to provide a framework for client-server applications in TCP/UDP domains to conveniently and securely use the services of a network firewall
- Client application contacts SOCKS server, authenticates, sends relay request
 - Server evaluates and either establishes or denies the connection



Bastion Hosts

- System identified as a critical strong point in the network's security
- Serves as a platform for an application-level or circuit-level gateway
- Common characteristics:
 - Runs secure O/S, only essential services
 - May require user authentication to access proxy or host
 - Each proxy can restrict features, hosts accessed
 - Each proxy is small, simple, checked for security
 - Each proxy is independent, non-privileged
 - Limited disk use, hence read-only code

Host-Based Firewalls

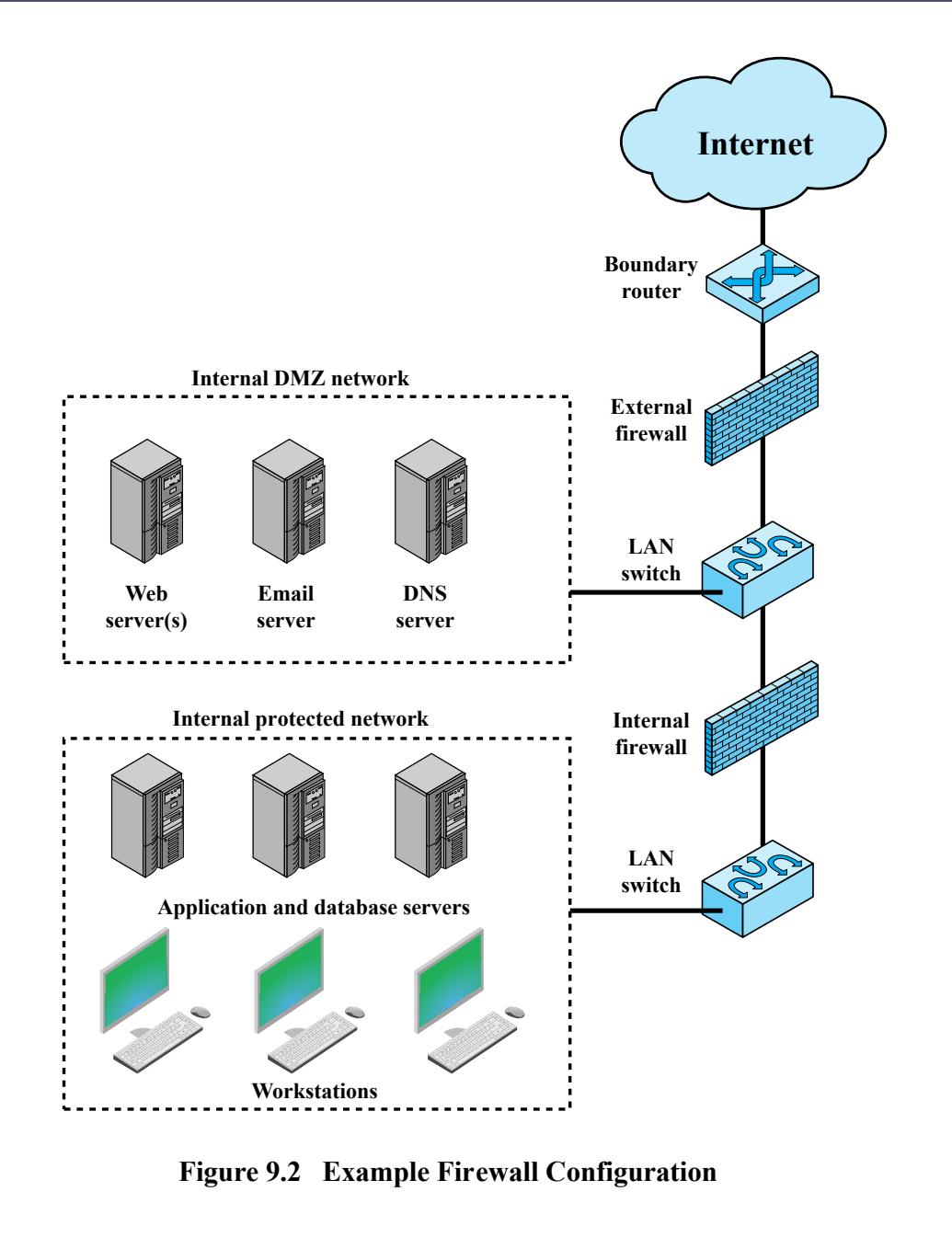
- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Filter and restrict packet flows
- Common location is a server

Advantages:

- Filtering rules can be tailored to the host environment
- Protection is provided independent of topology
- Provides an additional layer of protection

Personal Firewall

- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- For both home or corporate use
- Typically is a software module on a personal computer
- Can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically much less complex than server-based or stand-alone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity



