

Firewall and Intrusion

Syllabus :

At the end of this unit, you should be able to understand and comprehend the following syllabus topics :

- Firewall
 - Introduction
 - Characteristics and types
 - Benefits and limitations
 - Firewall architecture
- Computer Intrusions and Intrusion detection systems (IDS)
 - Need
 - Methods
 - Types of IDS
- Access Control
- Trusted Systems
- Password Management, Limitations and Challenges

5.1 Firewalls

- Your computer is connected to the internet. How do you protect it from someone trying to access it over the internet? How do you prevent some rogue programs on your computer to send information to the attacker? Firewalls could be a mechanism.

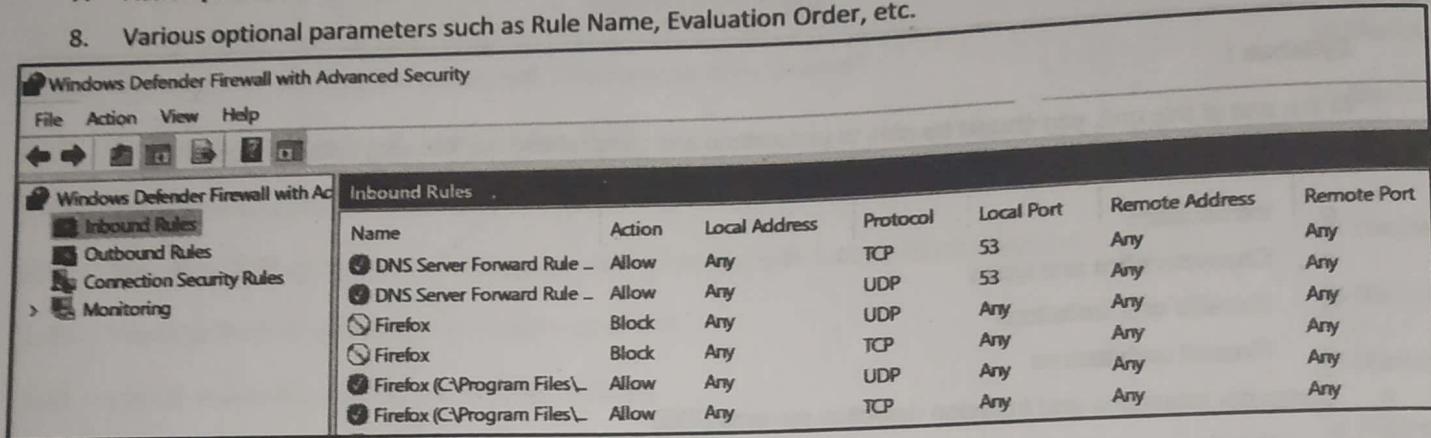
 **Definition :** Firewalls are network security systems that protect the computing resources on a trusted network from unauthorized access.

- For example, you can access google.com website but not its webserver's operating system. If you try connecting to the webserver except over the HTTP or HTTPS, the connection would be denied. That's what a firewall does at a high level.
- You need to define various rules, as per your security requirements, in the firewall and the firewall evaluates those rules before granting or denying access to the requested resource.

Components of a firewall rule

- Typically, a firewall rule consists of the following parameters :
 1. Source IP address or hostname

2. Destination IP address or hostname
3. Source Port number
4. Destination Port number
5. Direction of communication [inbound or outbound]
6. Protocol name [TCP, UDP, ICMP or various others]
7. Action [allow, deny, log, etc.]
8. Various optional parameters such as Rule Name, Evaluation Order, etc.



- This is a snapshot of Microsoft® Windows® Firewall.

5.1.1 Classification of Firewalls

SPPU – May 19

- Q. What are the various types of firewall ?** (May 19, 4 Marks)
- Q. Explain packet filtering firewall.** (May 19, 4 Marks)

Firewalls can be classified based on various attributes. Fig. 5.1.1 shows types of firewalls.

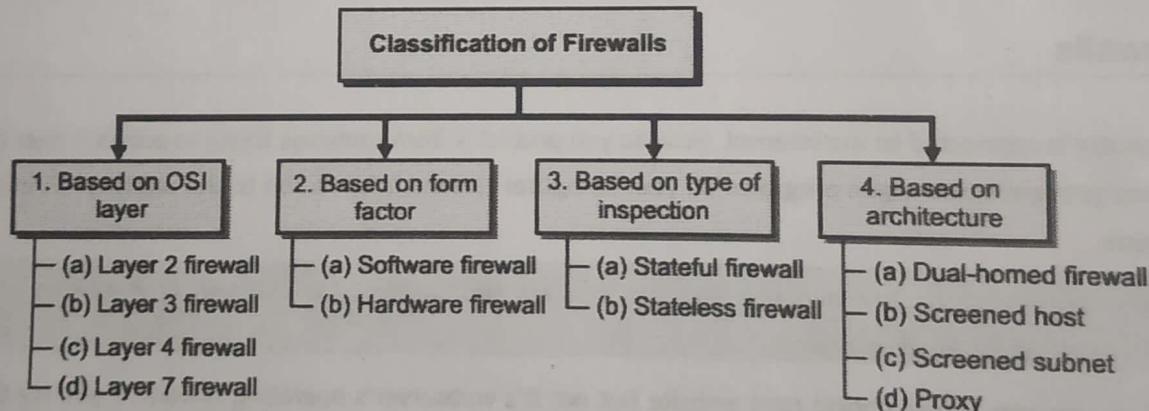


Fig. 5.1.1

1. Based on the OSI Layer

As you understand, OSI is a conceptual networking model. Based on the various layers, firewalls can be classified as following:

- a. **Layer 2 Firewall :** These firewalls work at the "Data Link" layer of the OSI model. These firewalls require MAC, VLAN or device hardware level information to operate. One of the greatest advantage of these types of firewalls is that they are not IP dependent.



- b. **Layer 3 Firewall** : These firewalls work at the "Network" layer of the OSI model. These filter traffic based on source/destination IP, port, and protocol. These are one of the most prevalent types of firewalls in use today. These are also called as Stateless firewalls. These are also called *first-generation* firewalls.
- c. **Layer 4 Firewall** : These firewalls work at the "Transport" layer of the OSI model. These firewalls do everything that a Layer 3 firewall does and additionally track the active network connections and allow/deny traffic based on the state of those connections.
These can effectively stop DoS attacks such as the ones based on TCP SYN/ACK as these are aware of the state of connection. These are also called as Stateful firewalls. These are also called *second-generation* firewalls.
- d. **Layer 7 Firewall** : These firewalls are called Layer 7 but can work at three layers – Session, Presentation and Application. For simplicity, these are just called Layer 7 firewalls. Layer 7 firewalls do everything that a Layer 4 firewall does and additionally include the ability to intelligently inspect the contents of the network packets passing through them. For example, a Layer 7 firewall could deny all the HTTP requests from Korean IP addresses. They have the actual packet content level visibility and are the most advanced types of firewall in use today. These are also called *third-generation* firewalls.

2. Based on the form factor

Form factor or the footprint is the way the firewall is actually packaged and deployed. They can be classified as,

- a. **Software Firewalls** : These firewalls work as a software program and require an operating system to run them. All the implementation logic is coded in software and they are installed, patched, upgraded and maintained like a regular computer software. These firewalls could work at any of the OSI layers as discussed before.
- b. **Hardware Firewalls** : Firewalls can also be deployed as a hardware device. Hardware firewall may have better performance and they come packaged in a ready to use hardware device. Like any other firewall, you need to configure it as per your security requirements.

3. Based on the type of inspection

Firewalls can keep track of connections or just work based on the configured rules. Based on their inspection types, these can be classified as

- a. **Stateful Firewalls** : These firewalls keep track of the state of connections apart from the defined firewall rules. These precisely understand various handshake protocols and can effectively stop attacks that try to manipulate connection establishment or maintenance process.
- b. **Stateless Firewalls** : Stateless firewalls typically work at the Layer 3 and take decisions based on the defined rule parameters such as IP, Port and Protocol. These do not track connection states and cannot effectively protect against attacks that manipulate connection processes.

4. Based on architecture

Firewalls can be deployed in many ways. They have special properties that make them suitable for one deployment type over the another. Based on the deployment possibilities, firewalls can be classified as

- a. **Dual-homed Firewalls** : A Dual-Homed Firewall has two interfaces – one facing the external network and the other facing the internal network. It receives the external packets on one of its interfaces, evaluates firewall rules, and passes on the traffic to the designated internal resources via the second interface. The two interfaces are kept separate to isolate the external traffic with the internal traffic physically.

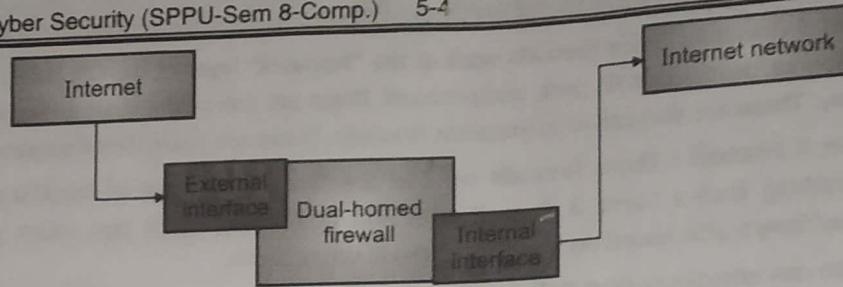


Fig. 5.1.2

- b. **Screened Host** : In a screened host firewall, all internet (and other regulated) traffic goes through the firewall, no matter what. The internet router device first screens (filters) all the packets that are relevant to the network and then passes it to the Screened Host firewall for further inspection and applying rules.

