USER AUTHENTFICATION

CHP 3

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)

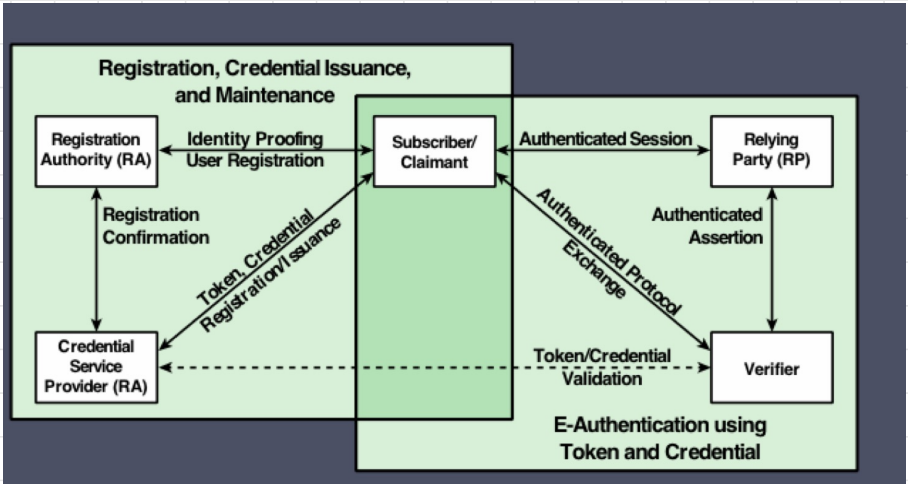


Figure 3.1 The NIST SP 800-63-2 E-Authentication Architectural Model

The four means of authenticating user identity are based on:

Something the individual knows	Something the individual possesses (token)	Something the individual is (static biometrics)	Something the individual does (dynamic biometrics)
• Password, PIN, answers to prearranged questions	• Smartcard, electronic keycard, physical key	• Fingerprint, retina, face	• Voice pattern, handwriting, typing rhythm

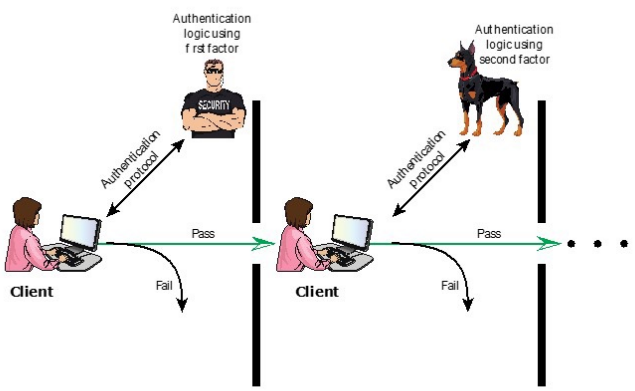


Figure 3.2 Multifactor Authentication

Multifactor authentication means using more than one method from the list of authentication types (see Figure 3.2).

The strength of an authentication system depends on how many factors it uses. Systems with two factors are stronger than those with one, and systems with three factors are stronger than those with two.

Risk Assessment for User Authentication

There are 3 seperate concepts

1. Assurance Level
2. Potential Impact
3. Areas of risk

Assurance Level

- indicates how certain an organization is that a users identity matches the credential presented
- It has 2 aspects
  1. confidence in identity verification process
  2. confidence that the credential user is the person it was issued to

4 levels of assurance

- LEVEL 1
  - minimal confidence in identity validity
  - Suitable for low stake situations → e.g online discussions
  - Authentication might just require a user ID and password
- LEVEL 2
  - moderate confidence in identity validity
  - Suitable for Public interactions → req, initial identity verification
  - secure authentification protocols are recommended
- LEVEL 3
  - high confidence in identity validity
  - Suitable for accessing sensitive but not highest value services → e.g submitting confidential docs
  - req atleast 2 authentification factors
- LEVEL 3
  - very high confidence in identity validity
  - Suitable for accessing critical, highest value services → e.g law enforcement databases
  - req multiple authentification factors and often in person registration

Potential Impact

- relate to how much harm a security breach (eg authentication failure) could cause
- FIPS 199 defines 3 level impact levels
  - Low
    - limited impact → eg reduction in mission effectiveness
    - minor damage to assets
    - minor financial or harm to individuals
  - Moderate
    - serious impact → significant mission degradation
    - significant damage to assets
    - significant financial or harm to individuals → but not life threating
  - High
    - severe impact → major mission loss
    - extensive damage to assets
    - major financial loss or severe harm to individuals → life threating

Table 3.2

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	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	None	None	Low	Mod/ High
Personal safety				
Civil or criminal violations	None	Low	Mod	High

Maximum Potential Impacts for Each Assurance Level

Password based Authentication

↳ widely used for defense against intruders

↳ user provides name and password

↳ system compares password with one stored for that login

↳ The ID provides security by

↳ Authorizing access

↳ only users with a registered ID can access the system

↳ Setting Privileges

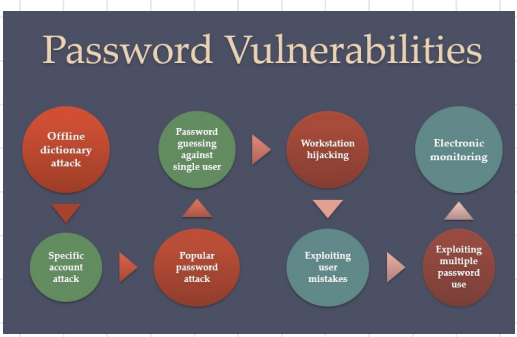
↳ users may have different access levels

eg superstar status ⟶ extra permissions

guest account status ⟶ limited access

↳ enables discretionary access control

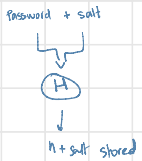
↳ allowing users to grant specific permissions to others for their files



Offline dictionary attack: The attacker obtains the password file and compares password hashes to hashes of common passwords.
Countermeasures include preventing access to the password file, detecting intrusions, and quickly reissuing passwords if compromised.
Specific account attack: The attacker targets one account and guesses until the password is found.
A standard countermeasure is an account lockout after several failed login attempts.
Popular password attack: The attacker tries common passwords across multiple accounts.
Countermeasures include policies to prevent users from choosing common passwords and monitoring IP addresses and client patterns.
Password guessing against a single user: The attacker guesses based on knowledge of the user and password policies.
Countermeasures include policies for complex, unique passwords, covering length, secrecy, and required changes.
Workstation hijacking: The attacker uses a logged-in, unattended workstation.
Countermeasures include automatic logouts after inactivity and intrusion detection for unusual behavior.
Exploiting user mistakes: Users may write down difficult passwords or share them, or attackers may use social engineering to obtain them. Systems may also have default passwords.
Countermeasures include user training, intrusion detection, and simpler passwords paired with other authentication.
Exploiting multiple password use: Attacks are more effective if users use the same password across different systems.
A policy forbidding this practice helps prevent such attacks.
Electronic monitoring: If passwords are sent over a network, they can be intercepted.
Simple encryption won't prevent reuse if the encrypted password is captured.

A common password security technique is to use **hashed passwords with a salt value.**
This method is found in most UNIX systems and others. Here's how it works (Figure 3.3a):

To set a new password, the user chooses or is given a password, which is combined with a salt value.
Older systems used the time the password was set as the salt, but newer systems use a random or pseudorandom number.
This password and salt are then input into a hashing algorithm to produce a hash code,
which is stored along with the salt in the password file.
This hash algorithm is deliberately slow to resist attacks.
Research has shown this method to be secure against many cryptanalytic attacks.



When a user logs in, they provide an ID and password (Figure 3.3b).
The system retrieves the stored salt and hashed password for that ID,
combines the salt with the user's input, and hashes it.
If the result matches the stored hash, access is granted.

The salt has three key benefits:
1. It prevents identical passwords from appearing the same in the password file,
even if multiple users choose the same password.
2. It makes offline dictionary attacks more difficult by increasing the possible passwords by 2^b for a salt length of b bits.
3.It prevents attackers from knowing if a user has reused the same password across different systems.

For offline dictionary attacks, an attacker would try to match guessed passwords to stored hashes.
Without a salt, they only need to hash each guess once,
but with the salt, they must hash each guess separately for every salt value in the file, multiplying the work.

There are two threats to this password scheme.
1. First, an attacker might gain access to a machine and use a "password cracker" program to guess passwords with minimal resource use.
2. Second, if an attacker gets a copy of the password file, they could run a cracker on another machine and try millions of passwords over time.

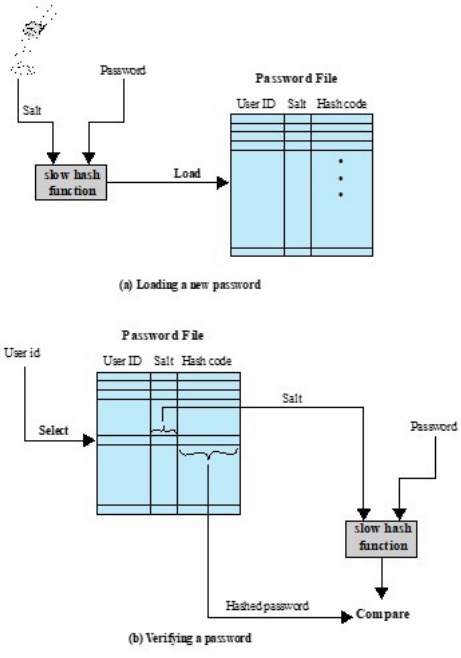


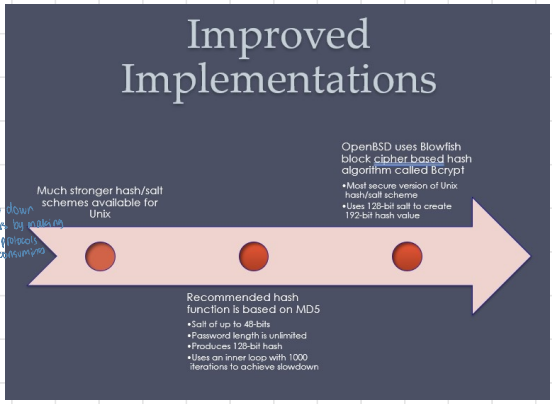
Figure 3.3 UNIX Password Scheme

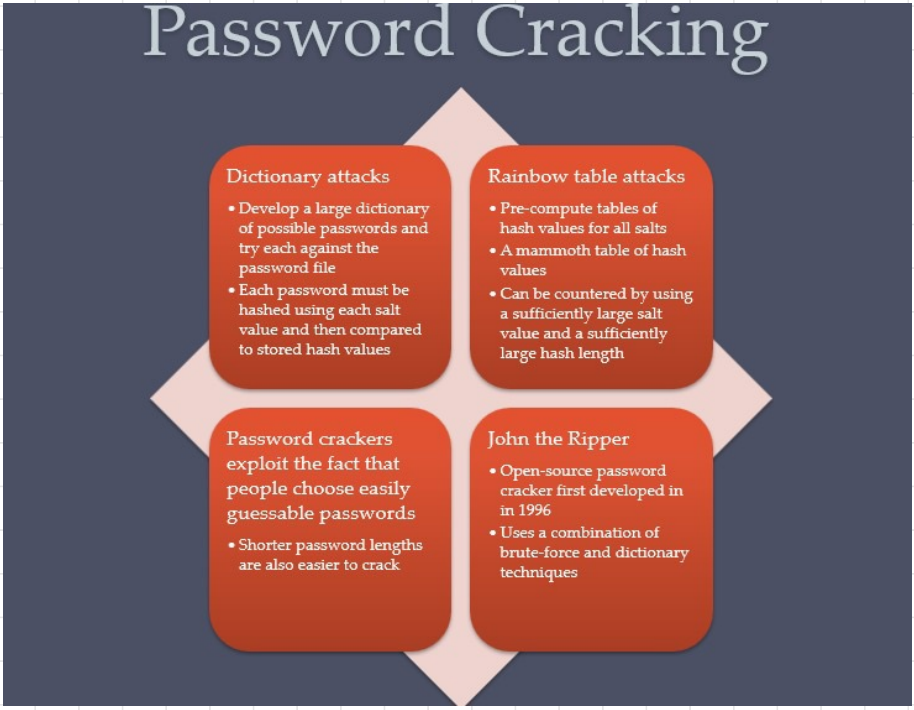
Salted Passwords

- **Encoding of password with random string (salt)**
  - Example: $stored_pw = hash($password+$salt);
  - Salt value stored along with hashed password
- **Cracking of stored passwords more expensive**
  - Same password maps to different hash values
  - Without salt: cracking depends on # words
  - With salt: cracking depends on (# words × # salts)
- **Security depends on quality of password, hash and salt**

UNIX Implementation

- Original Scheme
  - upto 8 character password
  - 12 bit salt used modifys DES encryption into a one way hash function
  - 0 value repeatedly encrypted 25 times
  - Output translated to 11 characters sequence
- NOW OUTDATED
  - as modren attacks like dictionary attacks can easily guess millions of passwords
  - despite this it is still used for compatibility with older systems





Modern Approaches

↳ Complex Password Policy

↳ forcing users to pick stronger passwords

but password-cracking methods have also advanced.

Processing Power: Graphics processors (GPUs) now enable password-cracking software to test billions of passwords per second, far surpassing traditional CPU speeds.
A single AMD Radeon HD7970 GPU, for instance, can try over 8 billion passwords per second.

Advanced Algorithms: Sophisticated models reduce search space by focusing on probable passwords. For example, researchers use language-based probability models and, more effectively, analyze real-world passwords.

The availability of large datasets, like RockYou.com's leaked 32 million passwords, has allowed researchers to develop more efficient techniques. Using these datasets, algorithms like probabilistic context-free grammars can prioritize guesses based on likely patterns, making password cracking even faster.