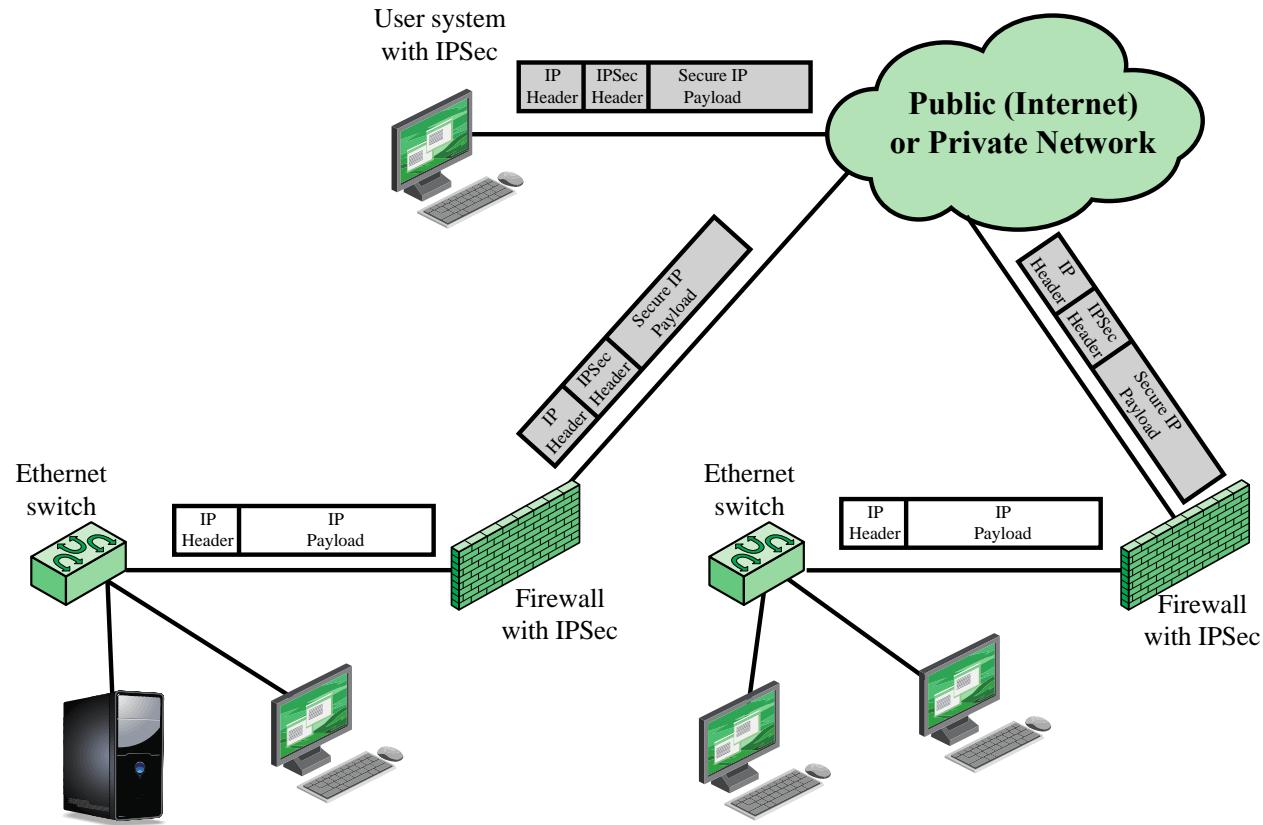


Figure 9.3 A VPN Security Scenario

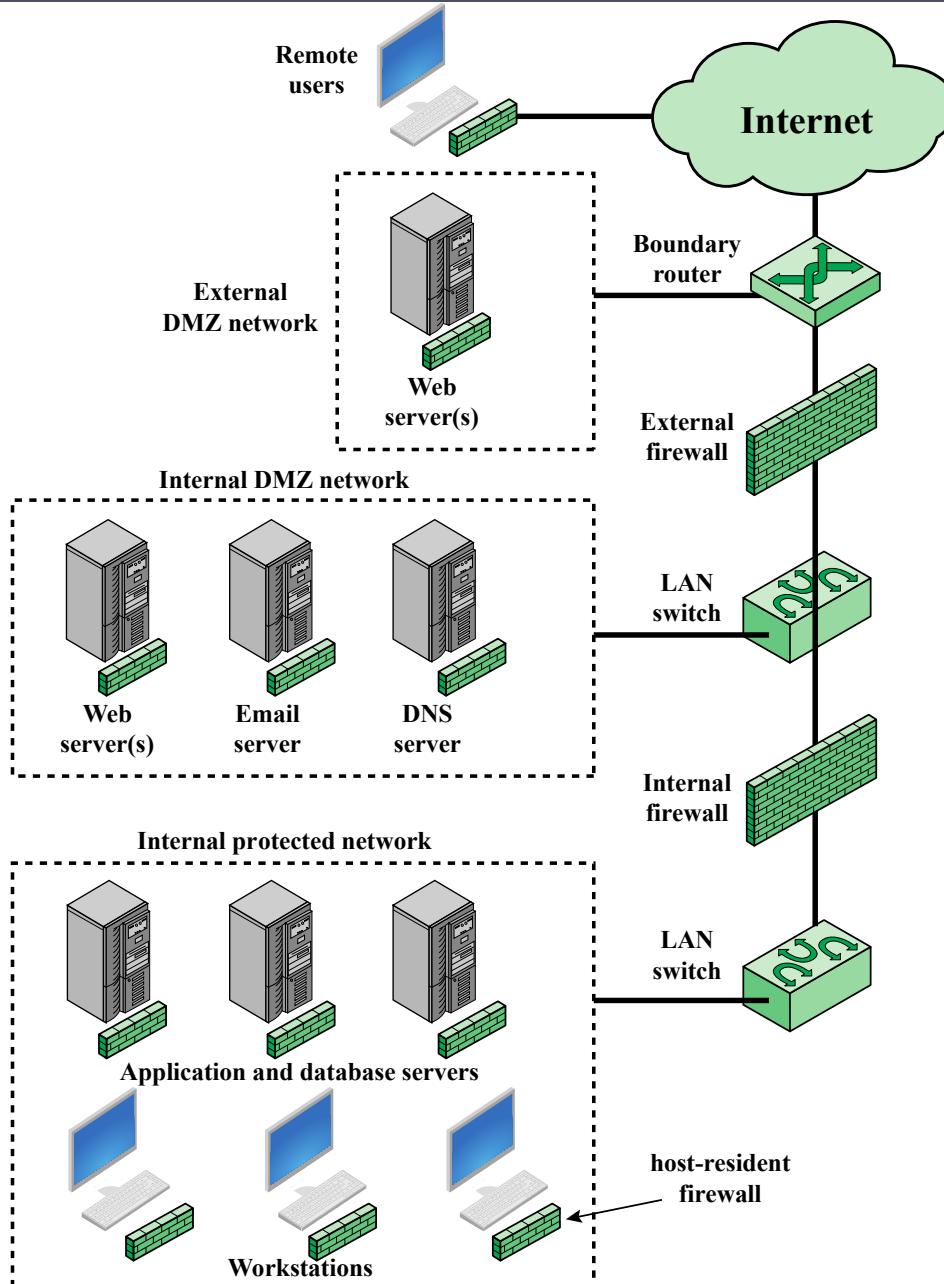


Figure 9.4 Example Distributed Firewall Configuration

Firewall Topologies

Host-resident firewall

- Includes personal firewall software and firewall software on servers

Screening router

- Single router between internal and external networks with stateless or full packet filtering

Single bastion inline

- Single firewall device between an internal and external router

Single bastion T

- Has a third network interface on bastion to a DMZ where externally visible servers are placed

Double bastion inline

- DMZ is sandwiched between bastion firewalls

Double bastion T

- DMZ is on a separate network interface on the bastion firewall

Distributed firewall configuration

- Used by large businesses and government organizations

Intrusion Prevention Systems (IPS)

- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

Host-Based IPS (HIPS)

- Can make use of either signature/heuristic or anomaly detection techniques to identify attacks
 - Signature: focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious
 - Anomaly: IPS is looking for behavior patterns that indicate malware
- Examples of the types of malicious behavior addressed by a HIPS include:
 - Modification of system resources
 - Privilege-escalation exploits
 - Buffer-overflow exploits
 - Access to e-mail contact list
 - Directory traversal

HIPS

- Capability can be tailored to the specific platform
- A set of general purpose tools may be used for a desktop or server system
- Some packages are designed to protect specific types of servers, such as Web servers and database servers
 - In this case the HIPS looks for particular application attacks
- Can use a sandbox approach
 - Sandboxes are especially suited to mobile code such as Java applets and scripting languages
 - HIPS quarantines such code in an isolated system area then runs the code and monitors its behavior
- Areas for which a HIPS typically offers desktop protection:
 - System calls
 - File system access
 - System registry settings
 - Host input/output

The Role of HIPS

- Many industry observers see the enterprise endpoint, including desktop and laptop systems, as now the main target for hackers and criminals
 - Thus security vendors are focusing more on developing endpoint security products
 - Traditionally, endpoint security has been provided by a collection of distinct products, such as antivirus, antispyware, antispam, and personal firewalls
- Approach is an effort to provide an integrated, single-product suite of functions
 - Advantages of the integrated HIPS approach are that the various tools work closely together, threat prevention is more comprehensive, and management is easier
- A prudent approach is to use HIPS as one element in a defense-in-depth strategy that involves network-level devices, such as either firewalls or network-based IPSs

Network-Based IPS (NIPS)

- Inline NIDS with the authority to modify or discard packets and tear down TCP connections
- Makes use of signature/heuristic detection and anomaly detection
- May provide flow data protection
 - Requires that the application payload in a sequence of packets be reassembled
- Methods used to identify malicious packets:

Pattern matching

Stateful matching

Protocol anomaly

Traffic anomaly

Statistical anomaly

Digital Immune System

- Comprehensive defense against malicious behavior caused by malware
- Developed by IBM and refined by Symantec
- Motivation for this development includes the rising threat of Internet-based malware, the increasing speed of its propagation provided by the Internet, and the need to acquire a global view of the situation
- Success depends on the ability of the malware analysis system to detect new and innovative malware strains