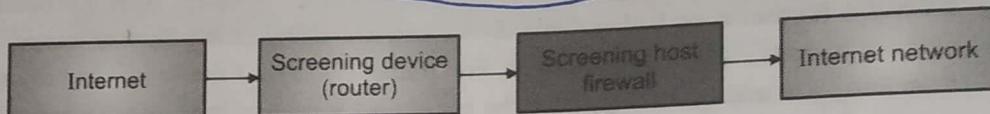


Fig. 5.1.3

- c. **Screened Subnet** : In screened subnet architecture, two firewalls are used. One just after the external network and the one just before the internal network. Any network that lies between the two firewalls is called a Demilitarized Zone (DMZ). You place your public facing servers such as webservers, email servers etc. in DMZ. An attacker would have to bypass both the firewalls before she can hit the internal network. This kind of architecture is commonly used in the industry today.

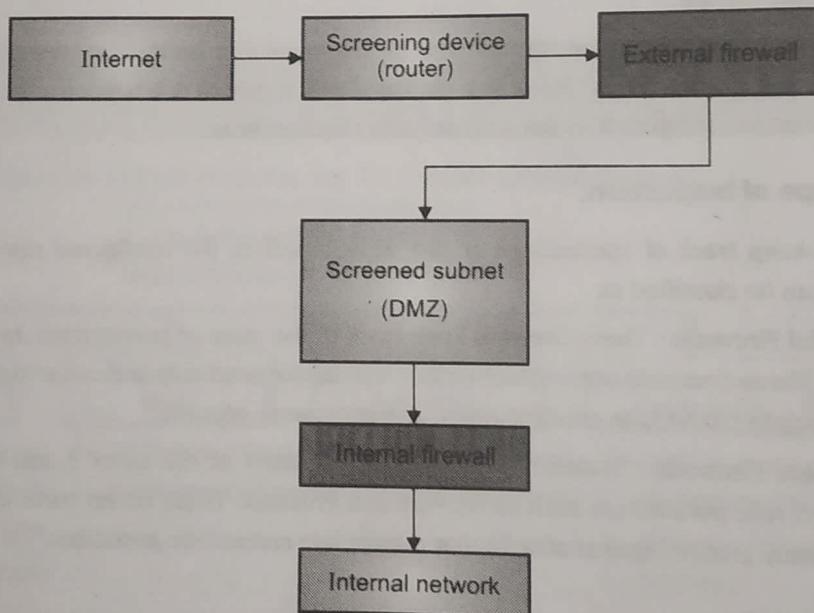


Fig. 5.1.4

- d. **Proxy** : A proxy firewall stands between the trusted and the untrusted network and takes allow or deny decisions after careful inspection of what is being passed along. Like a regular proxy, the proxy firewall breaks the connection between the source and the destination. After examining the traffic, it self-establishes a connection with the destination and passes the intended traffic to the destination as if the packets were originating from it.

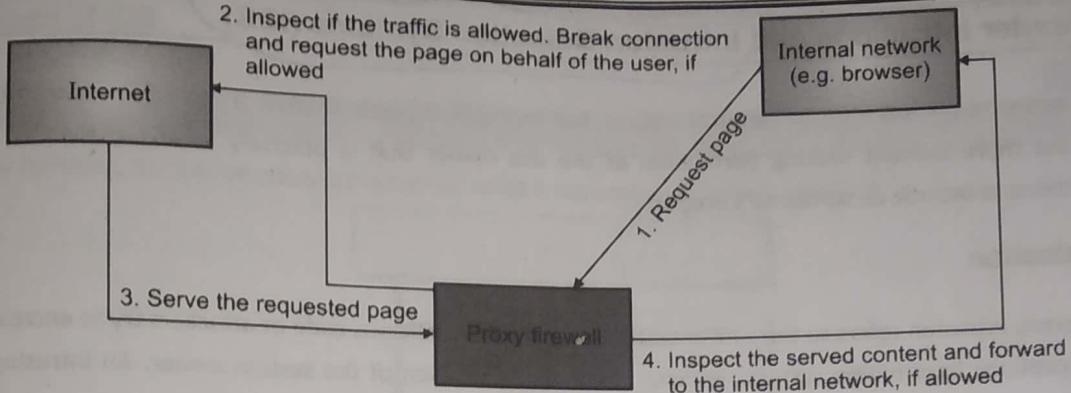


Fig. 5.1.5

5.1.2 Challenges in Managing and Deploying Firewalls

SPPU – May 19

Q. Discuss limitations of firewall.

(May 19, 4 Marks)

Note : Irrespective of what challenges or limitations firewalls may have, they are heavily used throughout the industry. You cannot just imagine any network without several firewalls in place to monitor, inspect and manage legitimate traffic and separate it from the illegitimate traffic. So, just know what some of the management or technical challenges are and do not worry too much about them.

1. Performance

Since the traffic (as well as the content) needs to pass through the firewalls, there is a little performance degradation of the network. The adequate traffic examination may add up to a few milliseconds of latency on each packet.

2. Business agility

Firewall rules are usually manually added, edited or deleted. The pace of business might be too high to require several changes to the firewall rules frequently. Keeping up with these changes without making errors is difficult.

3. Costs

Modern (or advanced) firewalls that provide content and protocol level inspection may be cost-prohibitive for small or medium sized organizations.

4. Insider attacks

Firewalls are usually designed and deployed to protect a trusted network from an untrusted network. But, if there were other vulnerabilities (such as a missing OS security patch) that were exploited such that an attacker is already on the trusted network, firewalls might not be able to protect or limit damages to the other resources on the trusted network.

5. Managing firewalls themselves

Like your OS, printers or other software or hardware devices, firewalls need to be installed, patched, updated, etc. to remain operational. This adds a management overhead. Additionally, firewalls could have known vulnerabilities that need to be patched else a firewall that itself is lacking protection may not be very useful in providing you the required level of protection.

5.2 Computer Intrusions and Intrusion Detection Systems (IDS)

Intrusion means to encroach (or to capture) a place. For example, suppose there is a vacant site and you manage to build a small hut there without seeking permission of the site owner that is precisely what intrusion is. You, as an individual, are trying to intrude on someone's property.

5.2.1 Introduction

- In digital terms, intrusion refers to the similar situation where the malicious code or attackers try to encroach (forcibly enter and capture) information systems without requiring permission of the system owner. An Intrusion Detection System (IDS) is defined as,

 **Definition :** A software that helps to find out if a system is breached.

Note : Breach is a word used in information security domain to describe any form of attack or unauthorized actions. You can use this word to mean anything that refers to the undesired actions and outcomes with respect to information security.

- So, in a nutshell, IDS can help you to find out if there were undesired actions or attacks carried out on your information systems. IDS works using various techniques as we will see later in this section. Note here that IDS does not help to prevent the attacks unlike anti-virus. It is only a system that can gather system information and find out if everything looks alright or not.

5.2.2 Need for IDS

SPPU - May 19

Q. Explain need of intrusion detection system.

(May 19, 2 Marks)

IDS is one of the software-based security mechanisms that help to protect information system. At a high level, it is needed for the following reasons:

1. Defense in Depth

As you saw in the security architecture section, security is about minimizing the damage that can be possibly done. Defense in depth (or the layered approach) of security designing ensures that even if one of the controls is to fail, the overall security of the system would still be possibly healthy. IDS fulfill this need to bring an added layer of protection where any breaches or their possibilities can be identified quickly.

2. Automate intrusion detection

Imagine that you have a large set of machines, say 1,000 and more. How would you inspect each and every machine and find out if there were attacks or attempts to attack it? IDS helps you to automate this need and alert you when it detects any threat or likely a breach.

3. Corrective actions

Learning from threats or breaches that the IDS identifies, you can take corrective actions on your infrastructure design and could possibly strengthen its security. You might have some unprotected areas in your infrastructure that can be highlighted with the use of IDS.

5.2.3 Types of IDS

Q. Define signature based IDS.

SPPU May 19

(May 19, 3 Marks)

Broadly speaking, IDS can be classified based on what it monitors and how it monitors.

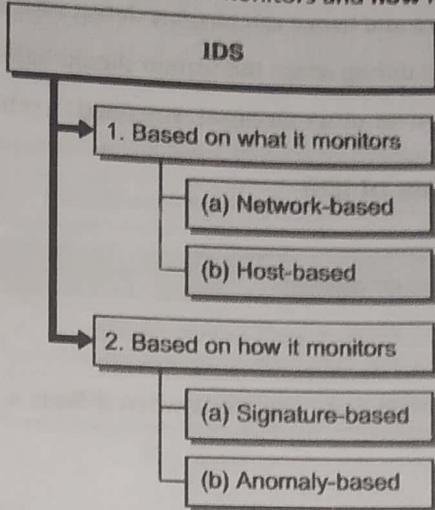


Fig. 5.2.1

1. Based on what it monitors

IDS can be classified into Network-based IDS (NIDS) and Host-based IDS (HIDS).

- Network-based IDS (NIDS)** : Network-based IDS evaluate intrusions from the networking side. They watch all network traffic as it reaches the various information systems. If there are any alerting situations based on the network traffic analysis, it notifies the administrator to take the corrective actions. NIDS do not have visibility into what's actually going on within the information system. It can only watch and detect threats and breaches from the networking viewpoint.
- Host-based IDS (HIDS)** : Host-based IDS are typically installed on the individual information systems and then they watch for suspicious activities occurring on the system. A system entity such as system services and processes, system files, privileged user actions, downloads etc. are closely monitored to detect any undesired activities. HIDS do not have visibility into what's going on at the networking side of the system. It can only watch and detect activities with respect to individual machines only.