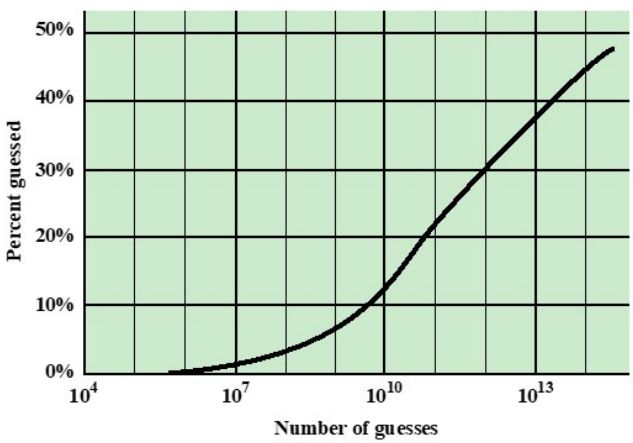


Figure 3.4 The Percentage of Passwords Guessed After a Given Number of Guesses

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

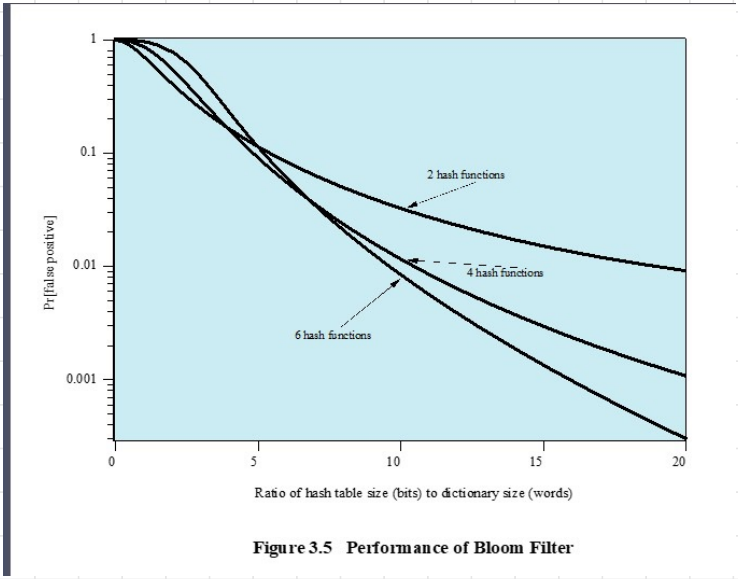


Figure 3.5 Performance of Bloom Filter

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 Contact Contactless	Electronic memory and processor inside Electrical contacts exposed on surface Radio antenna embedded inside	Biometric ID card

Types of Cards Used as Tokens

Memory cards

- can store but not process data
- most common is the Magnetic Stripe
- can be used alone for physical access
  - hotel room
  - ATM
- Provides greater security when combined with a PIN

cons

- req a special reader → increases cost
- loss of token → if card lost/stolen then no access → replacement cost
  → if PIN known → unauthorised access
- user dissatisfaction

Smart Tokens

- Physical characteristics
  - an embeded microprocessor
  - resembles a blank card
  - looks like calculators, keys, small portable objects
- Authentication protocol
  - Static
    - user verifies the identity to the token which then authenticates with the computer
  - Dynamic Password generator
    - the token generates a new password regularly
  - challange Response
    - the system sends a random challange and the token creates a response → open by encrypting the challange with a private key
- User Interface
  - a keypad and display for interaction
- Electronic interface
  - Contact
    - req insertion into a reader
    - connecting directly to the cards contact points
  - Contactless
    - works when close to a reader
    - uses radio frequency
    - ideal for quick access uses → e.g. building entry

Smart Cards

- is a key type of smart token
- resembles a credit card
- has an electronic interface
- contains a microprocessor → Processor, Memory, I/O ports
- typically contains 3 types of memory
  - ROM: stores unchanging data → card number, cardholder's name
  - EEPROM: holds variable application data and programs → operational protocols, remaining talk time for a telephone card
  - RAM: stores temporary data generated during application use

(electronically erasable programmable ROM)

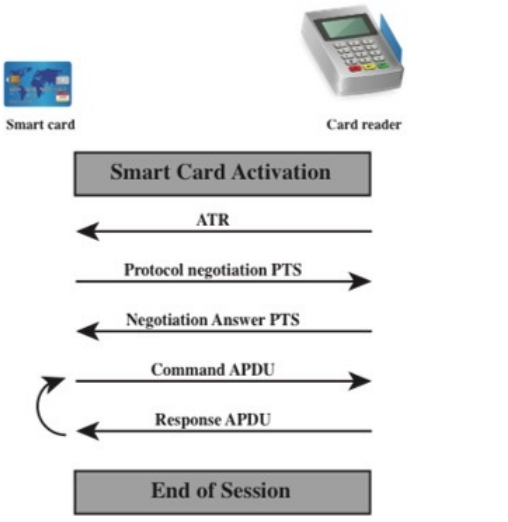


Figure 3.6 Smart Card/Reader Exchange

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)

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 acess 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

Table 3.4

Electronic Functions and Data for eID Cards

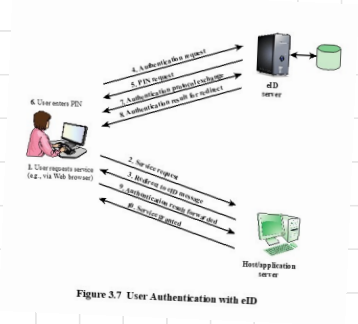
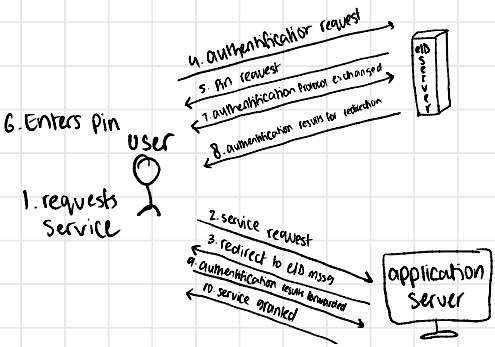


Figure 3.7 User Authentication with eID

An eID user visits a website and requests a service that requires authentication.
The website redirects this request to an eID server, which then asks the user to enter the PIN for their eID card.
After the correct PIN is entered, encrypted data is exchanged between the eID card and the terminal reader.
The server then performs an authentication exchange with the eID card's microprocessor.
If the user is authenticated, the result is sent back to the user's system, which redirects it to the web server.

In this scenario, specific software and hardware are needed on the user's system.
The software includes functions for handling the PIN and message redirection,
while the required hardware is an eID card reader, which can be an external or internal contact or contactless reader.



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

↳ authenticates an individual based on unique physical characteristics
↳ based on pattern recognition
↳ more complex and expensive in comparision → to tokens and passwords

↳ Physical characteristics include

1. Facial characteristics
2. Fingerprints
3. Hand geometry
4. Retinal pattern
5. Iris
6. Signature
7. Voice

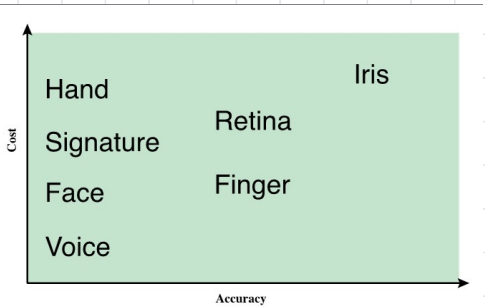


Figure 3.8 Cost Versus Accuracy of Various Biometric Characteristics in User Authentication Schemes.

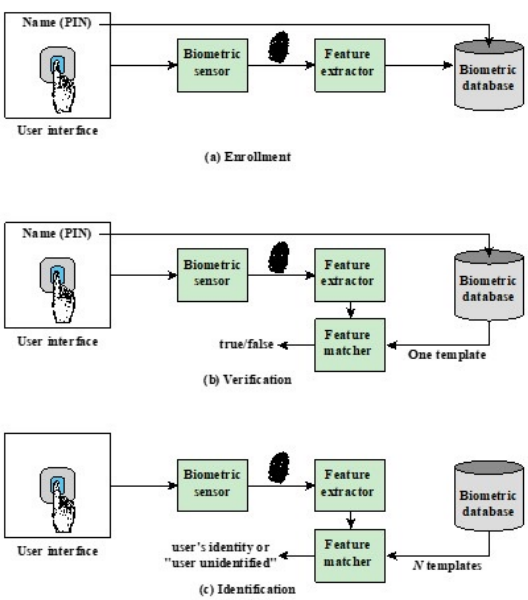


Figure 3.9 A Generic Biometric System. Enrollment creates an association between a user and the user's biometric characteristics. Depending on the application, user authentication either involves verifying that a claimed user is the actual user or identifying an unknown user.

Figure 3.9 shows how a biometric system works.
Each person who will be authorized must first be enrolled, similar to setting up a password.
To enroll, the user provides a name and often a password or PIN, while the system captures a biometric feature (like a fingerprint).
The system then digitizes this feature and creates a set of numbers, known as the user's template, which represents this unique biometric trait.
The system then stores the user's ID, PIN or password, and biometric template.

User authentication in a biometric system can involve either verification or identification:

Verification: The user enters a PIN and uses a biometric sensor.
The system then checks if the scanned biometric feature matches the stored template.
If they match, the user is authenticated.
Identification: The user only uses the biometric sensor without any other information.
The system compares the scanned template to all stored templates.
If it finds a match, the user is identified;
if not, access is denied.

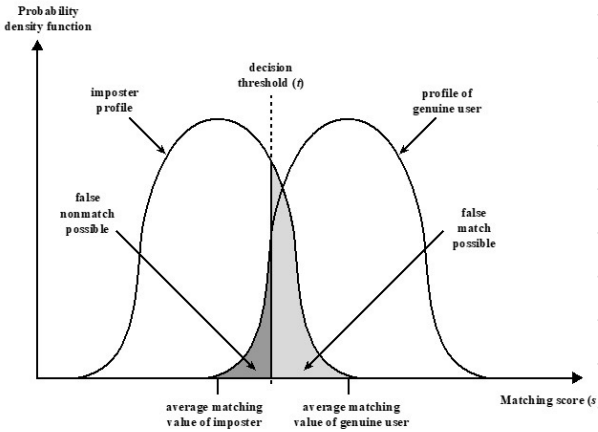


Figure 3.10 Profiles of a Biometric Characteristic of an Imposter and an Authorized Users In this depiction, the comparison between presented feature and a reference feature is reduced to a single numeric value. If the input value (s) is greater than a preassigned threshold (t), a match is declared.

In a biometric system, a physical characteristic of a person is converted into a digital form, or template, which is stored in the computer.
When the user needs to be authenticated, the system compares the stored template to the new template.
Since physical traits vary, an exact match isn't expected.
Instead, an algorithm generates a matching score that measures the similarity between the input and stored templates.

Key terms are:
False match rate: The rate at which samples from different people are mistakenly seen as a match.
False nonmatch rate: The rate at which samples from the same person are mistakenly seen as a non-match.

Figure 3.10 shows the challenge this creates.
If a user is tested repeatedly, their matching score varies, usually forming a bell curve.

For example, fingerprint results can change due to sensor noise, dryness, swelling, or finger placement.
The matching scores of a genuine user and an imposter may overlap.
In Figure 3.10, a threshold value is set:

$s \geq t \rightarrow$ match
$s < t \rightarrow$ not a match

The shaded areas represent where false matches or nonmatches can occur.
Adjusting the threshold changes the false match and nonmatch rates, but reducing one rate increases the other.

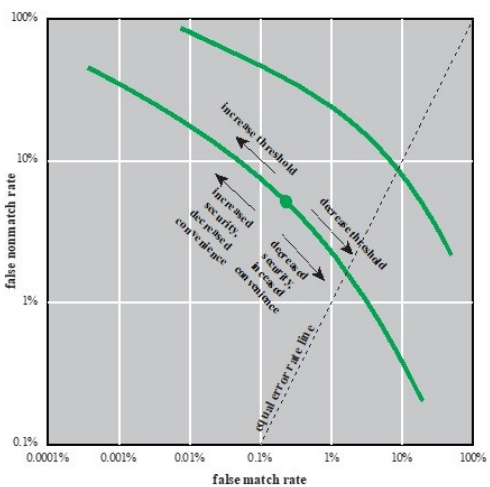


Figure 3.11 Idealized Biometric Measurement Operating Characteristic Curves (log-log scale)

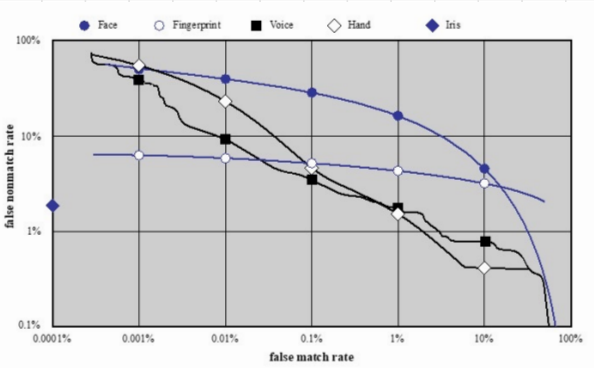


Figure 3.12 Actual Biometric Measurement Operating Characteristic Curves, reported in [MANS01]. To clarify differences among systems, a log-log scale is used.

Local User Authentication

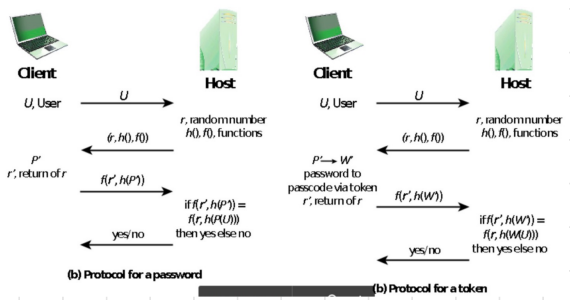
→ simplest method

- where a user accesses a system → e.g. a stand alone office PC or ATM

Remote User Authentication

→ more complex

- occurs over the internet/network
- introduces additional security risks → e.g. • eavesdroppers catching passwords
  • adversaries replaying observed authentication sequences
- uses a challange response protocol against these threats



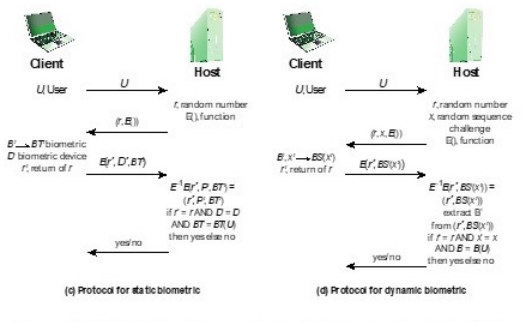


Figure 3.13 Basic Challenge-Response Protocols for Remote User Authentication

Figure 3.13a illustrates a basic password-based challenge-response protocol.
The user first sends their ID to the host, which generates a random number (nonce) and specifies two functions,
h() and f() as a challenge. the user response is .....
The host compares this response with its stored hash for the user's password.
If they match, the user is authenticated.
This approach secures passwords by only storing their hash and prevents capture of passwords during transmission, also defending against replay attacks by using a nonce.

Figure 3.13b shows a token-based protocol.
The user sends their ID, and the host responds with a random number and function identifiers. The user's token generates a passcode , either static or one-time, synchronized with the host.
The user activates the passcode by entering a password shared only with the token. The token then responds with
For a match, the user is authenticated.
This is similar to the password protocol, but the token may add another layer of security.

Figure 3.13c demonstrates a static biometric authentication protocol.
The user sends an ID, and the host replies with a random number and an encryption identifier
The user's device creates a biometric template and responds with the device ID.
The host decrypts this response and compares the biometric data and device ID with stored values.
If both match, the user is authenticated, ensuring that the device and biometric data are verified.

Figure 3.13d illustrates a dynamic biometric protocol.
Here, the host sends a random sequence along with the nonce.
The user then vocalizes, types, or writes the sequence to create a biometric signal
which is encrypted and sent back. The host checks that and compares
with stored data for this user. If the comparison exceeds a certain threshold, the user is authenticated.
This method adds a layer of security by using a live biometric interaction with the sequence challenge.

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 3.5

Some Potential Attacks, Susceptible Authenticators, and Typical Defenses

(Table is on page 96 in the textbook)

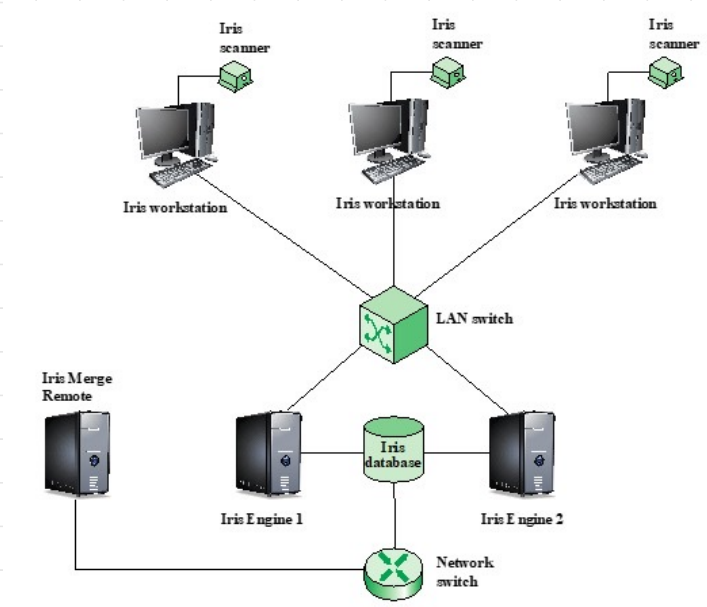
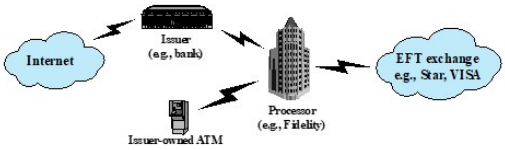
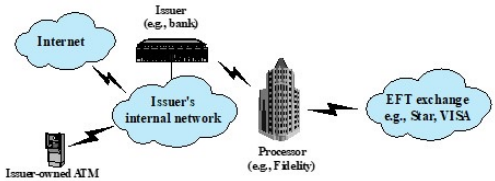


Figure 3.14 General Iris Scan Site Architecture for UAE System



(a) Point-to-point connection to processor



(b) Shared connection to processor

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.