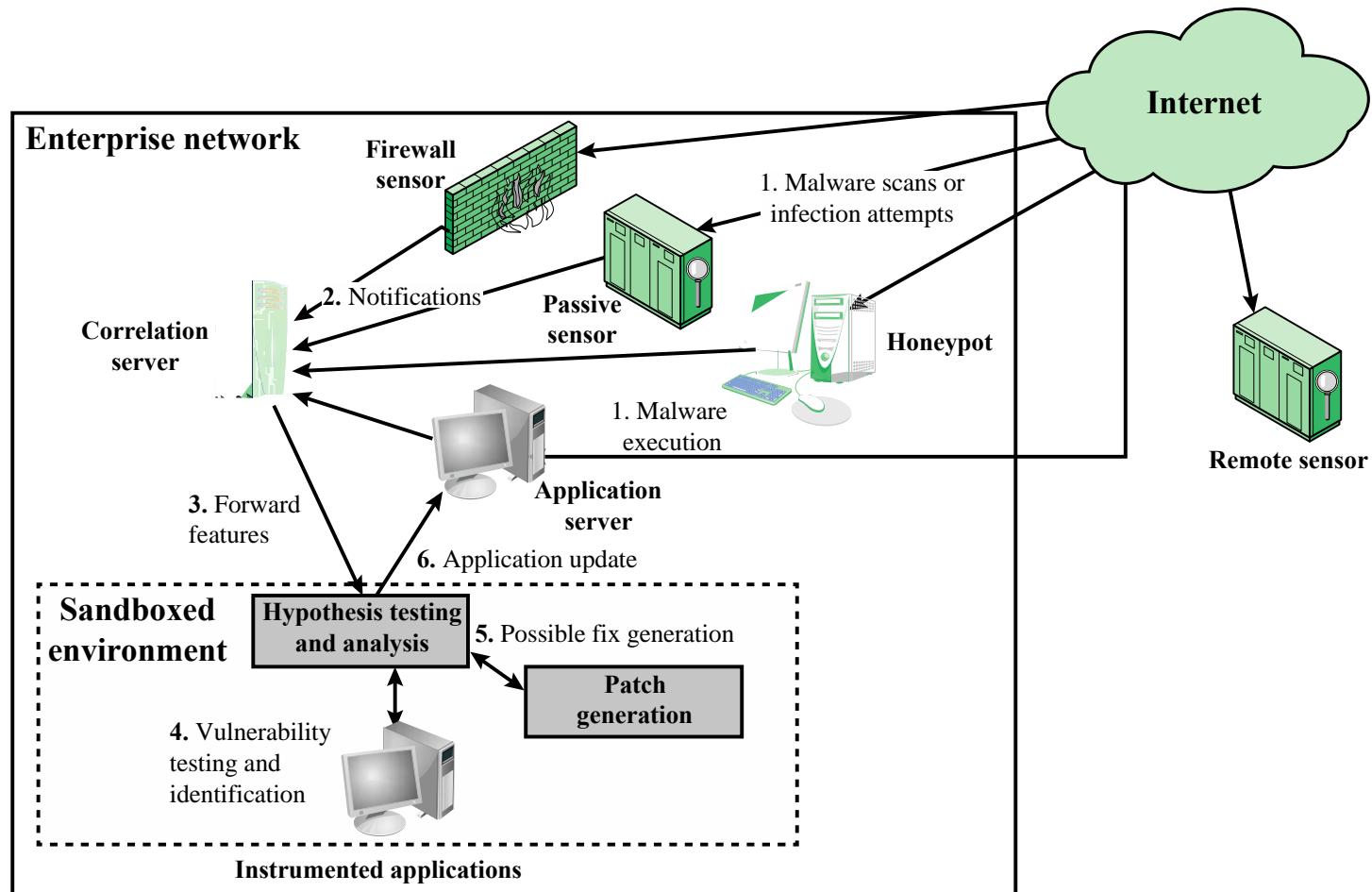


Figure 9.5 Placement of Malware Monitors (adapted from [SIDI05])

Snort Inline

- Enables Snort to function as an intrusion prevention system
- Includes a replace option which allows the Snort user to modify packets rather than drop them
 - Useful for a honeypot implementation
 - Attackers see the failure but cannot figure out why it occurred

Drop

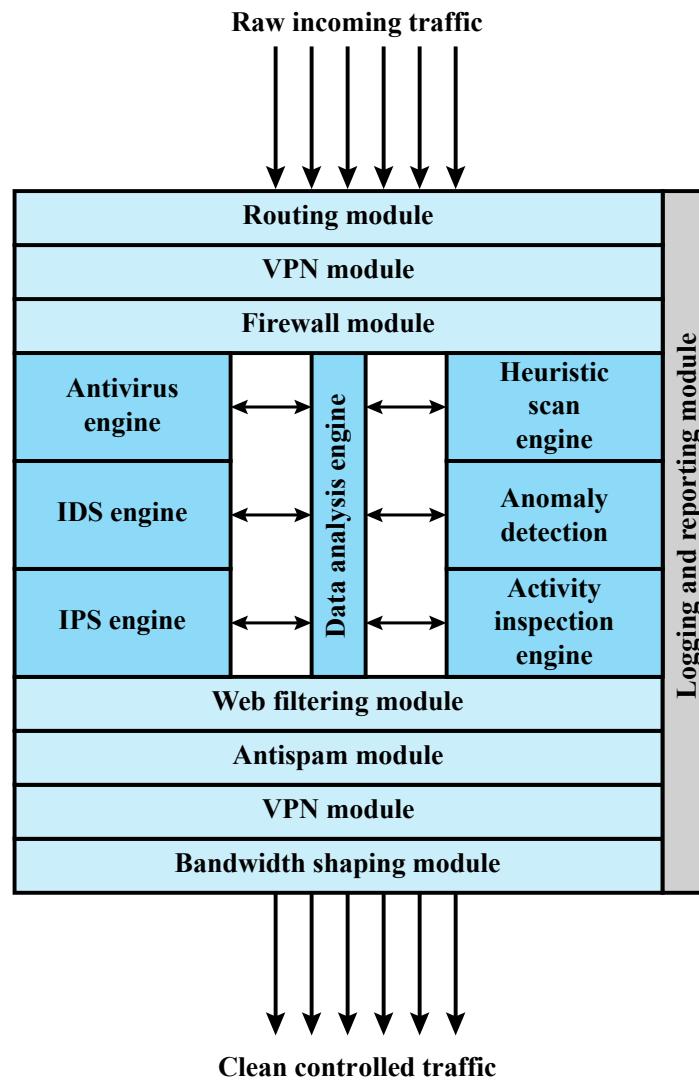
Snort rejects a packet based on the options defined in the rule and logs the result

Reject

Packet is rejected and result is logged and an error message is returned

Sdrop

Packet is rejected but not logged



**Figure 9.6 Unified Threat Management Appliance
(based on [JAME06])**

Table 9.3
Sidewinder G2 Security Appliance Attack Protections
Summary - Transport Level Examples

Attacks and Internet Threats	Protections
TCP	
<ul style="list-style-type: none"> • Invalid port numbers • Invalid sequence numbers • SYN floods • XMAS tree attacks • Invalid CRC values • Zero length • Random data as TCP header 	<ul style="list-style-type: none"> • TCP hijack attempts • TCP spoofing attacks • Small PMTU attacks • SYN attack • Script Kiddie attacks • Packet crafting: different TCP options set <ul style="list-style-type: none"> • Enforce correct TCP flags • Enforce TCP header length • Ensures a proper 3-way handshake • Closes TCP session correctly • 2 sessions, one on the inside and one on the outside • Enforce correct TCP flag usage • Manages TCP session timeouts • Blocks SYN attacks <ul style="list-style-type: none"> • Reassembly of packets ensuring correctness • Properly handles TCP timeouts and retransmits timers • All TCP proxies are protected • Traffic Control through access lists • Drop TCP packets on ports not open • Proxies block packet crafting
UDP	
<ul style="list-style-type: none"> • Invalid UDP packets • Random UDP data to bypass rules 	<ul style="list-style-type: none"> • Connection prediction • UDP port scanning <ul style="list-style-type: none"> • Verify correct UDP packet • Drop UDP packets on ports not open

(Table can be found on page 312 in the textbook)