2. Based on how it monitors

IDS can be classified into Signature-based and Anomaly-based.

- Signature-based** : Like banks and other organizations use human signature to validate requests and transactions similarly Signature-based IDS has a pre-loaded database of various attack signatures (patterns of a possible attack). When it watches the activities, it constantly compares the activities' patterns with that in the database. If a match is found, it raises an alert. If you notice, there are 3 things to understand here:
 - o Signature based IDS can only detect attacks if it already and historically knows about an attack pattern.
 - o For new types of attack, signature-based IDS would not raise alerts.
 - o It is important for you to update the signature definitions time to time (like how you do in anti-virus system).
- Anomaly-based** : Anomaly typically means "deviation from routine". For example, if you wake up at 7 AM every day and one day you wake up at 4 AM that is an anomaly situation.

If I were to plot your wake-up time graph, 4 AM would show up away from your regular wake-up time. That 4 AM point on the graph is called outlier (or away from other samples). Similarly, the Anomaly-based IDS first establishes the baseline (common routine) of activities. It might take up to 2-3 weeks to "learn" what's right for a system. Once the learning phase is over, it would watch out for any activities that are not part of that baseline and raise alerts. If you notice, there are 3 things to understand here as well:

- o It does not require signature and hence can possibly detect new attacks.
- o It requires a learning period during which the system should have undergone all possible activities.
- o If you plan to use the system for other purposes, you need to retrain the IDS.

5.2.4 Limitations and Challenges of IDS

SPPU - May 19

Q. Explain challenges of intrusion detection system.

(May 19, 3 Marks)

1. Does not prevent attacks

As you understand, IDS can only detect and raise alerts when it finds a likelihood of a breach. It cannot prevent or block the breach from happening.

2. High rate of false alerts (noise)

IDS might generate a lot of false alerts. It could happen so for example, when there is a new traffic from a source that IDS has not seen before. You need to spend your resources to take a note of each alert and appropriately deal with it – either fix it or ignore it.

3. Complex systems

IDS systems are typically complex in nature and require regular administrative actions and tuning for adequate operations.

4. Bypassing IDS

Advanced attackers know what actions and activities a version and brand of IDS can detect and what not. They tune their activities to bypass such detection mechanisms and go undetected.

5.3 Access Control

SPPU - May 19

Q. What is access control security services ?

(May 19, 4 Marks)

 **Definition :** Access Control Policies and Models dictate how and under what constraints (or conditions) principals (entities or subjects) access resources (objects).

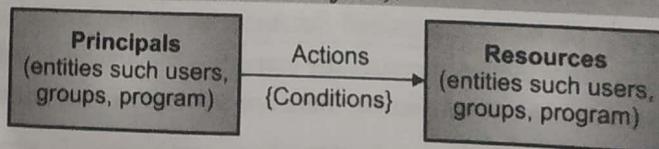


Fig. 5.3.1

– It follows the PARC model :

- o P = Principals (users, groups, programs)
- o A = Actions (Create, Read, Update, Delete)

- o R = Resources (OS, Network, Files, etc.)

- o C = Conditions (time of the day, type of OS, etc.)

Access control is the primary way to restrict entities from

- o Interacting with unauthorised resources
- o Carrying out unauthorised actions on authorised resources

There are 4 types of access control models.

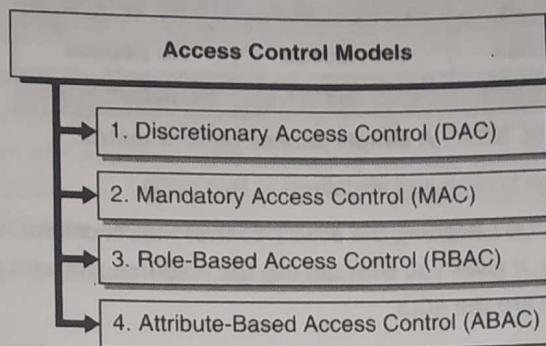


Fig. 5.3.2

1. Discretionary Access Control (DAC)

Definition : Discretionary Access Control (DAC) is an access control model based on subject's identity and need to know.

- This model is very simple to understand. As an owner of a particular resource, you can decide who uses that resource and with what permissions (how much). Access is provided based on individual's judgement on whom to provide access and how much.

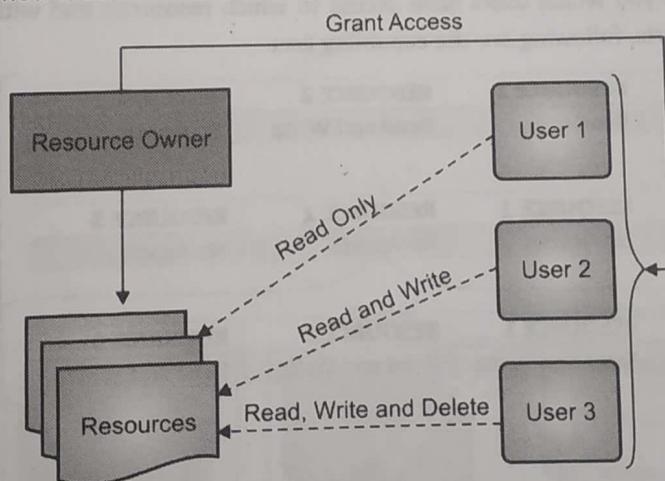


Fig. 5.3.3

- Let me give you an example. Suppose you own a car. You can hand over the keys to someone you trust who can drive your car outside the city limits. But, if you give your car for repairs, you would not like the car to be driven outside the city limits. The permissions assigned to the same resource (car) varies based on your judgement.
- Similarly, if you are an administrator on a system, you can decide which users (subjects or principals) to allow and what those users can do (which resources they can access and perform what actions on those resources).



- If you own certain files on the system, you can choose who else can access those files and in what capacity [read, write, delete, execute, share, print, etc.]. DAC is the most common type of access control model used. Typical operating systems such as Windows® and Linux enforce DAC model by default.
- DAC systems typically have an Access Control Matrix that lists the subjects and their rights (permissions) for respective objects (resources). Fig. 5.3.4 is a simplistic access control matrix.

USER	RESOURCE 1	RESOURCE 2	RESOURCE 3
JIM	Read only	Read and Write	No Access
JOHN	No Access	No Access	No Access
JACK	Read and Write	Read and Write	Read and Write

Fig. 5.3.4 : A simple access control matrix

- The Access Control Matrix can be broken and visualized as two parts.
 1. **Access Control Lists (ACLs)** : Reading the access control matrix column-wise gives the access control list for a particular resource. It gives you who can use the resource and with what rights. For the given access control matrix, following are the ACLs.

ACL for Resource 1		ACL for Resource 2		ACL for Resource 3	
USER	RESOURCE 1	USER	RESOURCE 2	USER	RESOURCE 3
JIM	Read only	JIM	Read and Write	JIM	No Access
JOHN	No Access	JOHN	No Access	JOHN	No Access
JACK	Read and Write	JACK	Read and Write	JACK	Read and Write

Access Control Lists

2. **Capability List** : Reading the access control matrix row-wise gives the capability of users across the resources. It gives you which users have access to which resources and with what rights. For the given access control matrix, following are the capability lists.

Capability of Jim	<table border="1"> <thead> <tr> <th>USER</th><th>RESOURCE 1</th><th>RESOURCE 2</th><th>RESOURCE 3</th></tr> </thead> <tbody> <tr> <td>JIM</td><td>Read only</td><td>Read and Write</td><td>No Access</td></tr> </tbody> </table>	USER	RESOURCE 1	RESOURCE 2	RESOURCE 3	JIM	Read only	Read and Write	No Access	Capability Lists
USER	RESOURCE 1	RESOURCE 2	RESOURCE 3							
JIM	Read only	Read and Write	No Access							
Capability of John	<table border="1"> <thead> <tr> <th>USER</th><th>RESOURCE 1</th><th>RESOURCE 2</th><th>RESOURCE 3</th></tr> </thead> <tbody> <tr> <td>JOHN</td><td>No Access</td><td>No Access</td><td>No Access</td></tr> </tbody> </table>	USER	RESOURCE 1	RESOURCE 2	RESOURCE 3	JOHN	No Access	No Access	No Access	
USER	RESOURCE 1	RESOURCE 2	RESOURCE 3							
JOHN	No Access	No Access	No Access							
Capability of Jack	<table border="1"> <thead> <tr> <th>USER</th><th>RESOURCE 1</th><th>RESOURCE 2</th><th>RESOURCE 3</th></tr> </thead> <tbody> <tr> <td>JACK</td><td>Read and Write</td><td>Read and Write</td><td>Read and Write</td></tr> </tbody> </table>	USER	RESOURCE 1	RESOURCE 2	RESOURCE 3	JACK	Read and Write	Read and Write	Read and Write	
USER	RESOURCE 1	RESOURCE 2	RESOURCE 3							
JACK	Read and Write	Read and Write	Read and Write							

Advantages of DAC

1. Easy to understand.
2. Easy to implement.
3. Flexibility to assign / revoke the needed rights granularly (precisely) on the resources.

Disadvantages of DAC

1. It requires careful evaluation and administration of each resource, user and her rights periodically.
2. Once the permissions are granted, the user has unrestricted access to the resource until permissions are manually revoked.