Case Study: ATM Security Problems

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

e) How do the slow hashing function and salt help the password authentication scheme in the UNIX operating system?
The slow hashing function makes brute force and dictionary attacks computationally hard (i.e. time-consuming and resource-intensive). Salting ensures that identical passwords have different hashs in the password database (thwarting rainbow table attacks).

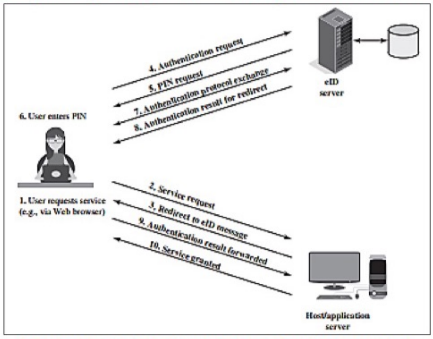
Q3.

Q2 part (e)

a) How do you determine a user's identity while doing THREE different types of authentications? **[1.5]**
There are four general means of authenticating a user's identity, which can be used alone or in combination:

1. Something the individual knows: Examples include a password, a personal identification number (PIN), or answers to a prearranged set of questions.
2. Something the individual possesses: Examples include electronic keycards, smart cards, and physical keys. This type of authenticator is referred to as a token.
3. Something the individual is (static biometrics): Examples include recognition by fingerprint, retina, and face. Or Something the individual does (dynamic biometrics): Examples include recognition by voice pattern, handwriting characteristics, and typing rhythm.

b) Illustrate all stakeholders and protocol exchanges while doing eID authentication. **[1.5]**



Q3 part (b) – textual answers will not be given any marks

Question 2: [CLO # 1]
[1.5 + 1 = 2.5 Points]

a) Illustrate a scenario where Electronic Identity cards (eID) hosted at NADRA eID Server is used by daraz.pk for the sale of small self-defense firearms.
NADRA eID server not only authenticate the user. Optional: It can even do a two factor authentication (without the knowledge of daraz.pk) using the citizens mobile phone number

b) Why biometric authentication is both strong and appropriate in your opinion?
NADRA stores the citizen biometric info. Firearm sale is risky and biometric authentication provides added security (two or multi-factor). It is appropriate, as there is a shipment delay where any physical risk assessment can be performed and action taken.

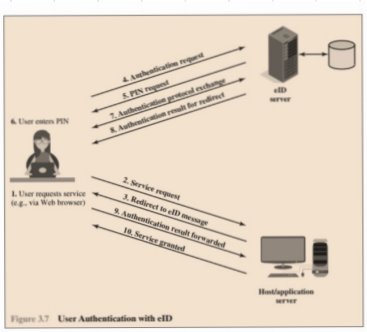


Figure 3.7 User Authentication with eID

Question # 3:

a) Differentiate between malwartizing and click jacking (at least 3 differences). **(3)**

Solution:

Malvertizing:

- 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:

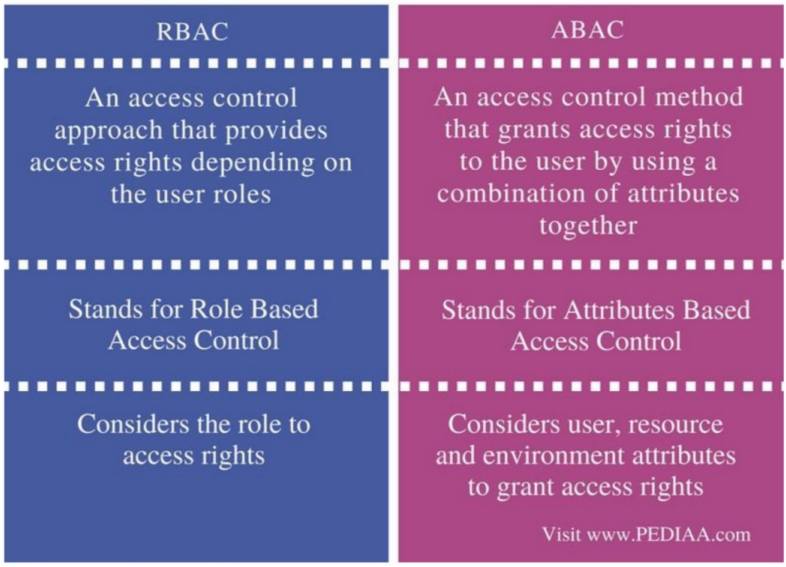
- Vulnerability used by an attacker to collect an infected user's clicks
  - The attacker can force the user to do a variety of things from adjusting the user's computer settings to unwittingly sending the user to Web sites that might have malicious code
  - By taking advantage of Adobe Flash or JavaScript 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

b) Suppose you bought a new smartphone and are enthusiastic about game applications available for it. When you download and start to install one game application, you are asked to approve the access permissions granted to it. It wants permission to "Send SMS messages" and to "Access your address-book". What threat might the application pose to your smartphone, should you grant these permissions and proceed to install it? **(3)**

Solution:

If when you download and start to install some game app, you are asked to approve the access permissions "Send SMS messages" and to "Access your address-book", you should indeed be suspicious that a game wants these types of permissions, as it would not seem needed just for a game. Rather it could be malware that wants to collect details of all your contacts, and either return them to the attacker via SMS, or allow the code to send SMS messages to your contacts, perhaps enticing them to also download and install this malware. Such code is a trojan horse, since it contains covert functions as well as the advertised functionality.

RBAC VERSUS ABAC



Roles examles are HR Manager, Director etc.

Attributes are location, time etc.

p = 283 keys for

$s = B^a \bmod p$ $s = A^b \bmod p$

$196^a \bmod 28$

Diffie-Hellman key exchange

Alice and Bob use the Diffie-Hellman algorithm to exchange a secret key. Eve intercepts the following values:

$p = 283$
$g = 12$
$A = 77$
$B = 196$

(a) What are the steps for Eve to compute s? (3 Marks)

Solution:

Eve has to calculate the discrete logarithm of A base g modulo p (*i. e.*, a) or the discrete logarithm of B base g modulo p (*i. e.*, b).

Assuming Eve found a, then $s = B^a \mod p$. Otherwise $s = A^b \mod p$.

(b) You are Eve. Actually compute s. (3 Marks)

Solution:

Try the possible values for $a = \{1, 2, 3, \ldots, 282\}$.

$12^1 \mod 283 = 12$ ...no.
$12^2 \mod 283 = 144$ ...no.
$12^3 \mod 283 = 30$ ...no.
$12^4 \mod 283 = 77$ success!

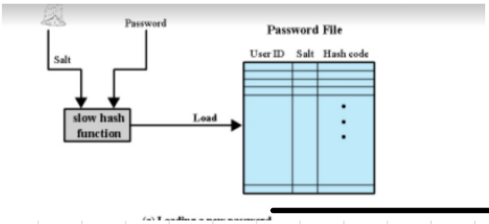
So $a = 4$, therefore $s = B^a \mod p = 196^4 \mod 283 = 90$.

Question # 1: Suppose your organization's employee management system is affected because of the employees' weak password issue. Discuss at least three types of possible password attacks, that could be the cause. **[03 points]**

1) Dictionary attacks
2) Rainbow attacks
3) Brute force attacks
4) Other related attacks

And their details.

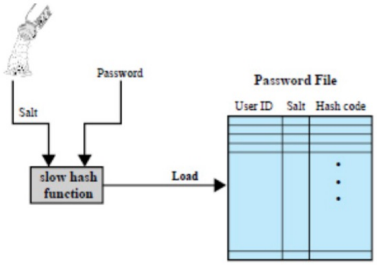
Question # 2: Illustrate Unix Password Scheme with the help of a diagram. **[03 points]**



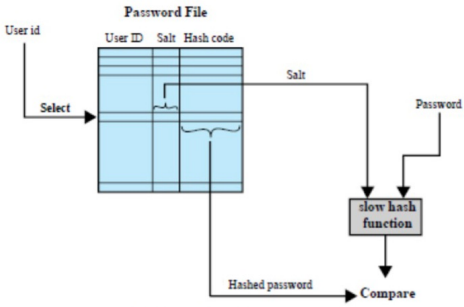
Question 1: [CLO # 1] **[1.5 + 1 = 2.5 Points]**

Illustrate the Unix password scheme with the help of a labelled diagram. Why slow-hash is important? Justify your answer.

Solution:



(a) Loading a new password



(b) Verifying a password

Slow hash is required to add computing delays for attackers trying to break the passwords. A rapidly computed algorithm could make brute-force attacks more feasible, especially with the rapidly evolving power of modern hardware.

Question 3: [CLO # 2] **[1.5 + 1 = 2.5 Points]**

Discuss the key similarities and differences between DAC, RBAC, and ABAC access control models / types. Also give two concrete examples of using some of those four access control types in your real applications or systems.

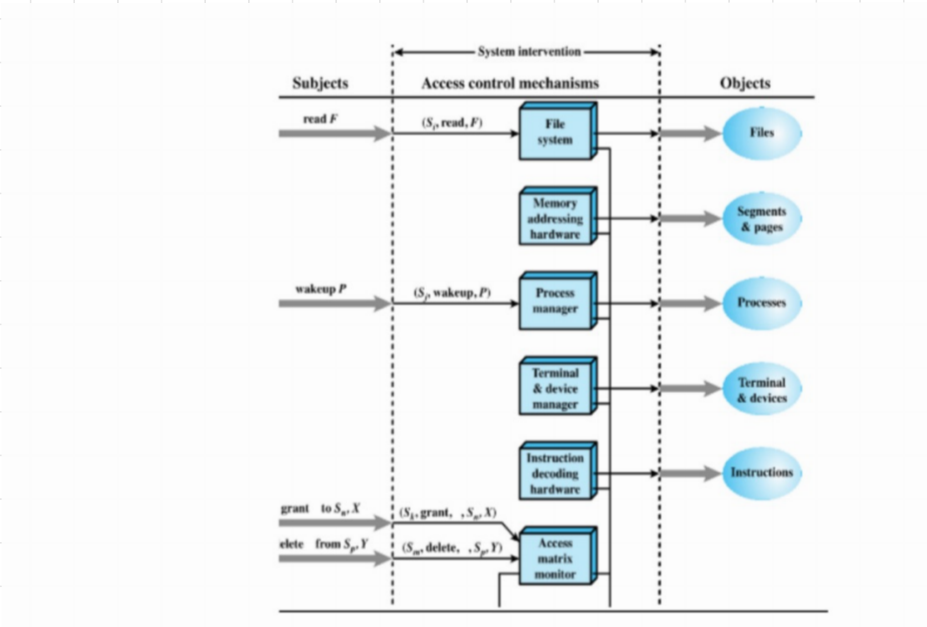
Solution:

All access control policies contain subjects (owners, groups, and world), objects, and access rights. DAC allows for one entity to grant another entity the same access to the same resources and is based on the identity of the user. All information regarding this scheme is contained in organized lists (e.g. Access Matrix, ACL, capability list). One example of this is the log-in system at Mines. Depending on your identity (username), you are granted certain capabilities. For example, I cannot download software on a school computer, but someone with an administrative ID can.

RBAC is not based on the user's identity but the role they play in the organization. Each role has specific access rights and those rights will likely not change frequently. The original RBAC model can be modified to include constraints (mutual exclusivity) or hierarchies. An example of a RBAC model is implemented in the Dresdner Bank, which grants access rights in order of job ranking. In a hierarchical setting, it is assumed the higher position will obtain all the access rights of the lower group.

The ABAC model uses attributes to define subjects, objects, and environment, and is capable of enforcing all the other models. The decision made by access control is dependent on four sources of information: subject/object attributes, AC policy, and environmental conditions.

e. How can an access control function be organized? Illustrate using various control mechanisms.



c) How the values of challenge and response are computed in the challenge-response authentication between a smart device and a computer. [2]

106 CHAPTER 3 / USER AUTHENTICATION

— **Challenge-response:** In this case, the computer system generates a challenge, such as a random string of numbers. The smart token generates a response based on the challenge. For example, public-key cryptography could be used and the token could encrypt the challenge string with the token's private key.

Q3 part (c) – award marks in case of text or diagram

2. In a public-key system RSA, you intercept the ciphertext C =10 sent to a user whose public key is e=5, n=35. What is the plaintext M? [5 Points]

We know that the ciphertext C = 10, and the public key PU = {e, n} = {5, 35}. Based on Euler's Totient function, φ (n) is defined as the number of positive integers less than n and relatively prime to n. We could find that φ (n) = 24.

Now, we guess two prime numbers p and q. Let p be 5 and q be 7. All the following conditions will be satisfied based on the guess: (1) n = p*q = 5*7=35 (2) φ (n) = (p-1)(q-1)=(5-1)(7-1)=4*6=24 (3) gcd(φ (n), e) = gcd(24, 5) =1, 1< e < φ (n)

We calculate d in the next step. Based on RSA key generation algorithm, d ≡ e-1 mod φ (n) which is equivalent to ed ≡ 1 mod φ (n) or ed mod φ (n) =1. (chapter 9.1 page 269)

We have e = 5, φ (n) = 24. So, 5d mod 24 =1, and d = 5.

Now, we find the private key PR = {d, n} = {5, 35}.

Based on RSA decryption algorithm, M = C^d mod n = 10^5 mod 35 = 5

We also can verify the correctness by the RSA encryption algorithm as the following: C = M^e mod n = 5^5 mod 35 = 10 Therefore, we conclude that the plaintext M is 5.

C=10 e=5, n=35 m: ?

n: p x q

n: 5 x 7 → both Prime

ϕ: (5-1)(7-1) = 24

e already given

d x e mod 24 = 1

5d mod 24 = 1

5 x 5 mod 24 = 1

25

d: 5

$d: 10^5 \bmod 35$

$= 100000 \bmod 35$

a) Suppose FLEX has RBAC implemented already. When will ABAC become necessary instead of RBAC? Explain. **[1.5]**

Sol:-

In RBAC permission on objects are granted to roles and roles are assigned to users. ABAC provides attributes to users, objects and environment and a dynamic policy to grant access to objects. This means ABAC can be implemented at a finer level than simple permission on objects in RBAC. Attributes and admission policy could be defined arbitrarily providing utmost flexibility to changing internal and external (compliance) requirements. ABAC can start with a simple model and grows (evolve) into a more complex mechanism that can not be implemented in RBAC (similar to the movie example from the textbook).

b) Give one example each for the following cloud specific threat: Insecure interfaces and APIs, Shared technology issues, Data loss or leakage and Account or service hijacking**. [1.5]**

Sol:-

The student needs to provide any 1 real life example of each of the treat

c) Assume you have been hired by the CSE department to establish an Access Control specification for the computer labs and files in it. Describe the advantages and disadvantages of using Discretionary Access Control (DAC) or Role-Based Access Control (RBAC) to implement your policy. Give a sample specification of access permission for Role-Based Access Control (RBAC) **[2]**

Sol:-

DAC:

Can be very intuitive and easy to implement. However, depending on the number of students, resources, and the permitted accesses, the administration of the security policy can be overwhelming and error prone.