Table 9.4

Sidewinder G2 Security Appliance Attack Protections Summary - Application Level Examples (page 1 of 2)

(Table can be found on pages 313-314
In the textbook)

Attacks and Internet Threats	Protections
	DNS
Incorrect NXDOMAIN responses from AAAA queries could cause denial-of-service conditions.	<ul style="list-style-type: none"> •Does not allow negative caching •Prevents DNS Cache Poisoning
ISC BIND 9 before 9.2.1 allows remote attackers to cause a denial of service (shutdown) via a malformed DNS packet that triggers an error condition that is not properly handled when the rdataset parameter to the dns_message_findtype() function in message.c is not NULL.	<ul style="list-style-type: none"> •Sidewinder G2 prevents malicious use of improperly formed DNS messages to affect firewall operations. •Prevents DNS query attacks •Prevents DNS answer attacks
DNS information prevention and other DNS abuses.	<ul style="list-style-type: none"> •Prevent zone transfers and queries •True split DNS protect by Type Enforcement technology to allow public and private DNS zones. •Ability to turn off recursion
	FTP
<ul style="list-style-type: none"> •FTP bounce attack •PASS attack •FTP Port injection attacks •TCP segmentation attack 	<ul style="list-style-type: none"> •Sidewinder G2 has the ability to filter FTP commands to prevent these attacks. •True network separation prevents segmentation attacks.
	SQL
SQL Net man in the middle attacks	<ul style="list-style-type: none"> •Smart proxy protected by Type Enforcement Technology •Hide Internal DB through nontransparent connections
	Real-Time Streaming Protocol (RTSP)
<ul style="list-style-type: none"> •Buffer overflow •Denial of service 	<ul style="list-style-type: none"> •Smart proxy protected by Type Enforcement technology •Protocol validation •Denies multicast traffic •Checks setup and teardown methods •Verifies PNG and RTSP protocol, discards all others •Auxiliary port monitoring
	SNMP
<ul style="list-style-type: none"> •SNMP flood attacks •Default community attack •Brute force attack •SNMP put attack 	<ul style="list-style-type: none"> •Filter SNMP version traffic 1, 2c •Filter Read, Write, and Notify messages •Filter OIDs •Filter PDU (Protocol Data Unit)

Table 9.4

Sidewinder G2 Security Appliance Attack Protections Summary – Application Level Examples

(page 2 of 2)

SSH			
<ul style="list-style-type: none"> •Challenge-Response buffer overflows •SSHD allows users to override “Allowed Authentications” •OpenSSH buffer_append_space buffer overflow •OpenSSH/PAM challenge Response buffer overflow •OpenSSH channel code offer-by-one 			
SMTP			
<ul style="list-style-type: none"> •Sendmail buffer overflows •Sendmail denial of service attacks •Remote buffer overflow in sendmail 	<ul style="list-style-type: none"> •Sendmail address parsing buffer overflow •SMTP protocol anomalies 	<ul style="list-style-type: none"> •Split Sendmail architecture protected by Type Enforcement technology •Sendmail customized for controls 	<ul style="list-style-type: none"> •Prevents buffer overflows through Type Enforcement technology •Sendmail checks SMTP protocol anomalies
Spyware Applications			
<ul style="list-style-type: none"> •Adware used for collecting information for marketing purposes •Stalking horses •Trojan horses 	<ul style="list-style-type: none"> •Malware •Backdoor Santas 	<ul style="list-style-type: none"> •SmartFilter® URL filtering capability built in with Sidewinder G2 can be configured to filter Spyware URLs, preventing downloads. 	

(Table can be found on pages 312 - 313 In the textbook)

Summary

- The need for firewalls
- Firewall characteristics and access policy
- Types of firewalls
 - Packet filtering firewall
 - Stateful inspection firewalls
 - Application-level gateway
 - Circuit-level gateway
- Firewall basing
 - Bastion host
 - Host-based firewalls
 - Personal firewall
- Firewall location and configurations
 - DMZ networks
 - Virtual private networks
 - Distributed firewalls
 - Firewall locations and topologies
- Intrusion prevention systems
 - Host-based IPS
 - Network-based IPS
 - Distributed or hybrid IPS
 - Snort inline
- Example: Unified Threat Management Products

Chapter 14

IT Security Management and Risk Assessment

IT Security Management Overview

Is the formal process of answering the questions:

What assets
need to be
protected



How are those
assets
threatened



What can be
done to counter
those threats

- Ensures that critical assets are sufficiently protected in a cost-effective manner
- Security risk assessment is needed for each asset in the organization that requires protection
- Provides the information necessary to decide what management, operational, and technical controls are needed to reduce the risks identified

Table 14.1

ISO/IEC 27000 Series of Standards on IT Security Techniques

27000:2016	“Information security management systems - Overview and vocabulary” provides an overview of information security management systems, and defines the vocabulary and definitions used in the 27000 family of standards.
27001:2013	“Information security management systems – Requirements” specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System.
27002:2013	“Code of practice for information security management” provides guidelines for information security management in an organization and contains a list of best-practice security controls. It was formerly known as ISO17799.
27003:2010	“Information security management system implementation guidance” details the process from inception to the production of implementation plans of an Information Security Management System specification and design.
27004:2009	“Information security management – Measurement” provides guidance to help organizations measure and report on the effectiveness of their information security management system processes and controls.
27005:2011	“Information security risk management” provides guidelines on the information security risk management process. It supersedes ISO13335-3/4.
27006:2015	“Requirements for bodies providing audit and certification of information security management systems” specifies requirements and provides guidance for these bodies.

IT Security Management

IT SECURITY MANAGEMENT: A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity, and reliability. IT security management functions include:

Determining organizational IT security objectives, strategies, and policies	Determining organizational IT security requirements	Identifying and analyzing security threats to IT assets within the organization	Identifying and analyzing risks	Specifying appropriate safeguards	Monitoring the implementation and operation of safeguards that are necessary in order to cost effectively protect the information and services within the organization	Developing and implementing a security awareness program	Detecting and reacting to incidents
---	---	---	---------------------------------	-----------------------------------	--	--	-------------------------------------