3. If a user mistakenly installs a malware program, then the malware program automatically inherits the DAC permissions that were assigned to the user. This inheritance and propagation (extension) of permissions is uncontrolled.
4. As the number of users increase, it becomes difficult to manage them and provide individual access right to each one of them.

2. Mandatory Access Controls (MAC)

 **Definition :** Mandatory Access Control (MAC) is an access control model that restricts access to system resources based on their sensitivity and the authorisation level of the entity trying to access the resources.

- Systems that are designed with the MAC model have highly restrictive use of rights. Unlike DAC model, one user (or resource owner) cannot provide rights to another user. The access control decisions are automatically taken by the system based on the sensitivity of the resource and the authorisation level of the entity trying to access the resource. MAC models are highly secure and are predominantly used in the military environment and systems. One example of such a system used today is SELinux (Security Enhanced Linux).
- Let's dive a little deeper to understand the MAC model.

A. Security Labels

- It is crucial to understand security labels to make any sense of MAC model.

 **Definition :** Security label is a way to associate a set of security attributes with a specific resource.

- A simple analogy to understand security label is food labels that you see on packed food items. Some are marked with a green dot meaning that those food items are safe to be consumed by vegetarians and some are marked with a red dot making them non-vegetarian products.
- Similarly, a resource can be labelled with security classification. Some of the security labels used in the military environment are:
 - o Top Secret
 - o Secret
 - o Confidential
 - o Sensitive
 - o Unclassified

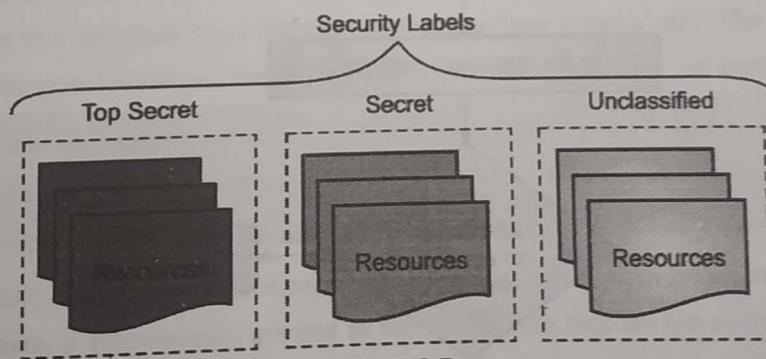


Fig. 5.3.5

- Here the security labels are hierarchical in nature. This means that "Top Secret" label is a higher sensitive label than the "Confidential" sensitive label. "Unclassified" is the lowest sensitive label. If a resource is assigned "Unclassified" label, it can be accessed by anyone in the general public. Similarly, "Top Secret" is the highest sensitive label. You may use the terms security labels and sensitive labels interchangeably.

B. Clearance Level

- As security labels are assigned to the resources, clearance levels are assigned to the entities (or principals).
- (Definition : A clearance level determines what resources an entity is authorised to access.)*

- Similar to security labels, clearance levels used in military are:

- o Top Secret
- o Secret
- o Confidential
- o Sensitive
- o Unclassified

- So, an entity with a clearance level of "Top Secret" can access all the resources that are marked with "Top Secret" security label or below. Since "Top Secret" is the highest clearance level, someone with that clearance level can access any information.
- For example, the prime minister of a country might have "Top Secret" clearance level. She will then have access to all national secret files, project plans and missions. Whereas a general government clerk might only have "Sensitive" clearance level. "Sensitive" clearance level would restrict access to resources that are marked "Sensitive" or below. Similar to security labels, clearance levels are also hierarchical in nature.

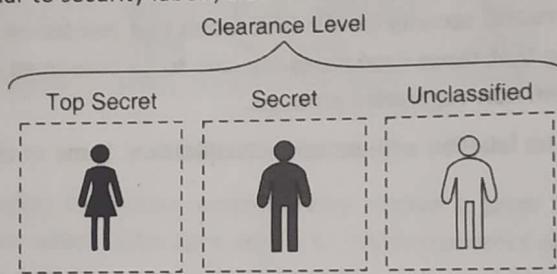


Fig. 5.3.6

C. Access Decisions in MAC

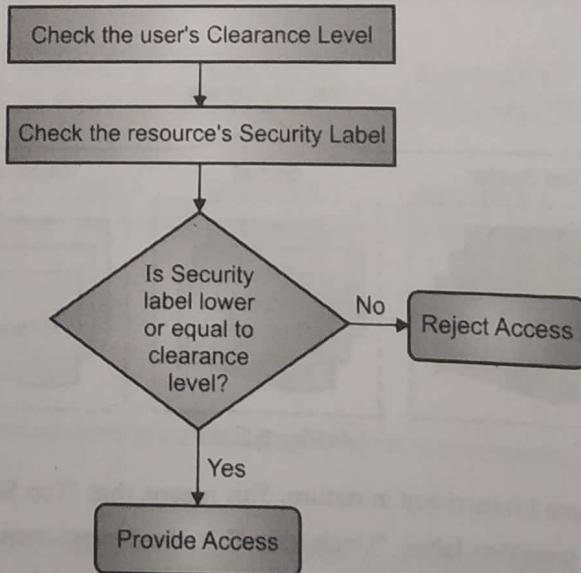


Fig. 5.3.7

Now that you understand security label and clearance level, let us put these two concepts together to understand how MAC systems decide whether to allow access or reject it. The system first checks the clearance level of the entity requesting access to the resource. Then, the security label of the requested resource is checked.

- o If the security label of the requested resource is lower or equal to the clearance level of the requesting entity, then the access is provided.
 - o If the security label of the requested resource is higher than the clearance level of the requesting entity, then the access request is rejected.
- As a rule, an entity is allowed to access resources that are marked with a security label lower or equal to its own clearance level.

Advantages of MAC

1. All resources on the system are adequately labeled.
2. Access decisions are automatically taken based on the clearance level of the requesting entity.
3. Access control policies are enforced system-wide.
4. It provides finer access policies and protects confidentiality and integrity of resources.
5. It is a scalable model for providing access control. Individual users are not required to provide access rights.

Disadvantages of MAC

1. Difficult to configure and implement.
2. Difficult to understand compared to DAC.
3. Inflexible to provide any specialized access.

3. Role-Based Access Control (RBAC)

- Individuals in organisations have different job functions. They are assigned roles as per their skills and as per the organisation's requirements. For example, a college principal has a very different role to play than a professor. Similarly, a director in a company has a different role to play than a junior staff. The various duties assigned to the individuals demand various access requirements and capabilities to match the given role.

Definition : Role-Based Access Control (RBAC) is an access control model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

- The objective of RBAC is to define a set of permissions for roles rather than individuals. A user, when assumes a role within the system, is automatically granted all the permissions that are pre-defined for that role. She should be able to carry out all the tasks that are assigned for the users in that role.
- For example, on a typical Windows® system, there are pre-defined groups (that work as roles).

Usermgr - [Local Users and Groups (Local)\Groups]		
	Name	Description
Local Users and Groups	Access Control Assistance Operators	Members of this group can remotely query authorization attributes and permissions for resources on this computer.
Users	Administrators	Administrators have complete and unrestricted access to the computer/domain
Groups	Backup Operators	Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
	ConfigMgr Remote Control Users	Members in this group can view and control this computer using Configuration Manager Remote Control
	Cryptographic Operators	Members are authorized to perform cryptographic operations.
	Distributed COM Users	Members are allowed to launch, activate and use Distributed COM objects on this machine.
	docker-users	Users of Docker for Windows
	Event Log Readers	Members of this group can read event logs from local machine
	Guests	Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
	Hyper-V Administrators	Members of this group have complete and unrestricted access to all features of Hyper-V.
	IIS_IUSRS	Built-in group used by Internet Information Services.
	Network Configuration Operators	Members in this group can have some administrative privileges to manage configuration of networking features
	Performance Log Users	Members of this group may schedule logging of performance counters, enable trace providers, and collect event traces both locally and remotely
	Performance Monitor Users	Members of this group can access performance counter data locally and remotely
	Power Users	Power Users are included for backwards compatibility and possess limited administrative powers
	Remote Desktop Users	Members in this group are granted the right to logon remotely
	Remote Management Users	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service)
	Replicator	Supports file replication in a domain
	System Managed Accounts Group	Members of this group are managed by the system.
	Users	Users are prevented from making accidental or intentional system-wide changes and can run most applications

- Each of these roles has pre-defined access rights.

Local Group Policy Editor		
File Action View Help		
Local Computer Policy	Policy	Security Setting
Computer Configuration	Access Credential Manager as a trusted caller	
Software Settings	Access this computer from the network	Everyone,*S-1-5-21-2606523528-2216722369-1744952207-1001,Administrators,Users,Backup Operators,Device Owners
Windows Settings	Act as part of the operating system	
Name Resolution Policy	Add workstations to domain	
Scripts (Startup/Shutdown)	Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVICE,Administrators
Deployed Printers	Allow log on locally	Guest,Administrators,Users,Backup Operators,Device Owners,Window Manager,Window Manager Group
Security Settings	Allow log on through Remote Desktop Services	Administrators,Remote Desktop Users
Account Policies	Back up files and directories	Administrators,Backup Operators
Local Policies	Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SERVICE,Administrators,Users,Backup Operators,Device Owners
Audit Policy	Change the system time	LOCAL SERVICE,Administrators
User Rights Assignment	Change the time zone	LOCAL SERVICE,Administrators,Users,Device Owners
Security Options	Create a pagefile	Administrators
Windows Defender Firewall with		

- Here the roles can be hierarchical. So, someone assuming "administrator" role can pretty much do anything on the system whereas "Guests" role has limited access. Users are assigned to the respective role(s). A user might be assigned more than one role on a system. Her capability to perform tasks on the system would depend on the role that she logs in with.