RBAC:

Simplifies administration, assigning users to roles and privileges to roles. Each user can use the privileges that are assigned to the roles that the user is assigned to. Generally, roles are more static and permanent than the user population, therefore, requiring less administration.

Sample specification:

1. **Roles:** student, faculty
2. **Users:** Mary , John
3. **Privileges:** (file1, +read) ; (file1, +write) ; (file1, -read) ; (file1, -write)
4. **User-Role assignment:** (Mary , student) ; (John , faculty)
5. **Role-privilege assignment:**
   students: (file1, +read); (file1, -write)

   Faculty: (file1, +read) ; (file1, +write)

Provide suitable short-answers to the following questions.

a) Why do we need database encryption after the implementation of role-based access control? Give a real-world example.

Sol:-

In top security environments we do not want to disclose all database contents (rows) to users granted permission on a certain table. This means users can only see database table rows if s/he has a key assigned that can decrypt that row. So in a military database, two users having select privilege on a table can see only rows that they can decrypt using their own key. This confidentiality can not be achieved only with access control.

b) A user answers a phone call from an individual claiming to be from IT services and requests the user to confirm their username and password for auditing purposes. Explain the form of malware propagation associated with this phone call.

Sol:-

Social engineering attempts to gain the confidence of an employee and convince that person to divulge confidential and sensitive information, such as usernames and passwords.

d) List three components (code segment) and four phases of malicious software.

Sol:-

The student needs to define: **Infection mechanism**, **Trigger** and **Payload**.

Infection mechanism: The means by which a virus spreads or propagates, enabling it to replicate. The mechanism is also referred to as the **infection vector**.

- **Trigger:** The 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. The payload may involve damage or may involve benign but noticeable activity.

Phases:-

Dormant phase, Propagation phase, Triggering phase, Execution phase

e) Why is RBAC considered fit for database access control?

Sol:-

1. The user issues an SQL query for fields from one or more records with a specific value of the primary key.
2. The query processor at the client encrypts the primary key, modifies the SQL query accordingly, and transmits the query to the server.
3. The server processes the query using the encrypted value of the primary key and returns the appropriate record or records.
4. The query processor decrypts the data and returns the results.

chp 9

FIREWALL AND INTRUSION PREVENTION SYSTEMS

Firewalls

- Protect local systems/networks from security threats
- while allowing access to the internet
- Provide an extra layer of defense
- can consist of 1 or multiple systems working together

Need for Firewall

- Organizations need it as internet access is essential but it brings security risks
- Employees may use personal connections if LANs isnt provided (internet through) which increases vulnerabilities
- It is costly and challenging to equipt every device with security features → eg intrusion protection
  - too many devices
  - scalable configuration and management
  - constant updates
- firewalls act as a protective barrier b/w the organisations network and the internet
- Placed b/w organizations network and the internet

Firewall Acess Policy

- It is essential for planning and implementation
- It defines the allowed types of traffic
  - address ranges
  - protocols
  - applications
  - content
- It is based on the og (organizations)
  - security risk assessment
  - broader security policy
- It is refined to specify filtering rules

Firewall characteristics

1. All network traffic must pass through the firewall
2. Only authorised traffic is allowed
3. Firewall must be secure from attacks

ways firewall Access Policy can filter Traffic

1. IP Address and Protocol values
   - Filters traffic based on
     - source/destination addresses
     - Port no.
     - flow direction
   - used in packet filter and stateful inspection firewalls
     - to limit specific services
2. Application Protocol
   - filters data based on authorised application protocols
     - e.g. checking emails for spam
     - restricting web requests to approved sites
   - used in application level gateways
3. User Identity
   - limits access based on user authentication
   - used for internal users using secure methods e.g. IPSec
4. Network Activity
   - Controls Access based on
     - request rate e.g. restricting to bussiness hours
     - activity patterns e.g. detecting suspicious behavior

Capabilities of a Firewall

Single Choke Point:
- Blocks unauthorized access.
- Prevents vulnerable services from entering or leaving the network.
- Protects against IP spoofing and routing attacks.
- Simplifies security management by centralizing control.

Monitoring Location:
- Allows monitoring of security-related events.
- Supports audits and alarms.

Additional Internet Functions:
- Acts as a network address translator (NAT).
- Logs and audits Internet usage.

Platform for IPSec:
- Supports VPNs using tunnel mode.

Limitations of a Firewall

Bypass Risks:
- Cannot prevent attacks through alternate connections like dial-out or mobile broadband.

Internal Threats:
- Cannot fully protect against insider threats or employees unintentionally aiding attackers.

Wireless LAN Security:
- Cannot secure an improperly protected wireless LAN or communications across internal firewalls.

External Device Risks:
- Devices infected outside the network (e.g., laptops or portable storage) can introduce threats when connected internally.

Firewall Monitoring and Filtering

Firewalls monitor traffic at different levels:
- Low-level packets (individually or as part of a flow).
- Transport connection traffic.
- Application protocol details.

Filtering Approaches:
- Positive filter: Allows only packets meeting specific criteria.
- Negative filter: Blocks packets that meet certain criteria.

Access Policy:
Determines filtering rules.
Firewall may analyze:
- ↳ Protocol headers.
- ↳ Packet payloads.
- ↳ Patterns in packet sequences.

Types Of Firewall

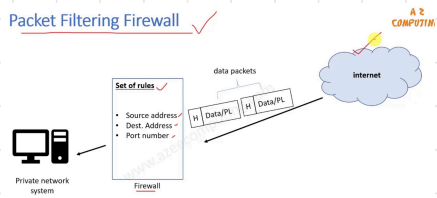
1. Packet Filtering Firewall
2. Stateful Inspection Firewall
3. Application Level Gateway
4. Circuit Level Firewall
5. Host based Firewall
6. Personal Firewall

1. Packet Filtering Firewalls

Function:
Applies rules to each incoming and outgoing IP packet
to decide whether to forward or discard it.
Typically filters packets in both directions (to and from the internal network).

Filtering Rules are based on info contained in a network packet :
Source IP Address: Originating system's IP address (e.g., 192.178.1.1).
Destination IP Address: Target system's IP address (e.g., 192.168.1.2).
Source/Destination Transport-Level Address: Port numbers defining applications (e.g., HTTP, SNMP).
IP Protocol Field: Specifies the transport protocol (e.g., TCP, UDP).
Interface: Determines the source or destination interface on the firewall.

Rules:
Organized as a list based on matches in IP or TCP headers.
A matched rule decides the packet's fate (forward or discard).

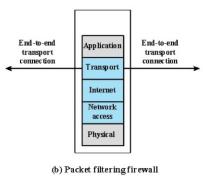


Default action: Taken if no rule matches.

Default Policies:

1.Default = Discard:
- Blocks everything unless explicitly permitted.
- More conservative and secure.
- Requires services to be allowed case by case.
- Preferred by businesses and governments.
- Initially inconvenient for users
  ↳ but less noticeable as rules are added.

2.Default = Forward:
- Allows everything unless explicitly prohibited.
- Easier for users but less secure.
- Security admins must address threats reactively.
- Common in open organizations like universities.



(b) Packet filtering firewall

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

SMTP Traffic Rule Set Example

Goal:
Allow inbound and outbound email (SMTP) traffic.
Block all other traffic.

Rules:
1.Inbound mail from external source allowed (port 25 for SMTP incoming).
2.Response to inbound SMTP connection allowed.
3.Outbound mail to external source allowed.
4.Response to outbound SMTP connection allowed.
5.Default policy: All other traffic is blocked (implicitly included in all rule sets).

Problems with the Rule Set:
1.Rule 4:
Allows external traffic to any destination port above 1023.
This creates a vulnerability, where an attacker can
connect from a high port to an internal web proxy server.
Solution, the source port is specified for each rule:
Rules 2 and 4 use source port 25.
Rules 1 and 3 use source port >1023.

2.Vulnerability in Rules 3 and 4:
SMTP typically uses port 25,
but external systems could use another service on port 25,
allowing an attacker to exploit the rule.
Solution: Add an ACK flag in rule 4.
This ensures that only packets acknowledging
an established connection are allowed.

SOLUTION

Revised Rule 4:
Direction: Inbound
Source address: External
Source port: 25
Destination address: Internal
Protocol: TCP
Destination port: >1023
Flag: ACK
Action: Permit

This rule only allows incoming packets with source port 25 that include the ACK flag, preventing unauthorized access.

Advantages and Weaknesses of Packet Filtering Firewalls

Advantages:

1.Simple to implement.
2.Transparent to users.
3.Fast performance.

Weaknesses:

1.Limited to Packet Information:
Cannot prevent application-specific attacks.
If an application is allowed, all its functions are permitted.
2.Limited Logging:
Logs only basic information like source and destination addresses, and traffic type.
3.Lack of User Authentication:
Most packet filters cannot support advanced user authentication
due to the lack of upper-layer functionality.
4.Vulnerable to Protocol Exploits:
Vulnerable to attacks like network layer address spoofing,
as they cannot detect changes in OSI Layer 3 addressing.
5.Configuration Errors:
Vulnerable to misconfigurations that allow unwanted traffic types, sources, or destinations.

Common Attacks on Packet Filtering Firewalls and Countermeasures

IP Address Spoofing:
Attack: Intruder sends packets with a fake internal IP address to bypass security.
Countermeasure: Discard packets with internal source addresses
if received on external interfaces (often done at the router).

Source Routing Attacks:
Attack: Attacker specifies the route a packet should take to bypass firewall security.
Countermeasure: Discard packets using source routing.

Tiny Fragment Attacks:
Attack: Attacker fragments the packet into tiny pieces, hoping the firewall only inspects the first fragment and allows malicious content in the other fragments.
Countermeasure: Enforce a rule that the first fragment must include a minimum amount of transport header information.
If rejected, all fragments are discarded.

Summary of Traditional Packet Filters and Their Limitations:

Traditional Packet Filter:
Makes decisions based only on individual packets
without considering the higher-layer context (like the state of the connection).

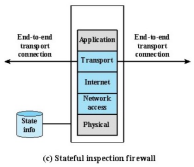
some bg for understanding
Client-Server Model:
Most TCP-based applications, like SMTP (for email), work on a client-server model
where the client initiates communication and the server listens for incoming connections.

TCP Connections:
The server application uses a well-known port (less than 1024),
while the client uses a dynamic port (between 1024 and 65535).
Example: SMTP uses port 25 on the server side, and a dynamic port on the client side.

Vulnerability:
Since traditional packet filters allow inbound traffic on high-numbered dynamic ports,
unauthorized users can exploit this vulnerability to bypass security measures.

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



(c) Stateful inspection firewall

inspect applications

TCP connections

2. Stateful Inspection Packet Firewall:

Stateful Inspection Firewall:
- Enhances packet filtering by maintaining a directory of outbound TCP connections.
  - as shown in Table 9.2 . There is an entry for each currently established connection.
- Only allows incoming traffic to high-numbered ports if it matches an established connection in the directory.

Functionality:
- Similar to packet filtering but also tracks the state of TCP connections.
  - Some firewalls track TCP sequence numbers to prevent attacks like session hijacking.
  - Can inspect application data for protocols
    - like FTP, IM, and SIPS

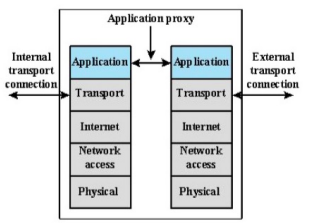
to identify and track related connections.

inspect users

3. Application-Level Gateway (Application Proxy):

Function:
Acts as a relay for application-level traffic (e.g., Telnet, FTP).
User contacts the gateway,
- which asks for the remote host name and user authentication.

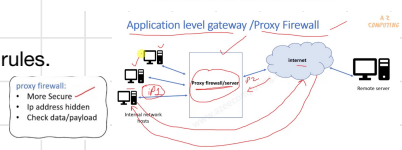
The gateway relays application data between the user and the remote host.
If the gateway doesn't support the application, the service is blocked.
The gateway can be configured to allow only specific features of an application.



(d) Application proxy firewall

Security:
More secure than packet filters
- as it focuses on a few allowed applications rather than multiple TCP/IP rules.

Allows easy logging and auditing of incoming traffic at the application level.



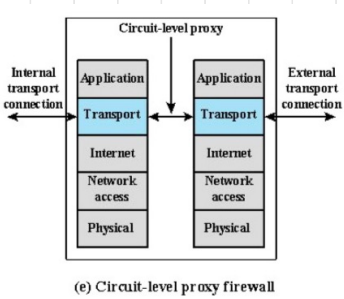
Disadvantage:
Adds processing overhead
- as the gateway examines and forwards all traffic in both directions between the users.

4. Circuit-Level Gateway (Circuit-Level Proxy):

Function:
Sets up two TCP connections:
- one between the gateway and an internal host, and
- one between the gateway and an external host.

Once the connections are established,
- it relays TCP segments between the two connections
- without inspecting the content.

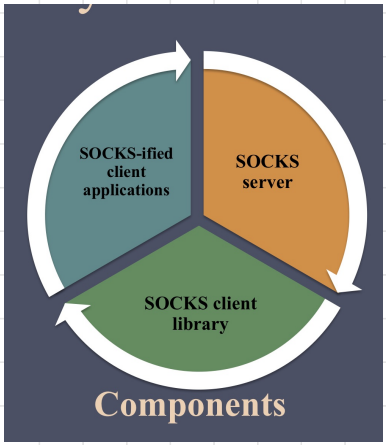
Security is based on determining which connections are allowed.



(e) Circuit-level proxy firewall

Use Case:
Often used when internal users are trusted.
Can combine application-level proxy for
- inbound traffic and circuit-level functionality for outbound traffic,
- reducing processing overhead for outgoing data.

SOCKS Protocol



Purpose:
SOCKS provides a framework for client-server applications (TCP and UDP)
↳ to securely use network firewall services.
It acts as a "shim-layer" between the application layer and the transport layer,
↳ but does not forward ICMP messages.

AL
TL

Components:
SOCKS server: Usually runs on UNIX-based firewalls,
↳ but also available for Windows systems.
SOCKS client library: Runs on internal hosts protected by the firewall.
SOCKS-ified client programs: Applications like FTP and Telnet,
↳ modified to use SOCKS via recompilation or dynamic libraries.

Operation:
A TCP client connects to the SOCKS server (TCP port 1080)
↳ to establish a connection.
After a successful connection,
↳ the client negotiates the authentication method and authenticates.
The SOCKS server then evaluates the connection request
↳ and either establishes the connection or denies it.
For UDP, a TCP connection is used for authentication,
↳ and UDP segments are forwarded as long as the TCP connection remains open.

Bastion Host:

Definition:
A bastion host is a critical, secure system
identified by the firewall administrator to protect the network.
It often serves as a platform for application-level or circuit-level gateways.

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

5. Host-Based Firewall

It is a software used to secure an individual computer or server.
It can be part of the operating system or added separately.
It filters and controls data flow like traditional firewalls.

Advantages of host-based firewalls:
Customizable Rules:
Filtering rules can be set specifically for the host,
allowing tailored security policies for servers and different applications.
Independent Protection:
Protection is provided regardless of the network's structure,
stopping both internal and external attacks.
Extra Layer of Protection:
When combined with traditional firewalls,
it adds an additional security layer,
allowing new servers with their own firewalls
without changing the network's firewall setup.