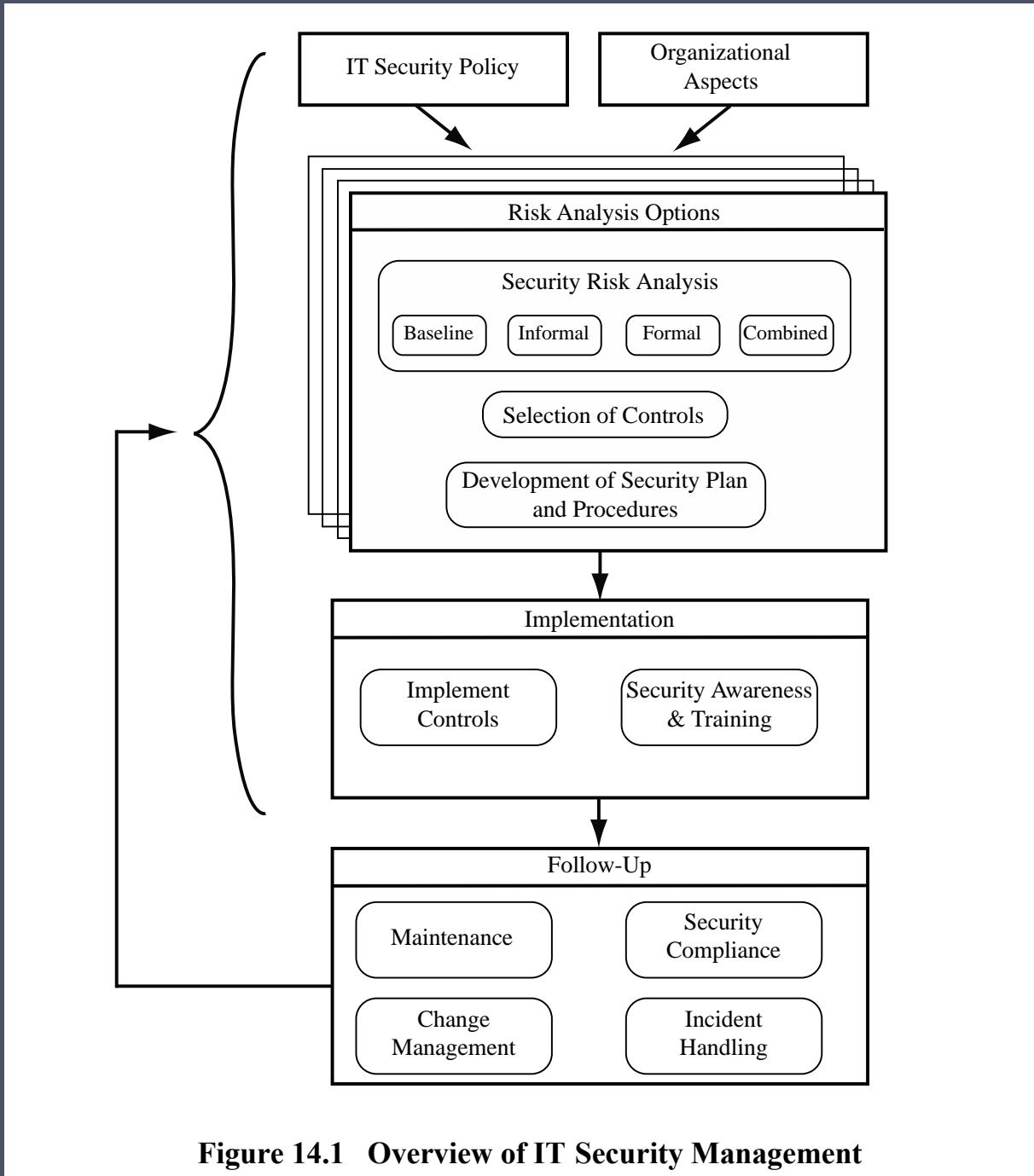


Figure 14.1 Overview of IT Security Management

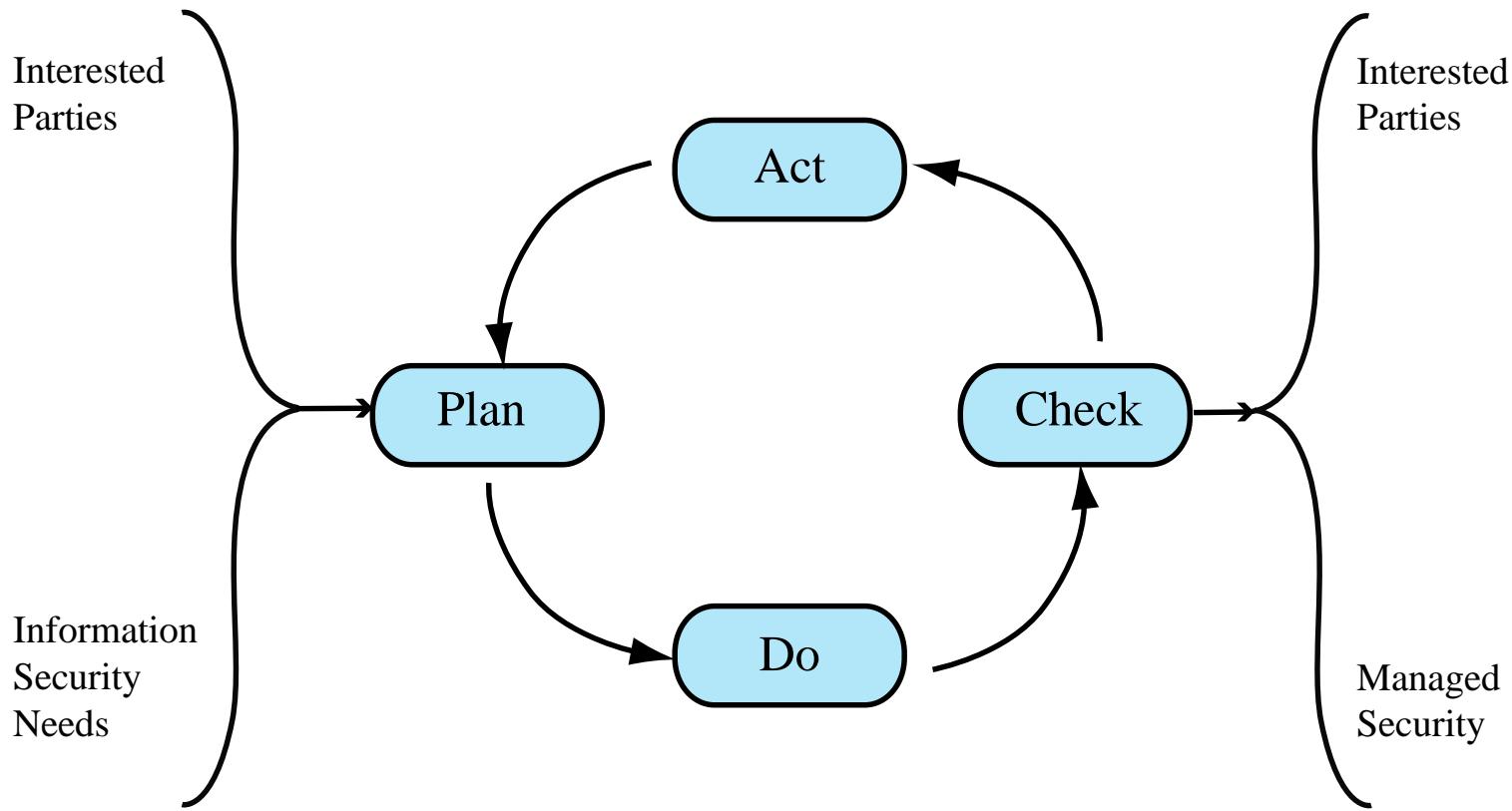


Figure 14.2 The Plan - Do - Check - Act Process Model

Organizational Context and Security Policy

- Maintained and updated regularly
 - Using periodic security reviews
 - Reflect changing technical/risk environments
- Examine role and importance of IT systems in organization

First examine organization's IT security:

Objectives - wanted IT security outcomes

Strategies - how to meet objectives

Policies - identify what needs to be done

Security Policy

Needs to address:

- Scope and purpose including relation of objectives to business, legal, regulatory requirements
- IT security requirements
- Assignment of responsibilities
- Risk management approach
- Security awareness and training
- General personnel issues and any legal sanctions
- Integration of security into systems development
- Information classification scheme
- Contingency and business continuity planning
- Incident detection and handling processes
- How and when policy reviewed, and change control to it

Management Support

- IT security policy must be supported by senior management
- Need IT security officer
 - To provide consistent overall supervision
 - Liaison with senior management
 - Maintenance of IT security objectives, strategies, policies
 - Handle incidents
 - Management of IT security awareness and training programs
 - Interaction with IT project security officers
- Large organizations need separate IT project security officers associated with major projects and systems
 - Manage security policies within their area

Security Risk Assessment

Critical component of process

Ideally examine every organizational asset

- Not feasible in practice

Approaches to identifying and mitigating risks to an organization's IT infrastructure:

- Baseline
- Informal
- Detailed risk
- Combined

Baseline Approach

- Goal is to implement agreed controls to provide protection against the most common threats
- Forms a good base for further security measures
- Use “industry best practice”
 - Easy, cheap, can be replicated
 - Gives no special consideration to variations in risk exposure
 - May give too much or too little security
- Generally recommended only for small organizations without the resources to implement more structured approaches

Informal Approach

Involves conducting an informal, pragmatic risk analysis on organization's IT systems

Exploits knowledge and expertise of analyst

Fairly quick and cheap

Judgments can be made about vulnerabilities and risks that baseline approach would not address

Some risks may be incorrectly assessed

Skewed by analyst's views, varies over time

Suitable for small to medium sized organizations where IT systems are not necessarily essential

Chapter 19

Legal and Ethical Aspects

“Computer crime, or cybercrime, is a term used broadly to describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity.”