Advantages of RBAC

- Roles fit more naturally to the job function rather than the individual user identities.
- Easy administration – users can come and go without needing to change the defined rights for a given role.
- Easy to understand.

Disadvantages of RBAC

- Role explosion – There are various job functions performed by individuals in an organization. It is complex to define precise role requirement for each task and manage them as the organization and business requirements evolve.
- Not all systems support fully functional RBAC capability.

4. Attribute-Based Access Control (ABAC)

Definition : Attribute-Based Access Control (ABAC) is an access control model in which access is decided by the policy enforced on subject and object attributes.

Subjects (entities) and Objects (resources) are assigned various attributes. These attributes are evaluated before every requested access and the access is granted only when the attributes of both subjects and the objects match based on the pre-defined policy.

A. Attributes

Definition : Attributes are key characteristics that can be assigned to various things to describe their state, behaviour or condition.

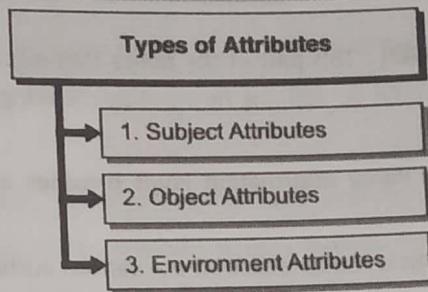


Fig. 5.3.8

There are 3 types of attributes involved in ABAC.

1. Subject Attributes (S) :

These are attributes associated with a subject that defines the identity and other characteristics of that subject. Some of the attributes could be role of the subject, identity of the subject, location of the subject, age of the subject, etc.

2. Resource Attributes (R) :

These attributes are associated with a resource. The resource could be a computer, file, data or anything else. The various attributes could be resource sensitivity, type of resource, location of the resource, age of the resource, etc.

3. Environment Attributes (E) :

It describes the operational, technical, situational or contextual information under which access decision should be evaluated. For example, time of the day, or day of the week, etc.

B. Policy

Definition : A policy is a set of statements or rules that specify the correct and expected behaviour of entities.

- ABAC system uses policies to describe various attributes to evaluate access decisions. ABAC policy rules are evaluated as IF THEN statements.

IF (Attributes are matched)

THEN (allow or deny)

...

...



For example :

- Nurses in the Cardiology Department can View the Records of Heart Patients.
- Underlined words in the above policy line are various attributes that must match to allow access.
- Policy is the crucial element of any ABAC system and there are various points that manage different parts of policy components and execution.

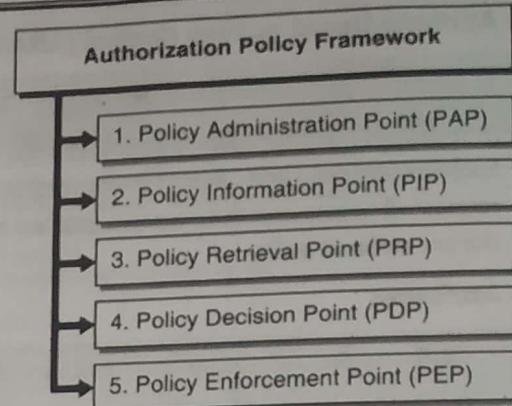


Fig. 5.3.9

1. **Policy Administration Point (PAP)** : This part of the policy framework involves general administration of various authorisation policies. These could be defining new policies, editing policies, deleting policies or archiving them for later reference.
2. **Policy Information Point (PIP)** : Policy Information Point provides attribute values for subjects, resources and environment.
3. **Policy Retrieval Point (PRP)** : This is the database where various authorisation policies are stored.
4. **Policy Decision Point (PDP)** : At this point, the various authorisation policies are evaluated. Based on the evaluation results, an authorisation decision is made either to allow or deny access.
5. **Policy Enforcement Point (PEP)** : Policy Enforcement Point receives all access requests for accessing resources from subjects. It consults PDP. If PDP allows the access, PEP lets the subject access the requested resources.

C. Access Decision in ABAC

- Let's understand how access decision is taken in ABAC.

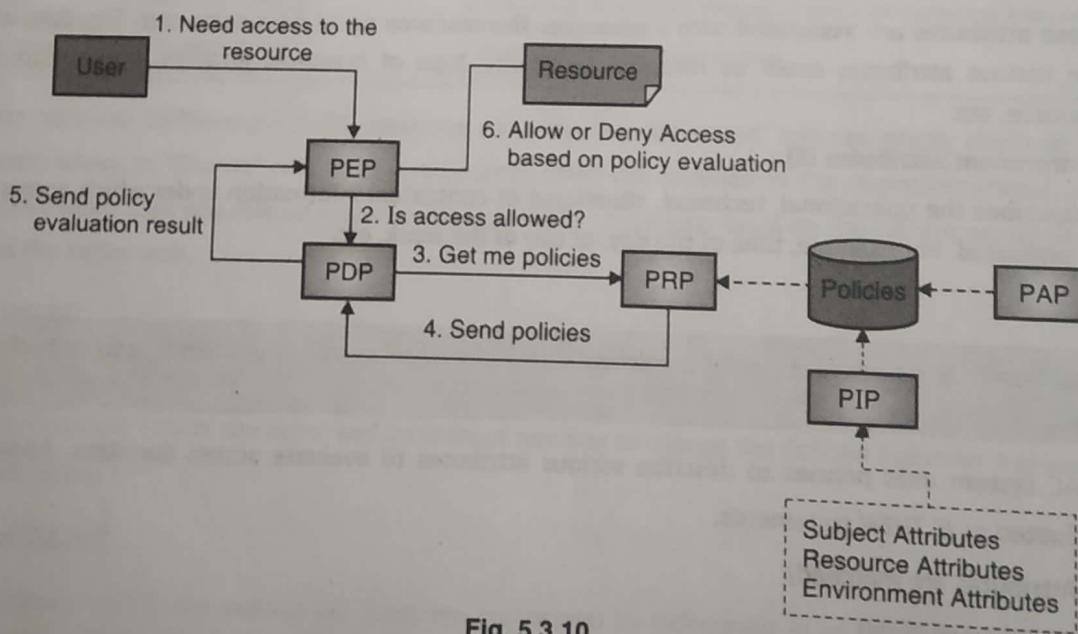


Fig. 5.3.10

- Access decision in ABAC is based on the policy definitions.

1. The user sends the request to PEP seeking access to the desired resource.
2. The PEP forwards the request to the PDP to evaluate if it should allow access based on the policies.

3. The PDP forwards the policy related information it requires from the PRP based on the user seeking the resource and environment conditions.
4. The PRP retrieves the various policies in the context of subject, resource and environment and sends the policies to the PDP for evaluation.
5. The PDP evaluates the policies related to the user, resource and environment conditions. It passes the evaluation result [allow access or deny access] to the PEP.
6. The PEP finally either allows access or denies it based on what it heard from PDP.

Advantages of ABAC

1. It is flexible enough to define granular conditions under which access should be granted.
2. It is scalable as the number of users and resources increases.
3. It offers a dynamic way of evaluating access decisions rather than evaluation based on identity or role.
4. It can be extended to the external users that are not part of the organisation.

Disadvantages of ABAC

1. Requires investment in infrastructure for an operational ABAC system.
2. Need to manage policies separately and periodically update them as the business environment evolves.
3. As the number of policies grows, it could be complex to understand.

5.4 Trusted Systems

SPPU - May 19

Q. What is trusted system ?

(May 19, 4 Marks)

- Designing a secure system is a complex task. You need to follow several basic elements of security and need to model the security of the system around approved principles. These security principles are often derived and stated in mathematical formulae. One such model is the State Machine Model.

Definition : The State Machine Model ensures that a system is in a secure state all the time. Any events that alter the state of the machine are not allowed.

- It means that the system boots up in a secure state, carries out operations that are secure and then shutdown securely. A system is continuously in the secure state. Let us examine two such state machine models in detail.

5.4.1 Bell-LaPadula (BLP) Model

- The Bell-LaPadula (BLP) Model was developed in 1970s for the US military to avoid disclosure of sensitive information. It addresses confidentiality aspects of access control and ensures that the sensitive information is not leaked. Its application has been mathematically proven to ensure confidentiality.

Definition : The Bell-LaPadula Model is a state machine model that enforces confidentiality aspects of access control.

- Like Mandatory Access Control, BLP model uses security levels for classifying subjects and objects.

Definition : A system that uses security levels for classifying subjects and objects is called a multilevel security system.

- The BLP model has 4 core components.
 1. **Subjects** : Entities that desire access to the resources
 2. **Objects** : The desired resources [file, information, server, etc.]
 3. **Actions** : Read, Write
 4. **Security Levels** : Sensitivity labels [for example, top secret, secret, confidential, sensitive, unclassified]
- The BLP model provides four rules for access control.

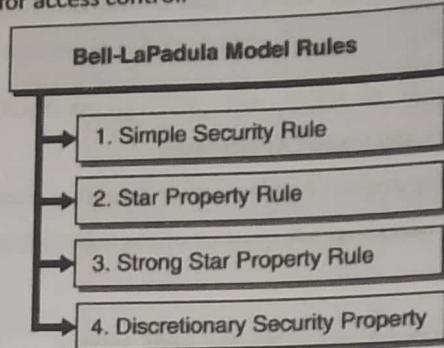


Fig. 5.4.1

1. Simple Security Rule

 **Definition :** The Simple Security Rule in the Bell-LaPadula Model states that a subject cannot read an object at a higher security level than itself.