6. Personal Firewall

A personal firewall controls traffic between
↳ a computer and the Internet or network,
used in home and corporate environments.
It is typically software on the computer or can be housed in a router for multiple home computers.

Key Functions:
Deny Unauthorized Access: Blocks unauthorized remote access to the computer.
Monitor Outgoing Activity: Detects and blocks malware, like worms.
Inbound and Outbound Connections:
Inbound connections are blocked by default,
↳ except those allowed by the user.
Outbound connections are usually allowed.

Types Of Firewalls Summary

1. **Packet Filtering Firewall**:
   Filters packets based on IP addresses, ports, and protocols.
   Simple but limited in scope.

2. **Stateful Inspection Firewall:**
   Monitors the state of active connections and determines which packets to allow based on the context.

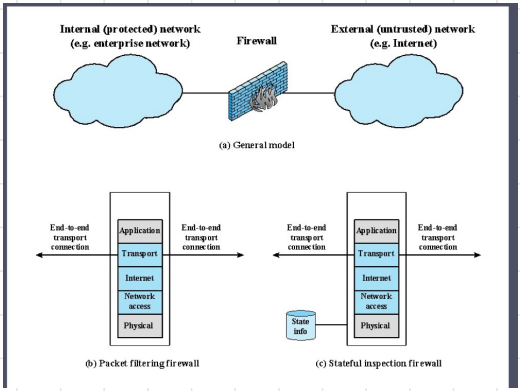
3. **Application-Level Gateway (Proxy Firewall):**
   Intermediates between internal and external systems, providing detailed inspection.

4. **Circuit-Level Gateway:**
   Operates at the session layer to validate connections.

5. **Personal Firewall:**
   Software designed to protect individual systems.

6. **Host Firewall:**
   Software designed to protect an individual computer or server.

Benefits:
Centralized security control and traffic monitoring.
Prevention of unauthorized access and traffic filtering.
Limitations:
Ineffective against internal threats or encrypted traffic.
Requires proper configuration to avoid vulnerabilities.



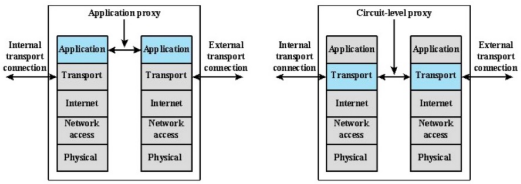


Figure 9.1 Types of Firewalls

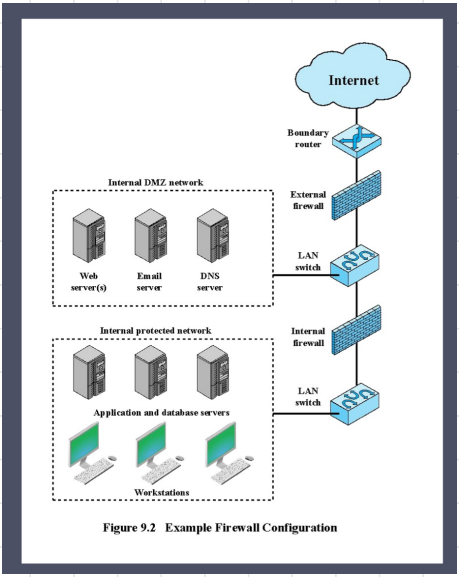


Figure 9.2 Example Firewall Configuration

Firewall Configuration with DMZ

Firewall Setup:
A common configuration includes an external firewall, internal firewalls, and a DMZ (Demilitarized Zone) network,
as shown in Figure 9.2

DMZ:
Located between the external and internal firewalls,
the DMZ contains systems needing external access
but requiring protection,
such as a corporate website, email server, or DNS server.

Roles of the External Firewall:
Provides access control for the DMZ systems and basic protection for the internal network.

Roles of the Internal Firewall:
Stronger Protection:
Offers more stringent filtering to protect servers and workstations from external attacks.
Two-Way Protection:
Protects the internal network from attacks originating in the DMZ.
Protects the DMZ from attacks coming from the internal network.
Segregating Internal Network:
Multiple internal firewalls can separate parts of the internal network, such as protecting servers from workstations. Figure 8.5 shows this setup and the use of different interfaces for the DMZ and internal network access.

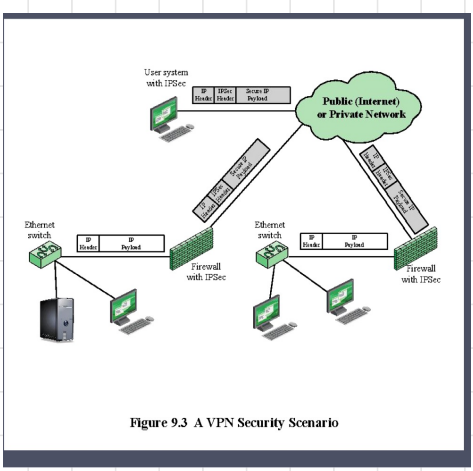


Figure 9.3 A VPN Security Scenario

Virtual Private Network (VPN) and IPSec

VPN Overview: A VPN connects computers over an insecure network (like the Internet) using encryption and special protocols for security.
Cost-Effective Solution: It allows corporate sites with LANs to connect via a public network, such as the Internet,
saving costs and offloading network management to the public provider.
Remote Access: VPNs also provide secure access for telecommuters and remote workers to connect to corporate systems.

Security Concern:
Public networks expose corporate data to risks like eavesdropping and unauthorized access. VPNs address this by using encryption and authentication at the lower protocol layers to secure the connection.

Common Protocol - IPSec:
IPSec is the standard protocol for
encrypting and authenticating traffic at the IP level.
How IPSec Works:
It encrypts and compresses traffic going to and from a public or private WAN
via networking devices like routers or firewalls.
These devices handle encryption transparently,
without impacting LAN workstations or servers.
Remote User Security: Users dialing into the WAN must also implement IPSec protocols and strong security to avoid attacks.

Implementation Considerations:
IPSec can be implemented within a firewall, as shown in Figure 9.3,
but if placed inside the firewall, VPN traffic is encrypted, and the firewall cannot perform its usual security functions (e.g., access control or virus scanning).
Alternatively, IPSec can be implemented outside the firewall,
in the boundary router, but this device may be less secure than a firewall.

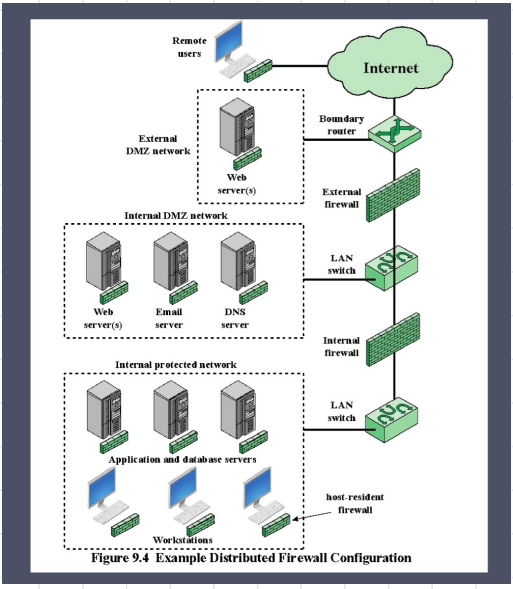


Figure 9.4 Example Distributed Firewall Configuration

Distributed Firewall Configuration

Distributed Firewall Setup:
IT combines stand-alone firewall devices with host-based firewalls,
all under central administrative control.
This configuration, as shown in Figure 9.4,
allows administrators to configure host resident firewalls on servers, workstations, and personal user systems.

Centralized Control:
Administrators can set policies and monitor security across the entire network,
protecting against internal attacks and providing tailored protection for specific machines and applications.

External and Internal DMZs:
With distributed firewalls, both internal and external DMZs may be used.
External DMZ: Web servers with less critical information can be placed outside the external firewall, protected by host-based firewalls.

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 System (IPS)

Definition:
attempts to block or prevent detected malicious activities
by monitoring and analysing network or system activities

3 Types:
1. Host-Based IDS (HIDS): Monitors activities on individual systems.
2.Network-Based IDS (NIDS): Monitors network traffic for suspicious patterns.
3.Hybrid IDS: Combines host and network-based monitoring.

Detection Methods:
1.Anomaly Detection: Identifies unusual behavior ,not typical of legitimate users.
2.Signature/Heuristic Detection: Recognizes known malicious activities.

Response Actions:
Modifies or blocks network packets across a perimeter or host.
Blocks or modifies system calls by programs on a host.

Functionality Comparison:
Like a firewall, it blocks traffic.
Uses IDS-developed algorithms to decide when to block.
Sometimes considered a new product type or another form of a firewall.

c) Explain signature based and anomaly-based detection. How Anomaly based detection is better than signature-based detection? **(3)**

Solution:

Signature Based 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 Based 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.

Why better: Anomaly based detects novel attacks

Examples
1. Snort inline
2. Unified Threat management systems

HIPS (Host-based Intrusion Prevention System):

Purpose
- HIPS detects and analyzes attacks.
- It can be tailored for specific platforms (e.g., desktops, servers).
- Some HIPS tools focus on specific server types (e.g., Web servers, database servers).

Detection Techniques:
- Uses signature detection and anomaly detection.
- Employs a sandbox to isolate and analyze code (e.g., Java applets, scripts).
- Runs quarantined code in a controlled environment.
- Stops code if it violates policies or matches malicious behavior.

Desktop Protection Areas:
- System Calls:
  Monitors kernel-level access to resources (memory, I/O, processor).
  Examines system calls for malicious activity.
- File System Access:
  Ensures file operations follow policies and are non-malicious.
- Registry Settings:
  Protects system registry from unauthorized modifications.
- Host I/O Communications:
  Monitors local and network communications to block exploit propagation.

Endpoint Security and Role of HIPS:

Focus on Endpoint Security:

- Hackers now target enterprise endpoints (desktops and laptops) more than network devices.
- Security vendors are emphasizing endpoint security products.

Traditional vs. HIPS Approach:

- Traditional endpoint security includes separate tools:
  - antivirus, antispyware, antispam, and firewalls.
- HIPS integrates these functions into a single suite for:
  - Better collaboration between tools.
  - Comprehensive threat prevention.
  - Easier management.

Endpoint vs. Network Security:

- Example: The San Diego Supercomputer Center reported no intrusions in four years
  - with only endpoint security and no firewalls.
- Best practice: Use HIPS as part of a layered security strategy that includes
  - network-level devices (e.g., firewalls, network-based IPS).

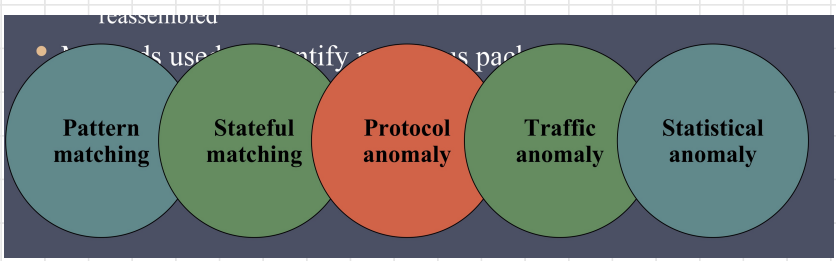
Network-Based IPS (NIPS)

Definition:
NIPS is like an inline NIDS but can discard packets and terminate TCP connections.

Techniques Used:
Similar to NIDS: Signature detection and anomaly detection.
Unique to NIPS: Flow data protection.

Flow Data Protection:
Reassembles application payload from a packet sequence.
Filters content of the flow with every new packet.
Drops malicious flows (current and future packets).

Methods to Identify Malicious Packets:
Pattern Matching: Detects known attack signatures in packets.
Stateful Matching: Considers the context of traffic streams.
Protocol Anomaly Detection: Flags deviations from standard protocols.
Traffic Anomaly Detection: Identifies unusual behaviors (e.g., UDP floods, new services).
Statistical Anomaly Detection: Monitors traffic baselines and flags deviations



Distributed or Hybrid IPS

Distributed/Hybrid IPS:
Combines host-based and network-based sensors.
Central analysis system gathers, correlates, and analyzes data.
Updates signatures and behavior patterns to coordinate system responses.

Digital Immune System:

Developed by IBM, refined by Symantec.
Created to combat rapidly spreading Internet-based malware.
Offers a global defense view.

How It Works:
Captures and analyzes new malware.
Provides detection and shielding against it.
Removes malware and shares information with client systems to prevent further spread.

Goal:
Rapidly respond to malware to neutralize it as soon as it appears.

Success Factors:
Relies on robust malware analysis to detect new and evolving threats.
Continuously updates to counteract emerging malware.

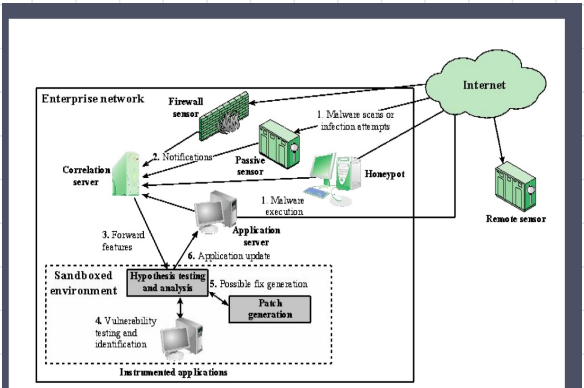


Figure 9.5 Placement of Malware Monitors (adapted from [SIDI05])

Hybrid Architecture for Malware Detection

Step 1: Sensors
- Placed across network and host locations.
- Detect malware activities (scanning, infection, execution).
- Can include IDS sensor logic.

Step 2: Alerts to Server
- Sensors send alerts and malware samples to a central server.
- Server correlates and analyzes data to identify potential malware and its characteristics.

Step 3: Sandbox Analysis
- Central server sends suspected malware to a protected sandbox for testing.

Step 4: Vulnerability Testing
- The Protected environment tests malware against a version of the targeted application.
- Identifies the specific vulnerability being exploited.

Step 5: Patch Creation
- Protected system creates and tests software patches.

Step 6: Patch Deployment
- If the patch works (resistant to infection and no functionality issues), it is sent to update the affected application.

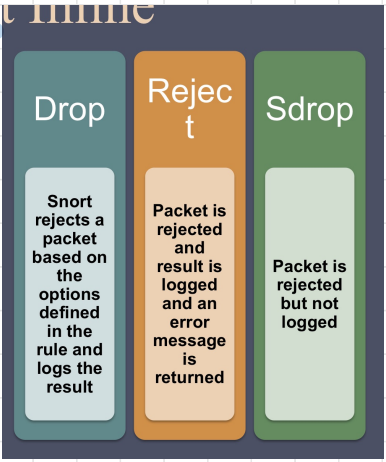
EXAMPLES OF IPS

1. Snort Inline (Enhanced Snort for Intrusion Prevention)

What is Snort Inline:
A modified version of Snort (lightweight intrusion detection system).
Functions as an intrusion prevention system by adding new rule types.

New Rule Types:
Drop:
Rejects a packet based on rule options and logs the result.
Reject:
Rejects a packet, logs it, and sends an error message:
TCP: Sends a TCP reset message to reset the connection.
UDP: Sends an ICMP port unreachable message.
Sdrop:
Rejects a packet without logging it.

It also has a Replace Option:
Allows packet modification instead of dropping it.