--From the New York Law School Course on Cybercrime, Cyberterrorism, and Digital Law Enforcement

Types of Computer Crime

- The U.S. Department of Justice categorizes computer crime based on the role that the computer plays in the criminal activity:

Computers as targets

Involves an attack on data integrity, system integrity, data confidentiality, privacy, or availability

Computers as storage devices

Using the computer to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or pirated commercial software

Computers as communications tools

Crimes that are committed online, such as fraud, gambling, child pornography, and the illegal sale of prescription drugs, controlled substances, alcohol, or guns

Article 2 Illegal access

The access to the whole or any part of a computer system without right.

Article 3 Illegal interception

The interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data.

Article 4 Data interference

The damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 System interference

The serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 Misuse of devices

- a** The production, sale, procurement for use, import, distribution or otherwise making available of:
 - i** A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
 - ii** A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5; and
- b** The possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in the above Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Article 7 Computer-related forgery

The input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

Article 8 Computer-related fraud

The causing of a loss of property to another person by:

- a** Any input, alteration, deletion or suppression of computer data;
- b** Any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Table 19.1

Cybercrimes Cited in the Convention on Cybercrime

Table 19.1

Cybercrimes Cited in the Convention on Cybercrime (page 2 of 2)

Article 9 Offenses related to child pornography

- a Producing child pornography for the purpose of its distribution through a computer system;
- b Offering or making available child pornography through a computer system;
- c Distributing or transmitting child pornography through a computer system;
- d Procuring child pornography through a computer system for oneself or for another person;
- e Possessing child pornography in a computer system or on a computer-data storage medium.

Article 10 Infringements of copyright and related rights

Article 11 Attempt and aiding or abetting

Aiding or abetting the commission of any of the offences established in accordance with the above Articles 2 through 10 of the present Convention with intent that such offence be committed. An attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

Table 19.2

CERT 2007 E-Crime Watch Survey Results

	Committed (net %)	Insider (%)	Outsider (%)	Source Unknown (%)
Virus, worms or other malicious code	74	18	46	26
Unauthorized access to/use of information, systems or networks	55	25	30	10
Illegal generation of spam e-mail	53	6	38	17
Spyware (not including adware)	52	13	33	18
Denial of service attacks	49	9	32	14
Fraud (credit card fraud, etc.)	46	19	28	5
Phishing (someone posing as your company online in an attempt to gain personal data from your subscribers or employees)	46	5	35	12
Theft of other (proprietary) info including customer records, financial records, etc.	40	23	16	6
Theft of intellectual property	35	24	12	6
Intentional exposure of private or sensitive information	35	17	12	9
Identity theft of customer	33	13	19	6
Sabotage: deliberate disruption, deletion, or destruction of information, systems, or networks	30	14	14	6
Zombie machines on organization's network/bots/use of network by BotNets	30	6	19	10
Web site defacement	24	4	14	7
Extortion	16	5	9	4
Other	17	6	8	7

(Table can be found on page 582 in the textbook)

Law Enforcement Challenges

- The deterrent effect of law enforcement on computer and network attacks correlates with the success rate of criminal arrest and prosecution
- Law enforcement agency difficulties:
 - Lack of investigators knowledgeable and experienced in dealing with this kind of crime
 - Required technology may be beyond their budget
 - The global nature of cybercrime
 - Lack of collaboration and cooperation with remote law enforcement agencies
- Convention on Cybercrime introduces a common terminology for crimes and a framework for harmonizing laws globally

The lack of success in bringing them to justice has led to an increase in their numbers, boldness, and the global scale of their operations

Cybercriminals

Are difficult to profile

Tend to be young and very computer-savvy

Range of behavioral characteristics is wide

No cybercriminal databases exist that can point to likely suspects

Are influenced by the success of cybercriminals and the lack of success of law enforcement

Cybercrime Victims

Many of these organizations have not invested sufficiently in technical, physical, and human-factor resources to prevent attacks

Reporting rates tend to be low because of a lack of confidence in law enforcement, concern about corporate reputation, and a concern about civil liability

Working with Law Enforcement

- Executive management and security administrators need to look upon law enforcement as a resource and tool
- Management needs to:
 - Understand the criminal investigation process
 - Understand the inputs that investigators need
 - Understand the ways in which the victim can contribute positively to the investigation

Pakistan is Prevention of Electronic Crimes Act, 2016 (“Act”)

- The law dealing with cyber crimes in Pakistan is Prevention of Electronic Crimes Act, 2016 (“**Act**”) which is applicable to every citizen of Pakistan wherever he may be and to every other person who is stationed in Pakistan for the time being.

Types of cyber crimes under the Act:

- Access or interfere the data or information system and copying or transmission of data; (Section 3, 4 and 5 of the Act).
- Unauthorized access, unauthorized copying, unauthorized transmitting or unauthorized interfering with the critical infrastructure OR threaten to commit any of the aforesaid offences with an intention to coerce, intimidate, create a sense of fear, panic, insecurity or public or community/society (Sections 6, 7 and 8 of the Act).
- Prepare or disseminate information through any information system or device with the intent to glorify an offence relating to terrorism, or any person convicted of a crime relating to terrorism OR threaten to commit any of the aforesaid offences with an intention to coerce, intimidate, create a sense of fear, panic, insecurity or public or community/society (Section 9 of the Act).

Types of cyber crimes under the Act:

- Whosoever prepares or disseminates any Hate Speech, information that invites motivation of people to fund or recruits for terrorism through any information system or device (Sections 11 & 12 of the Act).
- Electronic forgery and electronic fraud committed by interfering with any information system, device or data with the intent to cause damage or injury to the public; or to make any illegal claim; or title or to cause any person to part with property; or to enter into a contract; to commit fraud; alteration, deletion or suppression of data etc. (Sections 13 & 14 of the Act).
- An act to manufacture, generate, adapt, export, supply, offer to supply or import any information system, data or device, with an intent to be used or believing that it is primarily to be used to commit or to assist in the commission of an offence under this Act. (Section 15 of the Act).

Types of cyber crimes under the Act:

- Unauthorized use of another person's identity information or to obtain, sell, possess or transmit such information. (Sections 16 of the Act).
- Issuance of SIM (subscriber identity module); R-IUM (re-useable identification module); or UICC (universal integrated circuit) or any other module designed for authenticating users to establish connection with the network and to be used in cellular mobile, wireless phone or other digital devices without obtaining and verification of the subscriber's antecedents. (Section 17 of the Act).
- Dignity of Natural Person: Public exhibit or display or transmission of any information knowingly that such information is false and intimidate or harm the reputation or privacy of a natural person through an information system. (Section 20 of the Act).

Types of cyber crimes under the Act:

- Modesty of Natural Person: Intentional and public display or exhibition or transmission of any information which superimposes a photograph over any sexually explicit image or video of a natural person; includes a photograph in sexually explicit conduct of a natural person; intimates a natural person with sexual act; sexually explicit image or video of a natural person; or entices or induces a natural person to engage in sexually explicit act; through an information system to harm a natural person or his reputation, take revenge, create hatred or blackmail a natural person. (Section 21 of the Act).
- Child Pornography: Produce, offer or make available, distribute or transmit through an information system or to procure for himself or for any other person or without lawful justification possesses material in an information system any material which contain the elements of child pornography. (Section 22 of the Act).
- Writing, offering, making available, distributing or transmitting malicious code through an information system with an intent to cause harm to any information system or data resulting in the corruption, destruction, alteration suppression, theft or loss of information system. (Section 23 of the Act).