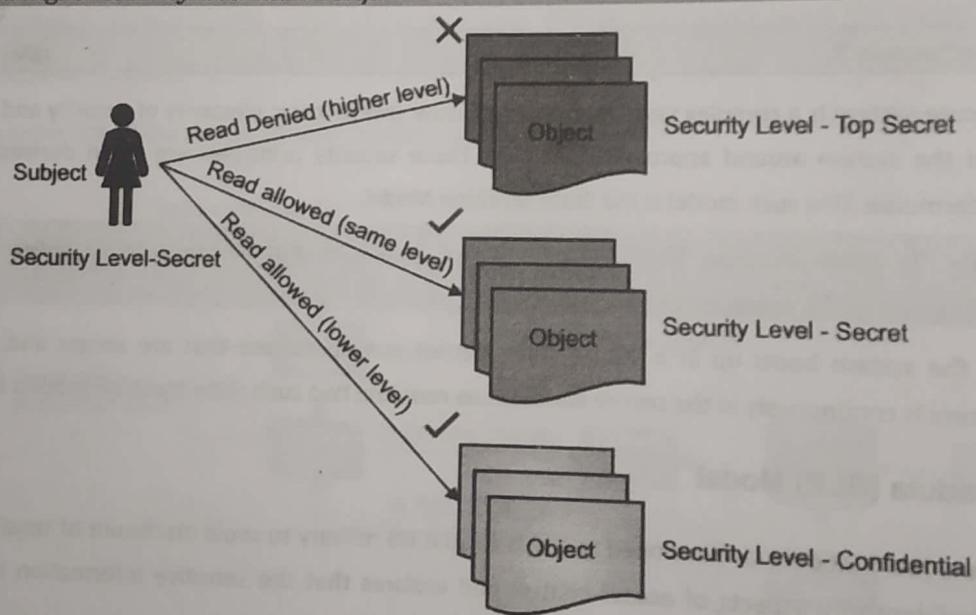


Fig. 5.4.2

- This rule is also called "No-Read Up" or simple security property (ss-property). What this means is that any subject must have a security level greater than or equal to the security level of the object it is trying to access. A subject cannot read an object at a higher security level than itself.

For example : take a practical scenario. Does everyone in a country can get access to the military plans and missions? Why not? The security level of military information is so high that general citizens do not have adequate clearance level to get access to it.

Take another example of your house. Can everyone access your locker? Why not? The trust level (or the security level) of everyone is not high enough to access the locker, isn't it? That's precisely what the simple security rule tells you. Do not allow an entity at a lower trust level to access higher trust level objects (or resources).

2. Star Property Rule

Definition : The Star Property Rule in the Bell-LaPadula Model states that a subject cannot write to an object at a lower security level than itself.

- This rule is also called "No-Write Down". What this means is that no subject can write to objects that are at a lower security level than itself. However, writing to objects at a higher security level is allowed.
- Let's take an example. Did you hear about the demonetization of 8 November 2016 before the PM announced it? Perhaps, no. Who else do you think would know about such a move? I hear you saying that very highly placed and trusted sources. Exactly. So, subjects that have access to highly trusted information are not supposed to write it down (or share) with someone who is not at an equally trusted level.
- That's precisely what the Star Property Rule in the BLP model tells you. Do not share (or write) higher security level information with an object at a lower security level. If you do so, subjects at a lower security level can read such objects and can know about the information you wrote that was not supposed to be shared. Remember that the BLP model focuses on confidentiality. Such, lower level sharing could mean disclosure and hence the Star Property Rule of the BLP model denies it.

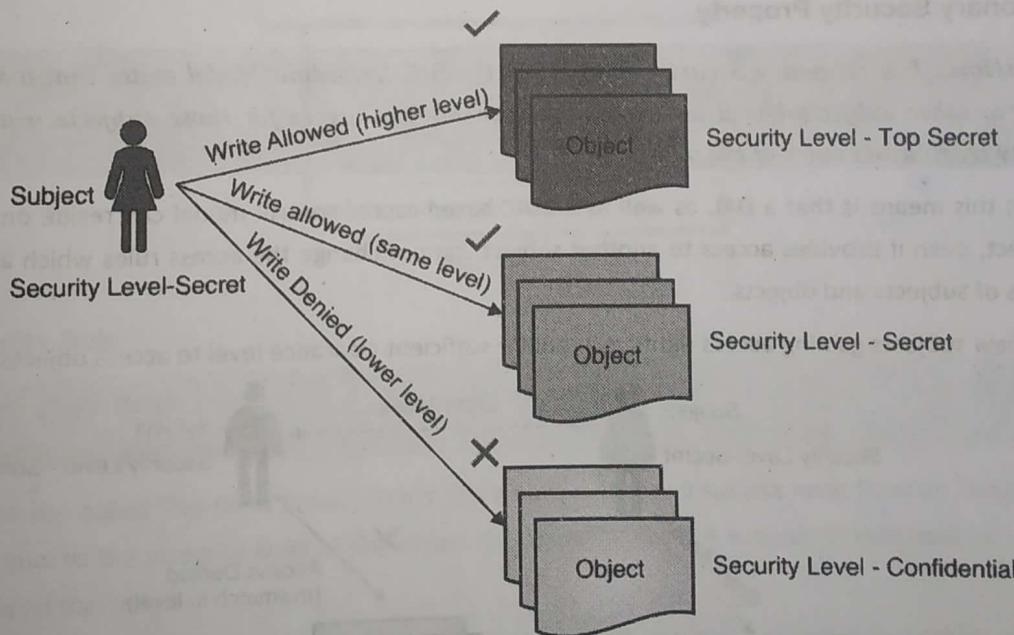


Fig. 5.4.3

3. Strong Star Property Rule

- Definition :** The Strong Star Property Rule in the Bell-LaPadula Model states that a subject can only read and write to an object at the same security level as itself.
- You can consider this as a combination of first two rules – Simple Security and Star Property. Simple Security Rule deals with Read operations whereas the Star Property Rule deals with Write operations.
 - So, if a subject has to do both – read and write – combining those two rules – gives permissions to do so only if the subject and the object are at the same security level.

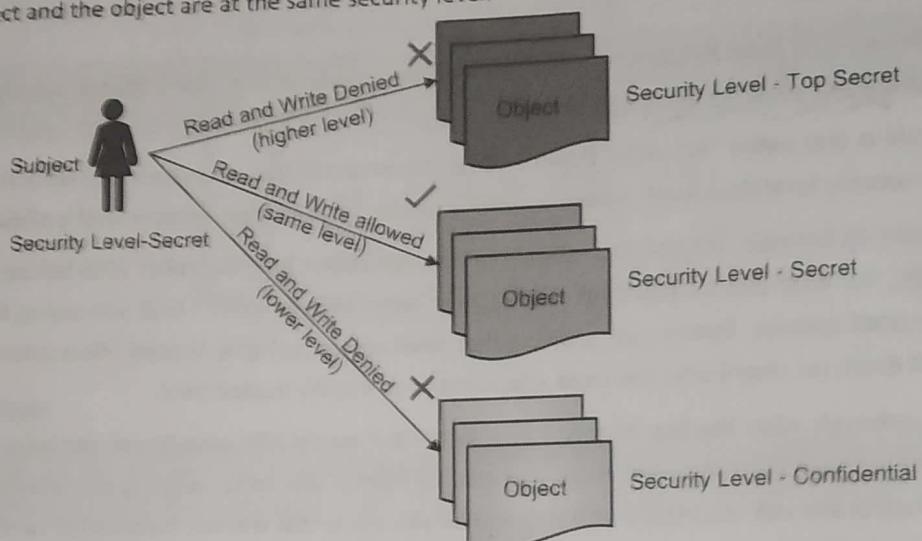


Fig. 5.4.4

4. Discretionary Security Property

- Definition :** Discretionary Security Property in the Bell-LaPadula Model states that a subject can provide access to other subjects based on its own judgement. The access for those subjects would still follow the security level-based rules of the model.

- What this means is that a DAC as well as a MAC based access control model can reside on the same system. A subject, even if provides access to another subject, cannot change the access rules which are based on security levels of subjects and objects.
- The new subjects gaining access rights still require sufficient clearance level to access objects.

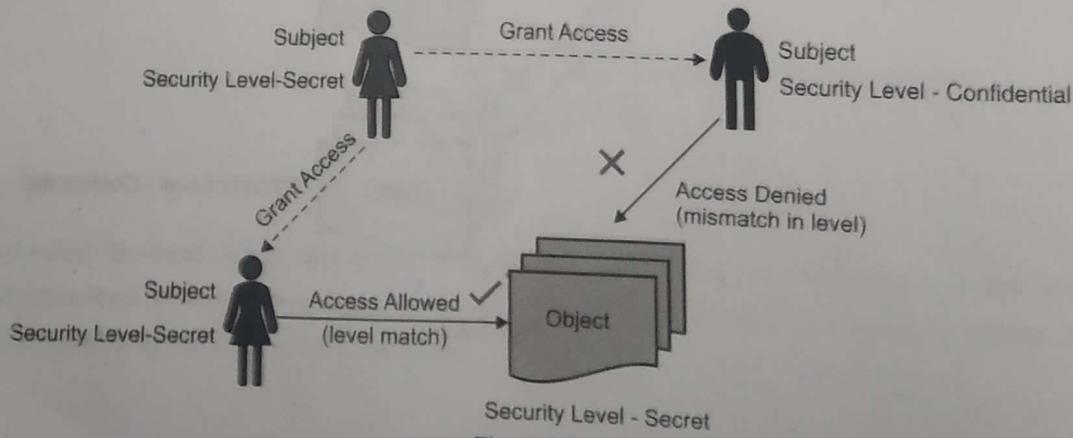


Fig. 5.4.5

Summary

Sr. No.	Rule Name	Purpose
1.	Simple Security	Secure Read Operations (no read up)
2.	Star Security Property	Secure Write Operations (no write down)
3.	Strong Star Property	Secure Read and Write Operations (read and write at same level only)
4.	Discretionary Property	Access Grant Operations (first 3 rules apply even if access is granted)

5.4.2 Biba Model

- The Biba Model was developed in 1975 to avoid alteration of information. It addresses integrity aspects of access control and ensures that the information (data) is not altered by unauthorised entities. Its application has been mathematically proven to ensure integrity.