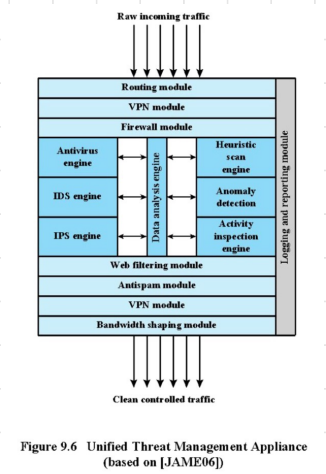


Figure 9.6 Unified Threat Management Appliance (based on [JAME06])

Defense in Depth:

Combines antivirus, antiworm, IPS, IDS, firewalls, etc., for layered defense.
Challenges:
Requires managing multiple devices and software.
Sequential deployment reduces performance.

2. Unified Threat Management (UTM):

Combines multiple security features in one device.
Functions include:
Network firewalling.
Network intrusion detection/prevention.
Gateway antivirus.
IDC Definition: Must inherently support all these features, even if not used simultaneously.
Performance Issues:
UTM devices often reduce throughput by 50%.
High-performance devices recommended to minimize degradation.

UTM Appliance Architecture (Figure 9.6):
Step 1: Decrypt inbound traffic (e.g., IPSec for VPNs).
Step 2: Firewall module filters traffic, discards violating packets.
Step 3: Modules process packets/flows across protocol levels.
Data analysis engine coordinates antivirus, IDS, and IPS engines.
Step 4: Data engine reassembles multipacket payloads for:
Antivirus scanning.
Web filtering and antispam checks.
Step 5: Reencrypt traffic as needed for internal network security.
Step 6: Threats reported to logging module for alerts and forensic analysis.
Step 7: Bandwidth-shaping module optimizes performance using QoS algorithms.

Table 9.3

Sidewinder G2 Security Appliance Attack Protections Summary - Transport Level Examples

Attacks and Internet Threats		Protections	
TCP			
•Invalid port numbers •Invalid sequence numbers •SYN floods •XMAS tree attacks •Invalid CRC values •Zero length •Random data as TCP header	•TCP hijack attempts •TCP spoofing attacks •Small PMTU attacks •SYN attack •Script Kiddie attacks •Packet crafting: different TCP options set	•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	•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			
•Invalid UDP packets •Random UDP data to bypass rules	•Connection prediction •UDP port scanning	•Verify correct UDP packet •Drop UDP packets on ports not open	

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

As an example of the scope of a UTM appliance, Tables 9.3 and 9.4 . lists some of the attacks that the UTM device marketed by Secure Computing is designed tocounter.

Table 9.4

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

Attacks and Internet Threats	Protections	
DNS		
Incorrect NXDOMAIN responses from AAAA queries could cause denial-of-service conditions.	•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.	•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.	•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		
•FTP bounce attack •PASS attack •FTP Port injection attacks •TCP segmentation attack	•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	•Smart proxy protected by Type Enforcement Technology •Hide Internal DB through nontransparent connections	
Real-Time Streaming Protocol (RTSP)		
•Buffer overflow •Denial of service	•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		
•SNMP flood attacks •Default community attack •Brute force attack •SNMP put attack	•Filter SNMP version traffic 1, 2c •Filter Read, Write, and Notify messages •Filter OIDs •Filter PDU (Protocol Data Unit)	

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

Table 9.4

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

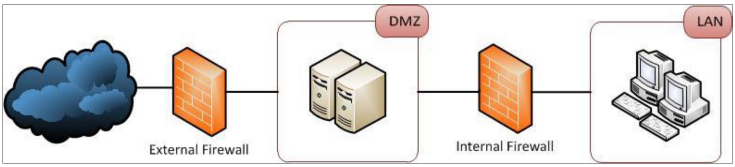
SSH			
•Challenge-Response buffer overflows •SSHD allows users to override "Allowed Authentications" •OpenSSH buffer_append_space buffer overflow •OpenSSH/PAM challenge Response buffer overflow •OpenSSH channel code offer-by-one		Sidewinder G2 v6.x's embedded Type Enforcement technology strictly limits the capabilities of Secure Computing's modified versions of the OpenSSH daemon code.	
SMTP			
•Sendmail buffer overflows •Sendmail denial of service attacks •Remote buffer overflow in sendmail	•Sendmail address parsing buffer overflow •SMTP protocol anomalies	•Split Sendmail architecture protected by Type Enforcement technology •Sendmail customized for controls	•Prevents buffer overflows through Type Enforcement technology •Sendmail checks SMTP protocol anomalies
•SMTP worm attacks •SMTP mail flooding •Relay attacks •Viruses, Trojans, worms	•E-mail Addressing spoofing •MIME attacks •Phishing e-mails	•Protocol validation •Anti-spam filter •Mail filters – size, keyword •Signature antivirus	•Anti-relay •MIME/Antivirus filter •Firewall antivirus •Anti-phishing through virus scanning
Spyware Applications			
•Adware used for collecting information for marketing purposes •Stalking horses •Trojan horses	•Malware •Backdoor Santas	•SmartFilter® URL filtering capability built in with Sidewinder G2 can be configured to filter Spyware URLs, preventing downloads.	

e can be found on pages 312 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

b. Propose a secure architecture for the network in such a way that your company's Webserver and Mail server can be contacted from outside without any restriction and the intranet is kept hidden from outside.

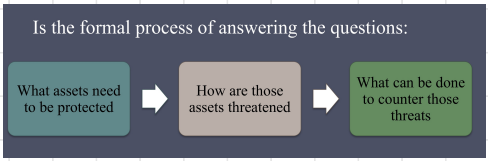


IT SECURITY MANAGEMENT

Chp 14

IT Security Management

is a process to maintain:
Confidentiality, Integrity, Availability, Accountability, Authenticity, and Reliability.



Purpose:
Ensures critical assets are protected cost-effectively.
Answers key security questions about assets and risks.

Steps in IT Security Management:

Define IT security objectives, strategies, and policies.
Perform risk assessments to analyze threats and determine risks.
- ↳What needs protection?
- ↳What are the risks?
- ↳How can risks be mitigated or accepted?

Select cost-effective controls for IT protection.
Develop security plans and procedures.
Implement controls with security awareness and training programs.
Monitor and maintain controls, detect, and respond to incidents.

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 Framework

Key Functions of IT Security Management:

1.Set objectives, strategies, and policies for IT security.
2.Determine organizational IT security requirements.
3.Identify and analyze security threats to IT assets.
4.Conduct risk analysis.
5.Specify and implement safeguards to mitigate risks.
6.Monitor safeguards for effectiveness and cost-efficiency.
7.Create a security awareness program for the organization.
8.Detect and respond to security incidents.

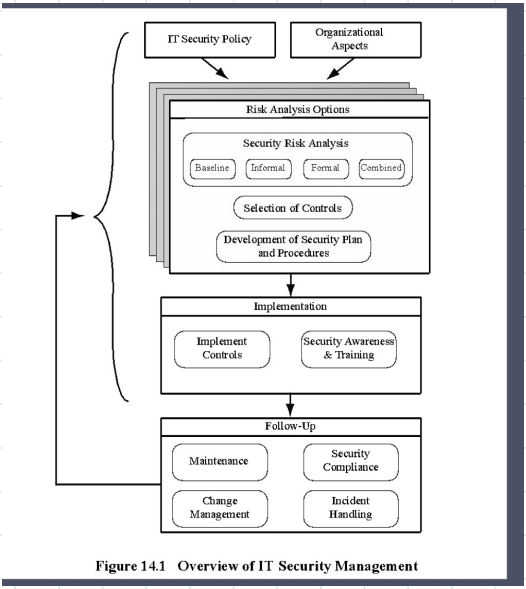


Figure 14.1 Overview of IT Security Management

IT Security Management Process

(Figure 14.1 Reference)

Illustrated Framework:

- Based on ISO27005 (2005) and ISO13335 (Part 3).
- Focuses on risk assessment details within IT security management.

Integration into Management:

- IT security management should align with the organization's overall management plan.
- Risk assessment for IT security should integrate with broader organizational risk assessments.

Role of Senior Management:

- Essential for senior management to:
  - Be aware of IT security processes.
  - Provide active support to ensure security objectives align with business goals.

Continuous Process:

- IT security management is cyclical, not a one-time task.
- Regular updates are required to address:
  - Rapid changes in IT technology.
  - Evolving risks in the environment.

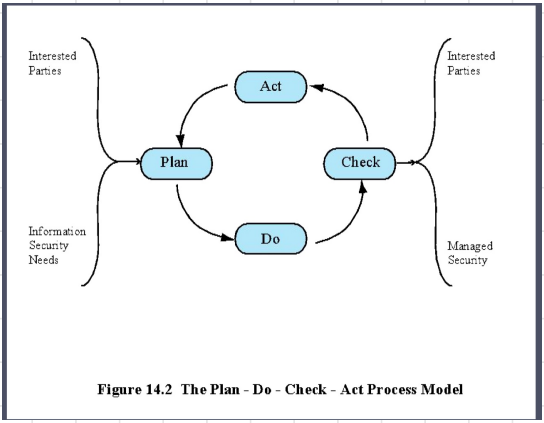


Figure 14.2 The Plan - Do - Check - Act Process Model

Security Risk Management Process

Iterative Model:

- Highlighted in ISO 31000 (Risk management principles, 2009).
- Applied to information security in ISO 27005.

Steps in the Model Process (Plan-Do-Check-Act Cycle):

Plan:

- Define security policies, objectives, processes, and procedures.
- Conduct risk assessments.
- Create a risk treatment plan with selected controls or decide to accept certain risks.

Do:

- Implement the risk treatment plan.

Check:

- Monitor and maintain the plan to ensure effectiveness.

Act:

- Improve the risk management process based on incidents, reviews, or changes in circumstances.

Illustration: Figure 14.2 aligns with Figure 14.1, showing this iterative process.

Outcome: Ensures security needs of all relevant stakeholders are effectively addressed.

Initial Steps in IT Security Management

1. Examine Objectives, Strategies, and Policies:

Review IT security in the context of broader organizational goals and risk profile.

- Objectives: Define IT security outcomes (e.g., legal requirements, standards, individual rights).
- Strategies: Describe how objectives will be achieved.
- Policies: Detail what actions are necessary to meet objectives.
- Regular updates are crucial to adapt to evolving risks and technology.

2.Assess IT Systems' Role and Importance:

Determine the significance of IT systems for organizational goals.
Evaluate value beyond costs, focusing on contribution to efficiency and decision-making.

3.Key Questions to Clarify IT Needs:

Which organizational functions rely on IT to operate efficiently?
What tasks can only occur with IT support?
What decisions depend on data managed by IT systems?
What data needs protection?
What are the consequences of IT system failures?

4.Risk Assessment and Action:

Identify risks to IT systems if they are critical to organizational success.
Address identified weaknesses through appropriate actions.

5.Develop Key Security Objectives:

Create a list of objectives based on organizational needs and IT importance.

6.Formulate Strategy Statements:

Broad strategies should describe how to consistently achieve objectives.
Content should align with organizational size, IT role, and identified goals.
Include methods for managing IT security effectively.

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

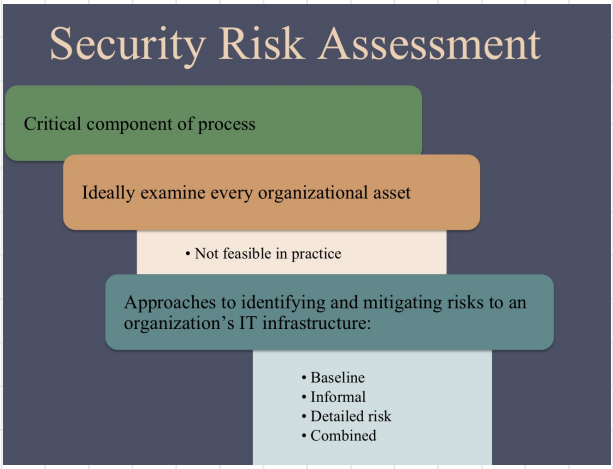
Senior Management Approval and Support:
Essential for ensuring adequate resources and emphasis on IT security.
Visible support encourages seriousness about security at all organizational levels.
Demonstrates due diligence in risk management.

Shared Responsibility and Central Control:
IT security responsibility is shared across the organization.
Risks include inconsistent implementation and loss of central monitoring/control.

Role of IT Security Officer:
Assign overall responsibility to a single person with IT security expertise.

Responsibilities include:
- Overseeing IT security management.
- Liaising with senior management.
- Maintaining IT security objectives, strategies, and policies.
- Coordinating responses to security incidents.
- Managing awareness and training programs.
- Interacting with project security officers.

Role of IT Project Security Officers (for Larger Organizations):
Develop and maintain security policies for specific systems.
Implement and monitor system-specific security plans.
Investigate incidents involving their systems.



IT Security Risk Management

Importance of Risk Management:
Prevents ineffective resource allocation.
Avoids leaving some risks unaddressed and deploying unnecessary safeguards.

Challenges in Risk Assessment:
Evaluating every asset and risk is impractical due to time and resource constraints.
Rapid changes in IT and threat environments can quickly render assessments outdated.

Acceptable Risk Levels:
Eliminating all risks is impossible.
Resources should be spent proportionally to the potential impact and likelihood of risks.
Prudent management involves balancing risk mitigation with budget, time, and personnel limits.

Objective of Risk Assessment:
Provides management with actionable information to allocate resources effectively.

Variety in Organizational Needs:
Different organizations (small businesses to governments) require tailored risk management methods.

Risk Assessment Approaches

1. Baseline Approach
2. Informal Approach
3. Detailed Risk Analysis
4. Combined Approach

1. Baseline Approach

Definition:

- Implements general security controls based on baseline documents, codes of practice, and industry best practices.

Advantages:

- No need for extensive resources or formal risk assessment.
- Easily replicable across multiple systems.

Disadvantages:

- Does not account for organizational-specific risks.
- Baseline level might be:
  - Too high: Leading to unnecessary costs or restrictive measures.
  - Too low: Leaving gaps and vulnerabilities.

Goal:

- Protect against common threats using widely accepted practices
- Acts as a foundation for additional security measures.

Best Use Cases:

- Suitable for small organizations with limited resources.
- Ensures a basic security level beyond the often insecure default configurations of many systems.

2. Informal Approach

Definition:

- Conducts a non-structured, practical risk analysis using the knowledge of internal experts or external consultants.

Advantages:

- No need for additional skills, so it is quick and inexpensive.
- Provides specific insights into risks and vulnerabilities of the organization's systems.
- More accurate and targeted controls compared to the baseline approach.

Disadvantages:

- No formal process, so some risks may be overlooked.
- Results may be biased by the perspectives of those conducting the analysis.
- Lack of strong justification for controls could lead to doubts about the costs involved.
- Inconsistent results over time due to varying levels of expertise among analysts.

Best Use Cases:

- Suitable for small to medium-sized organizations where IT systems aren't critical to the business.
- Ideal when there is no budget for more formal risk assessments.

most comprehensive approach

3. Detailed Risk Analysis

Definition:
A formal, structured process to assess risks to IT systems in an organization.

Process Involved:
Identification of assets.
Identification of threats and vulnerabilities.
Determination of the likelihood of risks and their potential impact.
Selection and implementation of appropriate controls to address identified risks.

Advantages:
Provides the most detailed analysis of IT system security risks.
Strong justification for the expenditure on proposed controls.
Helps in managing the evolving security of systems over time.

Disadvantages:
High cost in terms of time, resources, and expertise.
May cause delays in implementing protection for some systems.

Best Use Cases:
Legal requirement for some government organizations or critical service providers.
Recommended for large organizations with critical IT systems and resources to support the analysis.

most cost effective approach

4. Combined Approach

Definition:
Combines elements of the baseline, informal, and detailed risk analysis approaches.
Aims to provide quick protection, then adjust and refine controls over time.