Types of cyber crimes under the Act:

- Doing Cyber Stalking with an intent to coerce or intimidate or harass any person by using information system, information system network, internet website, electronic mail or any similar means of communication. The term Cyber Stalking includes: (a) foster personal interaction repeatedly to a person who clearly indicates a disinterest from the stalker; (b) monitor the internet, electronic mail, text message or any other form of electronic communication of another person; (c) watch or spy upon a person in a manner that results in fear of violence or serious alarm or distress in mind of such persons; and (d) take photograph or make video of a person and display or distribute such video in a manner without his consent that harms a person. (Section 24 of the Act).
- Spamming: A person commits the offence of spamming who with an intent transmits harmful, fraudulent, misleading, illegal or unsolicited information to any person without permission of the recipient or who causes any information system to show any such information for wrongful gain. (Section 25 of the Act).

Privacy

- Overlaps with computer security
- Dramatic increase in scale of information collected and stored
 - Motivated by law enforcement, national security, economic incentives
- Individuals have become increasingly aware of access and use of personal information and private details about their lives
- Concerns about extent of privacy compromise have led to a variety of legal and technical approaches to reinforcing privacy rights

European Union (EU) Directive on Data Protection

- Adopted in 1998 to:
 - Ensure member states protect fundamental privacy rights when processing personal information
 - Prevent member states from restricting the free flow of personal information within EU
- Organized around principles of:

Notice

Consent

Consistency

Access

Security

Onward
transfer

Enforcement

United States Privacy Initiatives

Privacy Act of 1974

- Deals with personal information collected and used by federal agencies
- Permits individuals to determine records kept
- Permits individuals to forbid records being used for other purposes
- Permits individuals to obtain access to records and to correct and amend records as appropriate
- Ensures agencies properly collect, maintain, and use personal information
- Creates a private right of action for individuals

Also have a range of other privacy laws

ISO 27002 states . . .

“An organization’s data policy for privacy and protection of personally identifiable information should be developed and implemented. This policy should be communicated to all persons involved in the processing of personally identifiable information. Compliance with this policy and all relevant legislation and regulations concerning the protection of the privacy of people and the protection of personally identifiable information requires appropriate management structure and control. Often this is best achieved by the appointment of a person responsible, such as a privacy officer, who should provide guidance to managers, users and service providers on their individual responsibilities and the specific procedures that should be followed. Responsibility for handling personally identifiable information and ensuring awareness of the privacy principles should be dealt with in accordance with relevant legislation and regulations. Appropriate technical and organizational measures to protect personally identifiable information should be implemented.”

Privacy and Data Surveillance

- The demands of big business, government and law enforcement have created new threats to personal privacy
 - Scientific and medical research data collection for analysis
 - Law enforcement data surveillance
 - Private organizations profiling
 - This creates tension between enabling beneficial outcomes in areas including scientific research, public health, national security, law enforcement and efficient use of resources, while still respecting an individual's right to privacy
- Another area of particular concern is the rapid rise in the use of public social media sites
 - These sites gather, analyze, and share large amounts of data on individuals and their interactions with other individuals and organizations
 - Many people willingly upload large amounts of personal information, including photos and status updates
 - This data could potentially be used by current and future employers, insurance companies, private investigators, and others, in their interactions with the individual

Privacy Protection

- Both policy and technical approaches are needed to protect privacy
- In terms of technical approaches, the requirements for privacy protection for data stored on information systems can be addressed in part using the technical mechanisms developed for database security
- With regard to social media sites, technical controls include:
 - The provision of suitable privacy settings to manage who can view data on individuals
 - Notification when one individual is referenced or tagged in another's content
 - Although social media sites include some form of these controls, they are constantly changing, causing frustration for users who are trying to keep up with these mechanisms
- Another approach for managing privacy concerns in big data analysis is to anonymize the data, removing any personally identifying information before release to researchers or other organizations for analysis

Data Privacy

- In terms of policy, guidelines are needed to manage the use and reuse of big data, ensuring suitable constraints are imposed in order to preserve privacy
 - Consent
 - Ensuring participants can make informed decisions about their participation in the research
 - Privacy and confidentiality
 - Privacy is the control that individuals have over who can access their personal information
 - Confidentiality is the principle that only authorized persons should have access to information
 - Ownership and authorship
 - Addresses who has responsibility for the data, and at what point does an individual give up their right to control their personal data
 - Data sharing – assessing the social benefits of research
 - The social benefits that result from data matching and reuse of data from one source or research project in another
 - Governance and custodianship
 - Oversight and implementation of the management, organization, access, and preservation of digital data

Ethical Issues

- Ethics:

“A system of moral principles that relates to the benefits and harms of particular actions, and to the rightness and wrongness of motives and ends of those actions.”

- Many potential misuses and abuses of information and electronic communication that create privacy and security problems
- Basic ethical principles developed by civilizations apply
 - Unique considerations surrounding computers and information systems
 - Scale of activities not possible before
 - Creation of new types of entities for which no agreed ethical rules have previously been formed

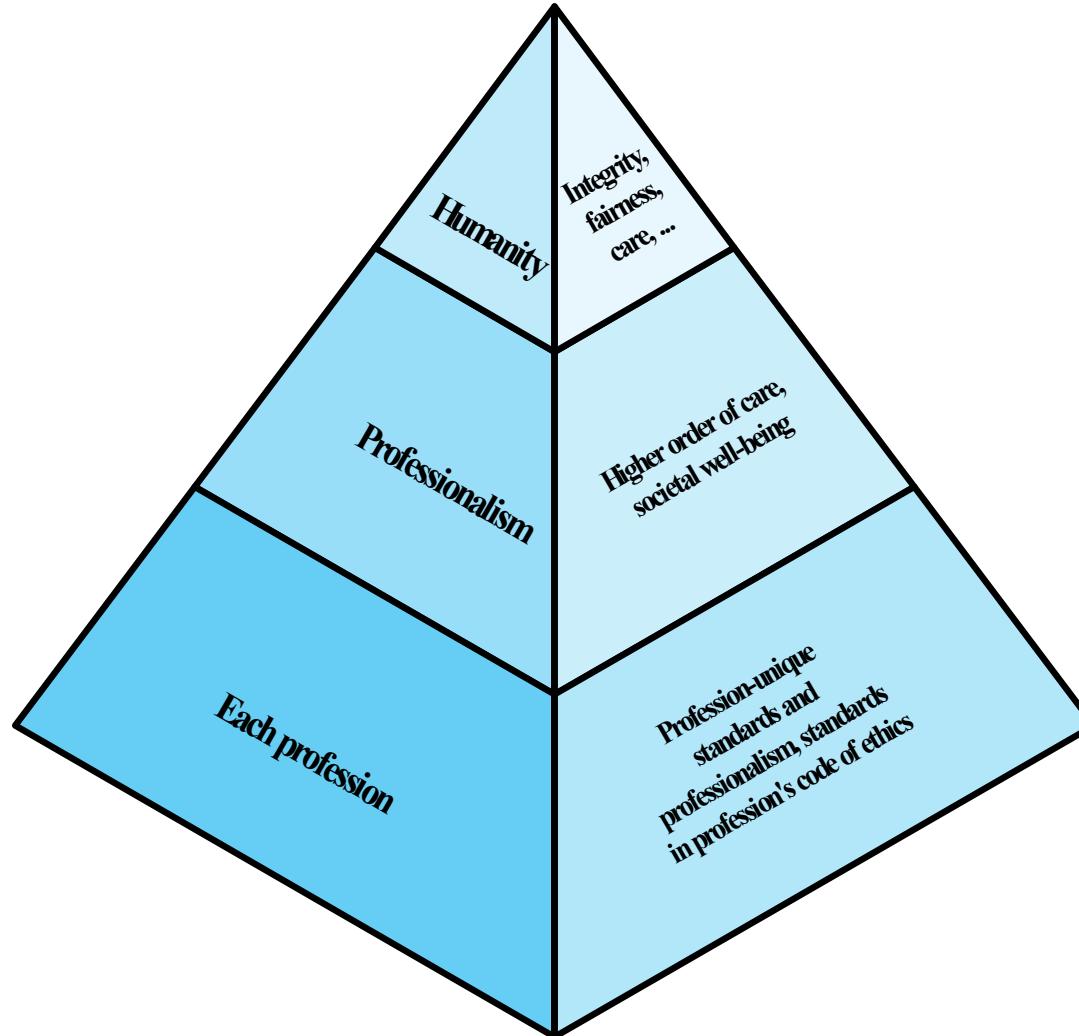


Figure 19.5 The Ethical Hierarchy

Ethical Issues Related to Computers and Information Systems

- Some ethical issues from computer use:
 - Repositories and processors of information
 - Producers of new forms and types of assets
 - Instruments of acts
 - Symbols of intimidation and deception
- Those who understand, exploit technology, and have access permission, have power over these