 **Definition :** The Biba Model is a state machine model that enforces integrity aspects of access control.

- Unlike the BLP model, the Biba model uses integrity levels for classifying subjects and objects. Integrity levels can be thought to follow similar hierarchy as security levels. It is just that it is called integrity level instead of security level when referring to the Biba model.
- The Biba model provides three rules for access control.

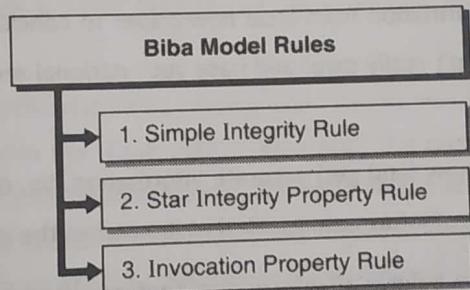


Fig. 5.4.6

1. Simple Integrity Rule

 **Definition :** The Simple Integrity Rule in the Biba Model states that a subject cannot read an object at a lower integrity level than itself.

- This rule is also called "No-Read Down". What this means is that any subject must have an integrity level greater than or equal to the integrity level of the object it is trying to read. A subject cannot read an object at a lower integrity level than itself.
- Confused? Do not compare the rule with the BLP model. Here you are not trying to protect confidentiality but ensuring integrity of information.

- Let's take an example. Suppose that you are the Prime Minister of a country. Should you attack on a country by just reading some article in a local newspaper that is speculating about the plans of the enemy country to attack your country? Probably not. You will check the information from your security agencies.
- The information coming from national security agencies would be more accurate and factual rather than speculative.

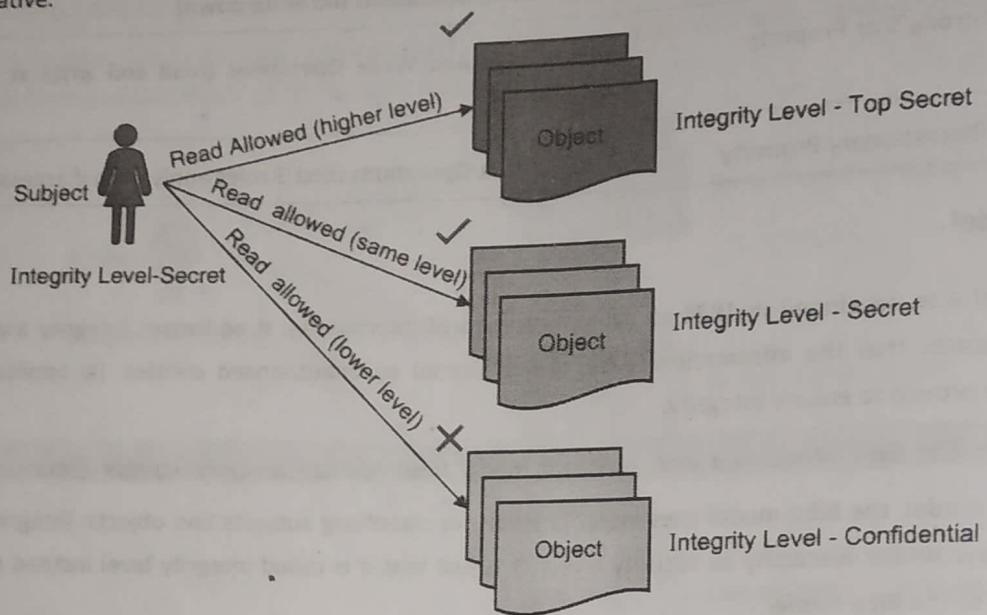


Fig. 5.4.7

- You won't read and consume information from local newspaper to conclude on your decisions. So, you, being Mr. PM, won't read (or rather won't really care) and base your national security decisions on articles at a lower integrity (assurance) level.
- You at your level really need to know (and get) accurate information. So, don't read articles that are at a lower integrity level. Maintain the source of information such that it matches the integrity level you are at.
- Let's take another example. Do you believe all information that you receive on WhatsApp or other social media platform? Haven't you encountered fake messages or rumours anytime? Don't you feel that all information on social media platform is not accurate and there is a need to validate the truth (integrity) of the information before believing it? Don't you check for the validity of the information from sources which are more trusted such as news channels and newspapers? That's precisely what Biba model tells. The information you consume should match your integrity level.

2. Star Integrity Property Rule

- Definition :** The Star Integrity Property Rule in the Biba Model states that a subject cannot write to an object at a higher integrity level than itself.
- This rule is also called "No-Write Up". What this means is that a subject is not allowed to write information to the objects that are at the higher integrity level. What would happen if such a write is allowed? The lower integrity subject can corrupt the higher integrity information.

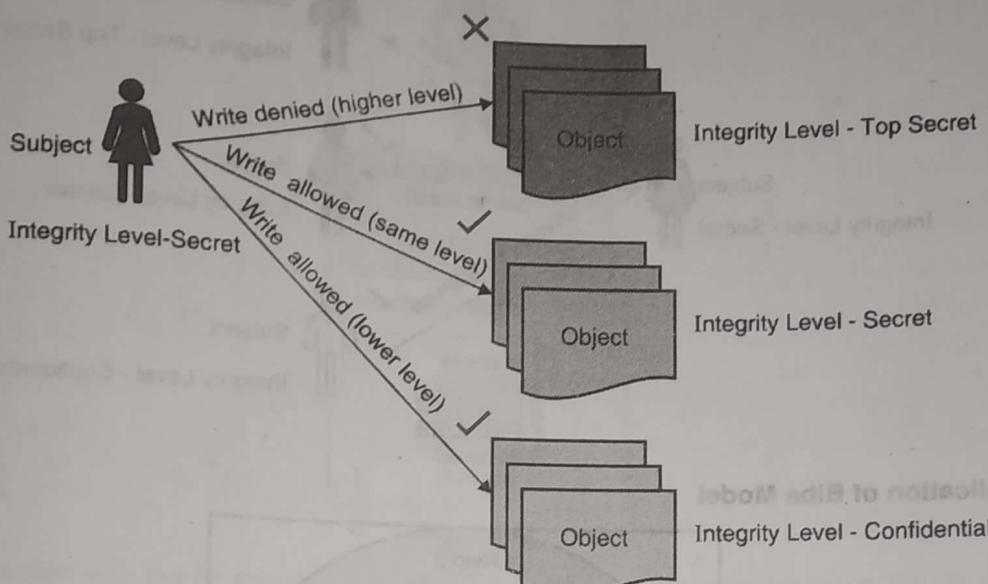


Fig. 5.4.8

- Again, don't be confused. You are not protecting confidentiality here but integrity. Let's take an example. Would a national level newspaper allow printing of national level news from anyone? Perhaps no. it would doubly check even from its most trusted journalists that the news is accurate to the best of their knowledge. So, basically, when someone is writing to a much valued (trusted) object, that source (or subject) who is writing it must be trusted enough to allow such a write. You do not allow anyone and everyone to write information on such trusted objects.
- Let's take another example. Who should be feeding exam results into the results portal? Would an institute allow everyone to enter the marks in the result portal? Why not? The reason again being that the institute does not want to corrupt the legitimate marks information. Someone who is at a lower integrity level might pass someone who is actually a fail. The marks can be increased or decreased as well during entering them in the results portal. So, the results portal, that is trusted by thousands of candidates, would not and should not display incorrect results. The integrity of results is much more important than the confidentiality of the results. That's what Biba's Star Integrity Property Rule tells you.

3. Invocation Property Rule

Definition : The Invocation Property Rule in the Biba Model states that a subject cannot communicate with another subject at a higher integrity level than itself.

- Let's take an example. Will an army chief work on instructions from a commander? Will a principal work on instructions from a peon? Will You work on instructions from a stranger without any authority? I think you get it now.
- The Invocation Property Rule allows a subject to communicate with another subject only if the subjects are at the same or lower integrity levels. A lower integrity level subject cannot communicate (or invoke or call) a higher integrity level subject.