Process Involved:
Start by implementing baseline security on all systems.
Perform a high-level risk assessment to identify critical or high-risk systems.
Conduct informal risk assessments on key systems to tailor controls.
Perform detailed risk analysis on key systems over time for refined protection.

Advantages:
Provides a basic level of security early through baseline and informal assessments.
Resources are focused on the most critical and high-risk systems.
Develops a strategic view of IT resources and major risks.
Easier to justify to management than conducting a full detailed risk analysis upfront.

Disadvantages:
If the initial high-level analysis is inaccurate, some systems may remain vulnerable until a detailed analysis is done.
Potential delay in addressing some risks, though baseline security should provide minimum protection.

Risk Assessment Approaches summary

1. Baseline Approach
Description: Uses basic, standardized security controls.
Pros: Simple, quick, cost-effective.
Cons: Not tailored to specific risks, too high to too low

2. Informal Approach
Description: Relies on expert judgment without structure.
Pros: Flexible, low-cost.
Cons: Biases, Inconsistent, may miss risks.

3. Detailed Risk Analysis
Description: Comprehensive evaluation of assets, threats, and vulnerabilities.
Pros: Strong risk insights, justified controls.
Cons: Time-consuming, resource-heavy.

4. Combined Approach
Description: Blends baseline, informal, and detailed methods.
Pros: Balanced, phased improvements, critical focus.
Cons: Requires careful planning.

Risk Treatment Options include:

Accepting risks.
Avoiding activities leading to risks.
Transferring risks (e.g., insurance).
Mitigating risks through controls.

c) An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up. What is the most likely cause? **(3)**

The most likely causes for the sequence of logged events not matching up are:

Time Synchronization Issues:
The devices (firewalls, proxy servers, IDS) might not be synchronized to the same time source. Without a unified time reference, logs will have inconsistent timestamps, making event correlation difficult.
Log Format Differences:
Each device may use a different logging format, making it hard to align events directly. The investigator might need to normalize the log data to a common format.
Network Delays or Asynchronous Event Reporting:
Events might be logged at slightly different times due to processing or transmission delays, causing apparent mismatches in the sequence of events.

chp 19

LEGAL & ETHICAL ASPECTS

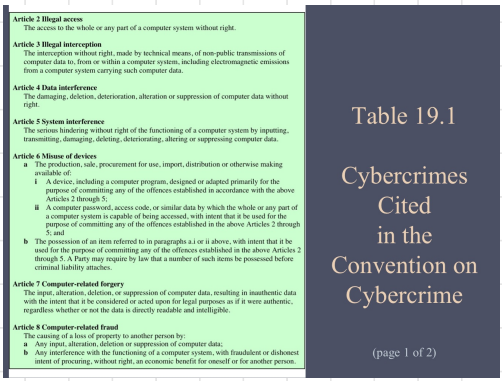
TYPE OF COMPUTER CRIMES

The U.S. Department of Justice (DOJ) categorizes computer crimes based on the computer's role in the crime:

1.Computers as targets:
Crimes involve attacking a computer system to steal data, control it without permission (e.g., theft of service), or disrupt its operation and data integrity.

2.Computers as storage devices:
Computers serve as storage for illegal materials
like stolen data, pirated software, or explicit content.

3.Computers as communication tool:
Crimes include traditional illegal activities conducted online,
such as selling drugs, weapons, and engaging in fraud, gambling, or Child pornography.



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

(page 1 of 2)

The deterrence of computer and network attacks depends on the success of arresting and prosecuting cybercriminals, but achieving this is challenging. Cybercrime creates a "vicious cycle" involving law enforcement, criminals, and victims.

Challenges for law enforcement

- Investigating cybercrime requires advanced technical knowledge, which many agencies, especially smaller ones, lack.
- Limited resources, such as processing power, communication tools, and storage, hinder investigations.
- Cybercrime often involves criminals operating across jurisdictions or countries, complicating collaboration between agencies.

Efforts like the international Convention on Cybercrime aim to address these challenges by
-introducing unified crime definitions and
-harmonized laws globally.

Cybercriminals

The limited success in prosecuting cybercriminals has resulted in
- growth in criminal activity,
- increased boldness of criminals , and
- expanded global reach.

WHY

1.Hard to profile:
Unlike other repeat offenders, cybercriminals are hard to profile, though they are often young and highly skilled with computers.

2.Identification Issues:
Additionally, the absence of cybercriminal databases makes identifying suspects more challenging.

Cybercrime Victims

Impact on victimes
The success of cybercriminals and the struggles of law enforcement influence victims' behavior.
Many organizations lack sufficient resources to prevent attacks and are hesitant to report incidents due to distrust in law enforcement, fear of reputational damage, and concerns about liability. This low reporting further hinders law enforcement, perpetuating the "vicious cycle."

Organizations should view law enforcement as a vital resource alongside technical and physical defenses. Effective collaboration requires understanding the investigation process, providing necessary inputs, and contributing positively, emphasizing people skills over technical expertise.

↓more detail

Cybercrime and Law Enforcement Challenges

Impact on Victim Behavior

Influence of Law Enforcement Challenges:
- Limited law enforcement success affects how victims respond.
- Victims often lack confidence in law enforcement effectiveness.

Common Victim Shortcomings:
- Insufficient investment in technical, physical, and human-factor resources to prevent attacks.
- Low rates of crime reporting due to:
  - ↳ Concerns about corporate reputation.
  - ↳ Fear of civil liability.

Vicious Cycle:
- Low reporting rates hinder law enforcement efforts.
- Weak law enforcement reinforces victim reluctance, perpetuating the problem.

Role of Law Enforcement in Cybersecurity

Perception Shift Needed:
Executive management and security teams must view law enforcement as a key resource.
Law enforcement should complement technical, physical, and human resources.

Critical Skills for Success:
Effective use of law enforcement relies on people skills, not just technical expertise.

Collaboration with Investigators:
Management must understand:
- The criminal investigation process.
- What inputs and information investigators need.
- How victims can contribute positively to investigations.

Intellectual property (IP) :

refers to intangible assets based on human knowledge and ideas,
such as software, data, creative works, or innovations.

There are three main types of IP with legal protection:

1. **Copyrights**: Protect original works like books, music, and software.
2. **Trademarks**: Protect symbols, names, and logos used to identify goods or services.
3. **Patents**: Protect inventions or processes

These protections prevent **infringement**—
↳ violations of the rights granted by IP laws.
IP owners have the right to take legal action against infringers,
with the nature of infringement differing based on the IP type.

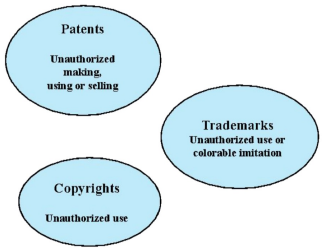


Figure 19.1 Intellectual Property Infringement

1. Copyright law

protects the tangible expression of an idea,
not the idea itself.

To claim copyright, the following conditions must be met:
- The work must be original.
- The original idea must be fixed in a concrete form,
  ↳ such as on paper, in software, or multimedia.

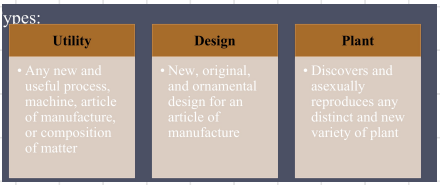
The copyright owner has exclusive rights, protected against infringement, including:
- **Reproduction right**: Allows making copies of the work.
- **Modification right**: Allows creating new works based on the original.
- **Distribution right**: Permits selling, renting, leasing, or lending copies of the work.
- **Public-performance right**: Applies mainly to live performances.
- **Public-display right**: Allows showing the work publicly, directly or through media.

Examples of items that can be copyrighted include:
- **Literary works**: Books, articles, brochures, ads, and directories.
- **Musical works**: Songs, jingles, and instrumentals.
- **Dramatic works**: Plays and operas.
- **Pantomimes and choreographic works**: Dance performances and mime.
- **Pictorial, graphic, and sculptural works**: Photos, posters, paintings, and sculptures.
- **Motion pictures and audiovisual works**: Movies, documentaries, TV shows, and interactive multimedia.
- **Sound recordings**: Music or spoken word recordings.
- **Architectural works**: Building designs and plans.
- **Software-related works**: Computer software and manuals.

2. Patents

Definition

↳ A patent gives the inventor a property right.
↳ The patent allows the inventor to exclude others from:
  ↳ Making, using, selling, or offering to sell the invention.
  ↳ Importing the invention into the country (e.g., U.S.).



Types of Patents

1.Utility Patents:
For new and useful processes, machines, manufactured items, compositions of matter, or improvements to them.
2.Design Patents:
For new, original, and decorative designs for manufactured items.
3. Plant Patents:
For new plant varieties that are asexually reproduced.

Example in Computer Security

the **RSA public-key cryptosystem** patent, which RSA Security held from 1983 to 2000, collecting fees for each use of RSA during that period.

3. Trademarks

Definition

A trademark is a word, name, symbol, or device used in trade
  ↳ to identify and distinguish the source of goods.
A **servicemark** is similar but applies to services instead of goods.

Key Points

The term "trademark" or "mark" commonly refers
  ↳ to both trademarks and servicemarks.

Trademark Rights allow the owner to:

- Prevent others from using confusingly similar marks.
  ↳ But not stop others from making or selling the same goods/services under a different mark.

↳ you can sell me something under a different name

Several forms of intellectual property are relevant to network and computer security:

Forms of Intellectual Property (IP)

1.Software:
Includes commercial, shareware, proprietary, and individually created software.
Protected by copyright, sometimes by patents.
2.Databases:
Organized collections of data with potential commercial value
↳ (e.g., economic forecasting databases).
Protected by copyright.
3.Digital Content:
Includes audio, video, multimedia, courseware, and website content.
Protected as original works under copyright.
4.Algorithms:
Example: RSA public-key cryptosystem, which can be patented.

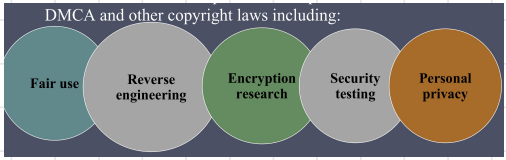
Protection Measures
Computer security techniques can protect some of these forms,
↳ like statistical databases that restrict access to raw data.
However, for software piracy (e.g., unauthorized copies or use of unlicensed software),
↳ legal actions are more effective than technical security measures.

Digital Millennium Copyright Act (DMCA),

Signed: in 1998,
Purpose: Implements WIPO treaties
Goal: strengthen protections of digital copyrighted materials
It also
1. strengthen protections of digital copyrighted materials
2. encourages copyright owners to use technological measures to protect their works,
↳ which can prevent access or copying of the content.
3.Prohibits attempts to bypass the measures
↳ including unauthorized decryption of content.
4.forbids the creation, sale, or distribution of tools
↳ that can break encryption intended to prevent access or copying.

Both **criminal** and **civil penalties** are applied
to those who attempt to circumvent these measures or assist in doing so.

DMCA Exemptions



Certain actions are exempt from the provisions
of the DMCA and other copyright laws:

1.Fair Use:
Allows others to use portions of a work for purposes
↳ like review, comment, and discussion.
2.Reverse Engineering:
Permitted if the user has the right to use the software and the goal is interoperability,
↳ not duplicating the program's functionality.
3.Encryption Research:
Allows "good faith" decryption efforts to help advance encryption technology.
4.Security Testing:
Permitted if done to test or correct security flaws, with the owner's authorization.
5.Personal Privacy:
Technological measures can be bypassed if it is necessary to prevent the revealing or recording of personally identifying information.

Despite these exemptions, there is concern, especially among researchers and academics, that the DMCA
- restricts security and encryption research,
- limits innovation, and
- threatens open-source software development.

Digital Rights Management (DRM)

Definition: DRM ensures digital rights holders are identified and receive payment.
It may also restrict actions like printing or distributing content.

Variety in Systems: No single DRM standard exists;
it includes various methods to manage and enforce intellectual property rights,
using secure automated tools to control content use and distribution.

Goals:
Manage the full lifecycle of content management :
↳ creation, contributions, access, distribution, use.
Handle rights information linked to the content.

Key Objectives of DRM Systems:
1.Protect content from unauthorized access, allowing only authorized use.
2.Support different content types (e.g., music, videos, books, images).
3.Enable content use on multiple platforms (e.g., PCs, mobile devices).
4.Allow distribution through various media (e.g., CDs, DVDs, flash memory).

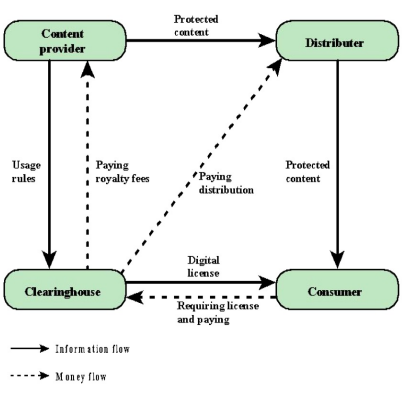


Figure 19.2 DRM Components

Figure 19.2, based on [LIU03], illustrates a typical
Digital Rights Management (DRM) model
with the following principal users:

1.Content Provider:
Owns the digital rights to the content and seeks to protect those rights.
Examples include music record labels or movie studios.

2. Distributor:
Provides distribution channels, like online shops or web retailers.
They receive content from the provider, create a catalog, and present content with rights metadata.

3. Consumer:
Accesses digital content by downloading or streaming through a distributor's channel, paying for a digital license.
The consumer's player or viewer requests a license from the clearinghouse and enforces the usage rights.

4. Clearinghouse:
Manages financial transactions, issuing digital licenses to consumers,
and pays royalties to the content provider and distribution fees to the distributor. It also logs license usage.

In this model, the distributor does not enforce access rights. The content provider encrypts the content, requiring the consumer to purchase a license from the clearinghouse. The clearinghouse checks the access rules and fees, then credits the provider and distributor after collecting the fee.

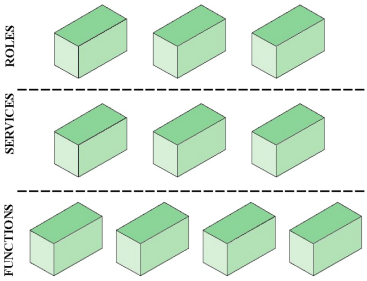


Figure 19.3 DRM System Architecture

Figure 19.3 illustrates a generic DRM system architecture
that supports DRM functionality,
where the system is accessed by **parties in 3 roles:**
1. Rights Holders: Content providers who own or have acquired rights to the content.
2.Service Providers: Distributors and clearinghouses that facilitate
↳ content distribution and transaction processing.
3. Consumers: Individuals who purchase access to content for specific uses.

The system interface includes the following **services**:
- Identity Management: Ensures unique identification of entities such as parties and content.
It involves:
- Allocation of unique party identifiers
- User profiles and preferences
- Device management for users
- Public-key management for secure communications

- **Content Management:** Manages the content throughout its lifecycle,
↳ including its distribution and use.
- **Rights Management:** Manages rights, rights holders, and related requirements
↳ to ensure proper enforcement of content usage.

Below these management modules, common **functions** include:
- **Security/Encryption**: Encrypts content and signs license agreements
↳ to protect the content and ensure secure access.
- **Billing/Payments**: Collects usage fees from consumers and distributes payments
↳ to rights holders and distributors.
- **Delivery Functions**: Handles the delivery of content to consumers
↳ once payment and access are confirmed.

This architecture facilitates secure and controlled access to digital content, ensuring all involved parties are properly identified, rights are managed, and payments are handled efficiently.