Professional/Ethical Responsibilities

- Concern with balancing professional responsibilities with ethical or moral responsibilities
- Types of ethical areas a computing or IT professional may face:
 - Ethical duty as a professional may come into conflict with loyalty to employer
 - “Blowing the whistle”
 - Expose a situation that can harm the public or a company’s customers
 - Potential conflict of interest
- Organizations have a duty to provide alternative, less extreme opportunities for the employee
 - In-house ombudsman coupled with a commitment not to penalize employees for exposing problems
- Professional societies should provide a mechanism whereby society members can get advice on how to proceed

Codes of Conduct

- Ethics are not precise laws or sets of facts
- Many areas may present ethical ambiguity
- Many professional societies have adopted ethical codes of conduct which can:

- 
- Be a positive stimulus and instill confidence
 - Be educational
 - Provide a measure of support
 - Be a means of deterrence and discipline
 - Enhance the profession's public image

1. GENERAL MORAL IMPERATIVES.

- 1.1 Contribute to society and human well-being.
- 1.2 Avoid harm to others.
- 1.3 Be honest and trustworthy.
- 1.4 Be fair and take action not to discriminate.
- 1.5 Honor property rights including copyrights and patent.
- 1.6 Give proper credit for intellectual property.
- 1.7 Respect the privacy of others.
- 1.8 Honor confidentiality.

2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES.

- 2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
- 2.2 Acquire and maintain professional competence.
- 2.3 Know and respect existing laws pertaining to professional work.
- 2.4 Accept and provide appropriate professional review.
- 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
- 2.6 Honor contracts, agreements, and assigned responsibilities.
- 2.7 Improve public understanding of computing and its consequences.
- 2.8 Access computing and communication resources only when authorized to do so.

3. ORGANIZATIONAL LEADERSHIP IMPERATIVES.

- 3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
- 3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.
- 3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.
- 3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
- 3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.
- 3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

4. COMPLIANCE WITH THE CODE.

- 4.1 Uphold and promote the principles of this Code.
- 4.2 Treat violations of this code as inconsistent with membership in the ACM.

Figure 19.6 ACM Code of Ethics and Professional Conduct

(Copyright ©1997, Association for Computing Machinery, Inc.)

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

1. to accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding of technology, its appropriate application, and potential consequences;
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics

Figure 19.7 IEEE Code of Ethics
(Copyright ©2006, Institute of Electrical and Electronics Engineers)

In recognition of my obligation to management I shall:

- Keep my personal knowledge up-to-date and insure that proper expertise is available when needed.
- Share my knowledge with others and present factual and objective information to management to the best of my ability.
- Accept full responsibility for work that I perform.
- Not misuse the authority entrusted to me.
- Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.
- Not take advantage of the lack of knowledge or inexperience on the part of others.

In recognition of my obligation to my fellow members and the profession I shall:

- Be honest in all my professional relationships.
- Take appropriate action in regard to any illegal or unethical practices that come to my attention. However, I will bring charges against any person only when I have reasonable basis for believing in the truth of the allegations and without any regard to personal interest.
- Endeavor to share my special knowledge.
- Cooperate with others in achieving understanding and in identifying problems.
- Not use or take credit for the work of others without specific acknowledgement and authorization.
- Not take advantage of the lack of knowledge or inexperience on the part of others for personal gain.

In recognition of my obligation to society I shall:

- Protect the privacy and confidentiality of all information entrusted to me.
- Use my skill and knowledge to inform the public in all areas of my expertise.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.
- Support, respect, and abide by the appropriate local, state, provincial, and federal laws.
- Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

In recognition of my obligation to my employer I shall:

- Make every effort to ensure that I have the most current knowledge and that the proper expertise is available when needed.
- Avoid conflict of interest and insure that my employer is aware of any potential conflicts.
- Present a fair, honest, and objective viewpoint.
- Protect the proper interests of my employer at all times.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not misrepresent or withhold information that is germane to the situation.
- Not attempt to use the resources of my employer for personal gain or for any purpose without proper approval.
- Not exploit the weakness of a computer system for personal gain or personal satisfaction.

Figure 19.8 AITP Standard of Conduct

(Copyright ©2006, Association of Information Technology Professionals)

Comparison of Codes of Conduct

- All three codes place their emphasis on the responsibility of professionals to other people
- Do not fully reflect the unique ethical problems related to the development and use of computer and IT technology
- Common themes:
 - Dignity and worth of other people
 - Personal integrity and honesty
 - Responsibility for work
 - Confidentiality of information
 - Public safety, health, and welfare
 - Participation in professional societies to improve standards of the profession
 - The notion that public knowledge and access to technology is equivalent to social power

The Rules

- Collaborative effort to develop a short list of guidelines on the ethics of computer systems
- Ad Hoc Committee on Responsible Computing
 - Anyone can join this committee and suggest changes to the guidelines
 - Moral Responsibility for Computing Artifacts
 - Generally referred to as The Rules
 - The Rules apply to software that is commercial, free, open source, recreational, an academic exercise or a research tool
 - Computing artifact
 - Any artifact that includes an executing computer program

As of this writing, the rules are as follows:

- 1) The people who design, develop, or deploy a computing artifact are morally responsible for that artifact, and for the foreseeable effects of that artifact. This responsibility is shared with other people who design, develop, deploy or knowingly use the artifact as part of a sociotechnical system.
- 2) The shared responsibility of computing artifacts is not a zero-sum game. The responsibility of an individual is not reduced simply because more people become involved in designing, developing, deploying, or using the artifact. Instead, a person's responsibility includes being answerable for the behaviors of the artifact and for the artifact's effects after deployment, to the degree to which these effects are reasonably foreseeable by that person.
- 3) People who knowingly use a particular computing artifact are morally responsible for that use.
- 4) People who knowingly design, develop, deploy, or use a computing artifact can do so responsibly only when they make a reasonable effort to take into account the sociotechnical systems in which the artifact is embedded.
- 5) People who design, develop, deploy, promote, or evaluate a computing artifact should not explicitly or implicitly deceive users about the artifact or its foreseeable effects, or about the sociotechnical systems in which the artifact is embedded.

Summary

- Cybercrime and computer crime
 - Types of computer crime
 - Law enforcement challenges
 - Working with law enforcement
- Intellectual property
 - Types of intellectual property
 - Intellectual property relevant to network and computer security
 - Digital millennium copyright act
 - Digital rights management
- Privacy
 - Privacy law and regulation
 - Organizational response
 - Computer usage privacy
 - Privacy, data surveillance, big data, and social media
- Ethical issues
 - Ethics and the IT professions
 - Ethical issues related to computers and information systems
 - Codes of conduct
 - The rules