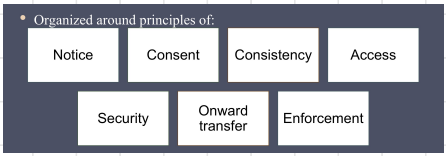
Privacy

The issue of privacy, which **overlaps with computer security,**
has become a growing concern due to
Increased Collection of Personal Information:
The amount of personal data collected and stored has grown significantly,
↳ driven by law enforcement, national security, and economic motives.
Economic factors, such as the value of personal data in the global information economy,
↳ have been a major driving force.

As a result, individuals are becoming more aware
of how their personal information is accessed by government agencies, businesses, and other entities, including other internet users.

This increasing awareness has raised significant concerns
↳ about the potential compromise of personal privacy.
The potential compromise of personal privacy has led
↳ to legal and technical efforts to protect privacy rights.

EU Data Protection Directive (1998):



Aimed to protect privacy rights
↳ while allowing the free flow of personal information within the EU.
Requires member states to create laws based on the Directive.

Principles of Personal Information Use

1. **Notice**: Organizations must inform individuals
   - about the data
     - ↳ being collected,
     - ↳ its use, and
     - ↳ available choices.
2. **Consent**: Individuals must agree to how their data is used or shared,
   - especially sensitive information like·
     - ↳ race,
     - ↳ religion,
     - ↳ health,
     - ↳ personal beliefs.
3. **Consistency**: Organizations must use data only as described
   ↳ in the notice and according to individual choices.
4. **Access**: Individuals have the right to
   ↳ access, correct, or delete their personal information.
5. **Security**: Organizations must ensure adequate security measures
   ↳ to protect personal data.
6. **Onward Transfer**: Third parties receiving personal data must
   ↳ provide the same privacy protection.
7. **Enforcement**: Individuals can take legal action
   ↳ if organizations fail to follow the law.
   - Each EU member has an agency to enforce privacy rights.

Privacy Act of 1974:

The first comprehensive privacy law in the U.S.,
focusing on personal information collected by federal agencies.

Main objectives:

1. Allow individuals to know what records about them
   ↳ are collected, used, or shared.
2. Prevent records obtained for one purpose from being used
   ↳ for another without consent.
3. Give individuals the right to access and correct their records.
4. Ensure personal information is accurate, relevant, and not excessive.
5. Provide a private right of action for individuals
   ↳ if their personal information is misused.

Exceptions:
Certain situations, like criminal investigations, national security concerns, and conflicts between privacy rights,
may allow exceptions.

Privacy Functions in Trusted Systems (Common Criteria)

The Common Criteria specification defines privacy functions that should be implemented in trusted systems to protect users from identity misuse.
These functions fall under four major areas:

1.Anonymity:
Allows users to use resources or services without revealing their identity.
Other users or processes cannot determine the identity of the user
↳ involved in a specific operation.
The system should not request the real name of the user,
↳ and this doesn't conflict with access control,
which is tied to user IDs, not personal info.

2.Pseudonymity:
Users can access resources without revealing their real identity
↳ but can still be held accountable for their actions.
The system assigns an alias to the user,
↳ which prevents others from identifying them
but allows the system to trace back to the real user via the alias.

3.Unlinkability:
Ensures that multiple uses of resources or services
↳ by a user cannot be linked together by others.

4.Unobservability:
Ensures that a user can use a resource or service
↳ without being observed by others, especially third parties.
The system should avoid collecting privacy-related information
↳ that could compromise unobservability.
Authorized users may be given the ability
↳ to observe resource or service usage.

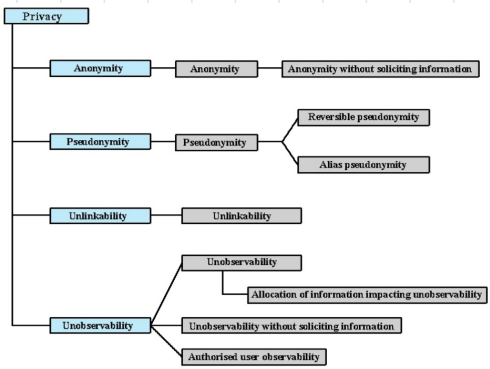


Figure 19.4 Common Criteria Privacy Class Decomposition

Note: The Common Criteria specification focuses on the privacy of individuals using computer resources,
not the privacy of personal information about those individuals.

Privacy and Data Surveillance

New Threats to Privacy:
-Big businesses, government, and law enforcement increase threats to personal privacy.
-Law enforcement and intelligence agencies use data surveillance techniques,
↳ as shown by the Snowden revelations.
-Private organizations collect detailed personal data through
↳ websites, social media, electronic payments, mobile phones, and sensors.
-Data is often collected for one purpose but reused for others,
↳ like targeted marketing and research.
-Tension exists between using data for societal benefits (e.g., public health, national security) and
↳ protecting individual privacy rights.

Concerns with Social Media:
-Public social media platforms like Facebook collect and share large amounts of personal data.
-People willingly share private information, which can be analyzed by companies.
-Little regulation exists on the impact of others' data (e.g., photos, status updates) on individuals.
-This data, including metadata (e.g., time, location),
↳ can be used by employers, insurers, or investigators, potentially harming the individual.

Privacy Protection

Need for Policy and Technical Approaches:

Both policy and technical measures are necessary
↳ to protect privacy when organizations seek detailed information about individuals.

Technical Mechanisms for Privacy Protection:

↳ **Database Security**:
- Techniques for securing stored data can help protect privacy.

↳ **Social Media Privacy Controls:**
- Provide privacy settings to control who can view personal data.
- Notify individuals when they are tagged or referenced in others' content.
- Social media platforms often change these controls, causing user frustration.

Anonymization in Big Data:

-Anonymizing data by removing personally identifiable information
↳ can protect privacy during big data analysis.
-However, re-identification risks exist, so great care is needed.
-A recent framework from the US Federal Trade Commission encourages protecting against
↳ re-identification while enabling big data analysis.

Guidelines for Big Data Use in order to preserve privacy

1. **Consent**: Ensure participants make informed decisions about their involvement.
2. **Privacy & Confidentiality**: Individuals control who can access their personal data;
   ↳ only authorized people should access it.
3. **Ownership & Authorship**: Determine responsibility for data and
   ↳ when individuals lose control over their data.
4. **Data Sharing & Social Benefits**: Assess the benefits of reusing data
   ↳ from different sources for research.
5. **Governance & Custodianship**: Manage, organize, and preserve digital data
   ↳ with proper oversight.

Cost-Benefit Analysis:

-A suitable analysis should balance privacy costs
↳ with the benefits of big data use,
↳ considering who benefits and how certain the benefits are.

Changes in Laws:

-Several countries (US, UK) are changing laws to limit bulk collection of metadata,
↳ which is seen as personal data by many.
-Efforts aim to regulate mass surveillance and protect privacy,
↳ with court decisions addressing the balance between privacy rights and security benefits.
-Some legislation has been declared invalid,
↳ and safeguards are being imposed to protect privacy.

Ethical Issues

Ethics concerns the morality of actions, benefits, and harms, applying basic moral principles, with unique issues in computing.

Unique Ethical Issues:

Scale of Activities: Computer technology enables
- ↳ larger-scale recordkeeping,
- ↳ more detailed personal data collection
- ↳ precise data mining and matching.

Expanded Communication and Interconnection: The internet increases the potential for harm through widespread communication and connection.

New Entities: Technologies like databases, web browsers, chat rooms, and cookies
- ↳ introduce new ethical issues for which there are no established rules.

Ethical Hierarchy:

Top: Basic ethical values shared by all humans (integrity, fairness, justice).

Middle: Ethical obligations specific to professionals
- ↳ due to their special training.

Bottom: Profession-specific ethical values tied
- ↳ to specialized knowledge and the impact professionals have.

Most professions include these levels in a code of conduct.

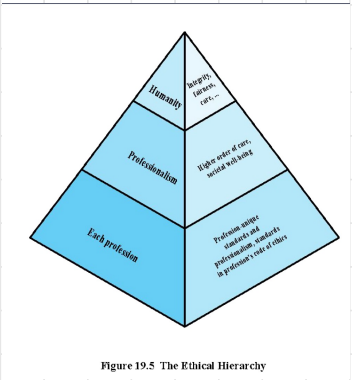


Figure 19.5 The Ethical Hierarchy

Ethical Issues in Computers:

Repositories & Processors of Information:
Unauthorized access to stored data raises fairness and appropriateness concerns.

Producers of New Assets:
Computer programs are new assets with different ownership rules.

Instruments of Acts:
Questions arise about responsibility for the integrity of computer outputs.

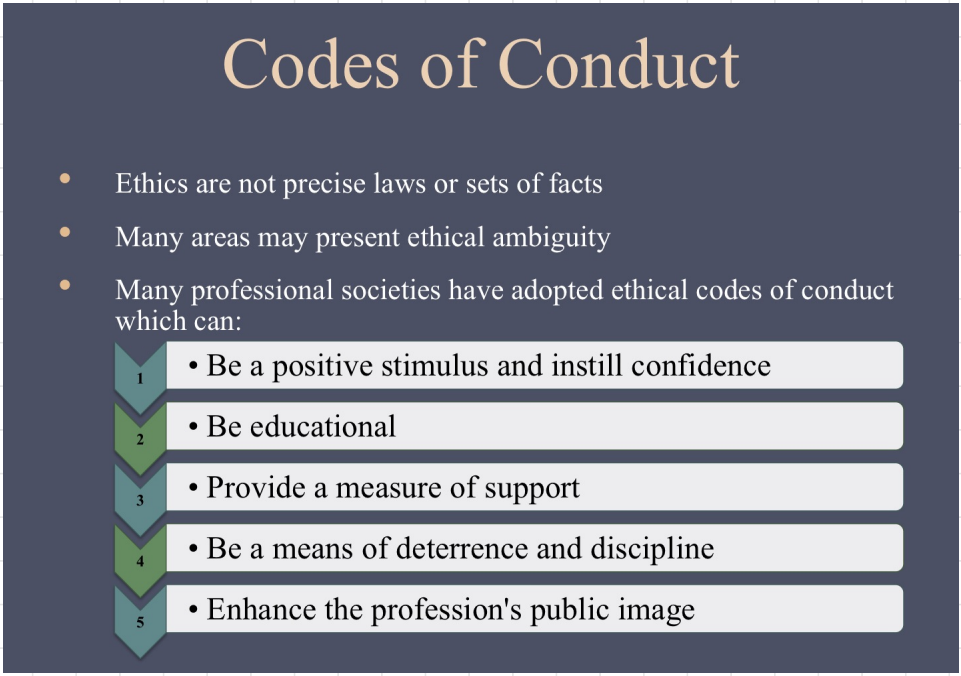
Symbols of Intimidation & Deception:
The perception of computers as infallible or anthropomorphic can mislead or deceive.

Ethical Conflicts for IT Professionals:

Loyalty vs. Professional Duty:
IT professionals may face situations where their duty to the public or clients conflicts with loyalty to their employer,
leading to potential whistleblowing (e.g., shipping a product with insufficient testing).

Whistleblowing:
A difficult decision where professionals may report harmful situations,
but organizations should provide alternatives like an ombudsperson to handle concerns.

Conflict of Interest:
IT professionals must disclose financial interests,
such as a consultant's investment in a vendor
, if it influences product recommendations.



Comparison of Codes of Conduct

Common Themes in Professional Codes of Conduct:
-Dignity and worth of others.
-Personal integrity and honesty.
-Responsibility for one's work.
-Confidentiality of information.
-Public safety, health, and welfare.
-Participation in professional societies to improve standards.
-Public knowledge and access to technology as social power.

Observations:
All codes emphasize the professional's responsibility to people, which is central to ethics.
However, these codes are generic and could apply to any profession.
They do not specifically address the unique ethical issues related to computers and IT systems, as highlighted in previous discussions.

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

1. Security goals, CIA triads, underground economy, Classical Cryptography
2. One-time pad and stream ciphers
3. Pseudorandom generators
4. attack and weakness of stream ciphers
5. Block Ciphers
   a. DES
   b. AES
   c. Modes of Encryption
6. MACs and HMAC
7. Diffie Hellman Key Exchange
8. Public Key Cryptography (RSA)
9. Digital Signatures
10. Public Key Infrastructure
11. User Authentication
    a. password based authentication
    b. Access Control (discretionary, Mandatory, Role based, ACL, Capabilities)
12. Malicious Software
    a. Malware and their Types
    b. Propagation
    c. Defenses
    d. Rootkits
13. Firewalls and Intrusion detection → chp 9
14. SQLi, XSS and XSRF → 11 or 5
15. Network Security Topics (IPSEC, VPN, DNSSEC, DDoS, etc) → ?
16. Software Security (control Hijacking attacks and defenses) → 11
17. IT Security Management and Risk Assessment: security policies, policy formation and enforcement, risk assessment. Textbook Chapter 14, Sections 14.1 to 14.3 → 14
18. Legal and Ethical Aspects: Cybercrime, Intellectual Property, Privacy and Anonymity of Data and Ethical Issues.Textbook Chapter 19, Sections 19.1 to 19.4 → 19

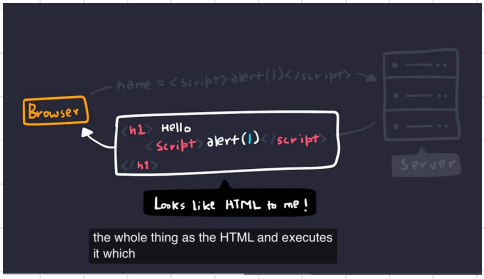
chp 8 ? chp 5 ?

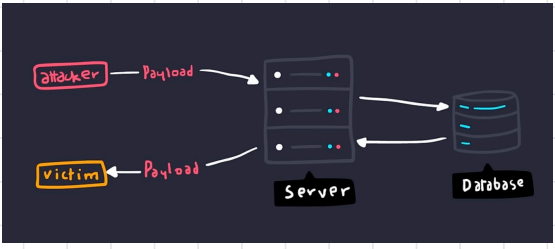
SOFTWARE SECURITY

CHP 11

XSS

↳ java script injection





ishma hafeez
notes

c) Which particular type of SQL Injection is shown in Figure 2? Justify your answer. **(3)**

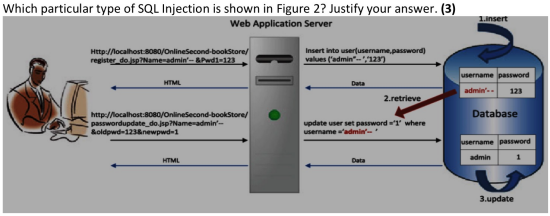


Figure 2: SQL Injection Attack

Solution:

SQL 2nd order Injection. Read the idea of 2nd order SQL injection.

↳ malicious code gets stored in the database

d. Show a scheme of database encryption using a block diagram involving client and server.

Database Encryption Scheme

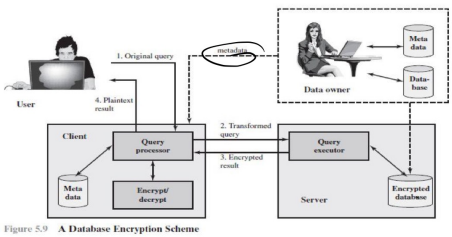


Figure 5.9 **A Database Encryption Scheme**

- **Data owner:** organization that produces data to be made available for controlled release
- **User:** human entity that presents queries to the system
- **Client:** frontend that transforms user queries into queries on the encrypted data stored on the server
- **Server:** an organization that receives the encrypted data from a data owner and makes them available for distribution to clients