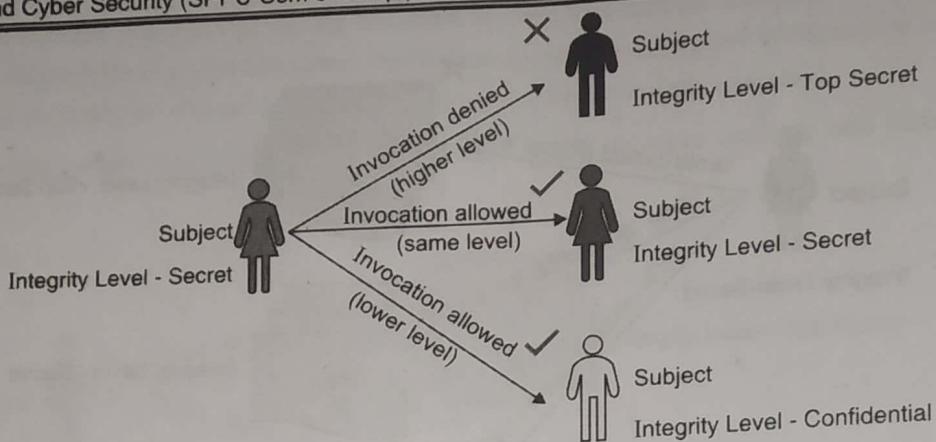


Fig. 5.4.9

Practical Application of Biba Model

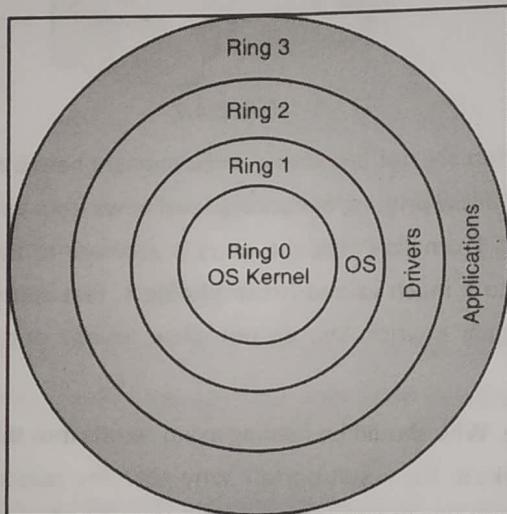


Fig. 5.4.10

- So, where is Biba model seen these days? In the CPU and Operating System architecture.
- The CPU typically has a protection ring architecture whereby the most trusted components of the system have access to higher privileges (permissions), and the untrusted components are executed in the outer ring with lesser privileges.
- The OS and CPU developers do not know in advance that what are application developers going to do. Hence, the protected ring mechanism ensures that the higher privilege commands and instruction sets are not available to the applications. Applications if need to execute such commands then they must make a system call to the operation system which can execute the commands on the behalf of such applications.
- Similarly, Operating Systems (OS) put strict controls in terms of what a user or application can do. OS is responsible for managing all interactions with the hardware on a computer and thus is directly responsible for managing its logical security. It also employs the layered architecture to protect the information systems.
- The outer most layer is User Space. In this space, the user installs applications and interacts with other functions of the operating system such as playing a music or storing a file. Space below user space is called the kernel space. This is operating system's private area. User or applications cannot directly interact with the OS in this area.

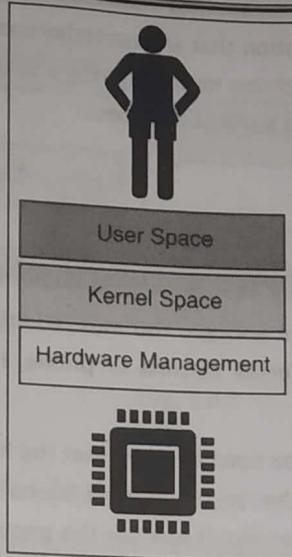


Fig. 5.4.11

- Also, interaction with the hardware is restricted via the OS only. In the kernel space, the OS performs various functions such as Input Output Management, Memory Management, Disk Management, CPU process handling and other general hardware functions.
- So, to maintain the overall system integrity the entities are controlled according to the Biba model. Entities are only allowed to read and write to what their integrity level permits. So, for example, a virus program is restricted to write to the kernel memory.

Summary

Sr. No.	Rule Name	Purpose
1.	Simple Integrity	Secure Read Operations (no read down)
2.	Star Integrity Property	Secure Write Operations (no write up)
3.	Invocation Property	Secure Communications (no interaction with higher level subject)

5.5 Authentication Methods

Before you jumpstart on authentication methods, let's refresh a few terms and concepts around it.

5.5.1 Introductory Concepts

1. Identification

- Identification (in short ID) is defined as,

Definition : A way to claim an entity's presence with respect to the process being carried out.

- This means that during a process, your presence (or your consent) is ascertained (or established). For example, when you try to login to your Facebook account, you provide your Email or Phone number to establish your presence during the login process.

- There are several other forms of identification that we use today such as Aadhar Card, PAN Card, Voter ID, Debit Card, Admit card, etc. All of these identification methods bring a sense of credibility that you are present, or you give your consent (approval) to complete a particular process.

2. Authentication

- Authentication is defined as,

 **Definition :** A way to ensure that the entity is indeed what it claims to be.

- This means that providing just the ID is not enough. You must additionally prove that the ID belongs to you. For example, even if I know your Facebook email address or phone, I cannot login as you until I also know the password.
- Thus, knowing just the ID is not enough. You need to prove that the ID belongs to you and that is what is precisely called authentication. It is for this reason that you need to additionally sign when you submit Aadhar card or PAN card as an ID proof to ensure that someone didn't just use the photocopy of those IDs without your permission (or consent).
- Some of the ways to authenticate an ID are passwords, biometric (like your Aadhar fingerprints or phone sensor), PIN (like for Debit Card), or OTP (SMS that you get to confirm a transaction).

3. Authorisation

- Authorisation is defined as,

 **Definition :** A way to determine what resource an entity can access.

- Once you have provided your ID and have been successfully authenticated, the next step is authorisation where the system determines if you have the permission to access the desired object. For example, even if you have a valid voter ID card but if your name is not on the electoral list at a particular area booth, you won't be allowed to vote. Having authenticated ID is one thing and getting access to the resource is another.
- Just because you have an authenticated ID, does not mean that you have automatically access to the resources. So, authenticated ID is a must for authorisation but that does not always guarantee that you would be allowed access.

4. Accountability

- Accountability is defined as,

 **Definition :** A way to record your actions.

- Suppose, you used a system to take print outs. That system logs this action (pretty much like you record attendance in lab or classroom) to build a trace (evidence or proof) that you used the printer.
- If you were not supposed to use the printer, the evidence can be used to find you accountable for using it without permissions and could result in particular consequences.
- Accountability is a key determinant of how securely a system is operating. The logs generated are continuously monitored and necessary alarms are raised if any entry is found to be suspicious.
- Let's summaries the 4 access control steps with the help of Fig. 5.5.1.

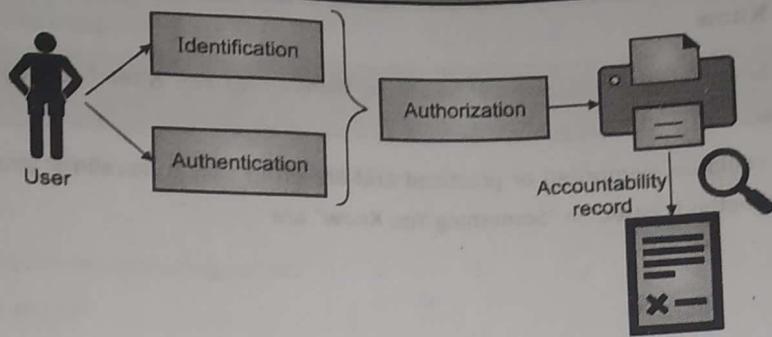


Fig. 5.5.1

5. Non-repudiation

- Non-repudiation is defined as,

Definition : A way to prove your actions.

- It is used in conjunction with authentication and accountability. Non-repudiation provides an assurance that someone cannot deny their actions later on. For example, if I sent you an email, I cannot later deny that I did not.
- To send an email, I must have used my email ID and password and then sent it over to you over a secure network where no one could change the email body. If you can establish all of these facts truthfully, you have proven that I sent that email and thus established non-repudiation.

5.5.2 Types of Authentication Methods

- Over time, various authentication methods have evolved to address
 - o the ease of authentication
 - o make it hard to break authentication
 - o make authentication techniques suitable for various devices
- At a high level, authentication methods are categorised as shown in Fig. 5.5.2.

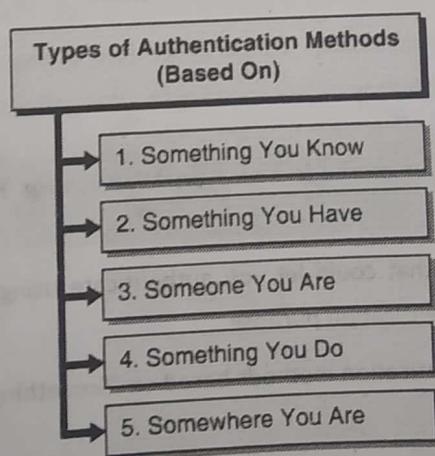


Fig. 5.5.2



1. Something You Know

 **Definition :** The authentication methods based on "Something You Know" rely upon your secret knowledge about something.

- These secrets could be memorised or practiced and are often easy to recall for you. Some of the examples of authentication methods based on "Something You Know" are
- Passwords
- PIN
- Passphrases
- Secret questions
 - o Mother's maiden name
 - o First pet name
 - o First car purchase year
 - o First school name
 - o City in which you were born
 - o Or other secret questions whose answers would be likely known just to you
- Lock key combination

Advantages of "Something You Know" type authentication

- Easy to implement by developers in the product (OS, Applications or Websites)
- Easy to recall for the user
- Easy to authenticate for the user
- Easy to change for the user
- Chances of errors are low
- Can be used by non-person entities (hardware devices, applications, OS, programs, processes, etc.)

Disadvantages with "Something You Know" type authentication

- Easy to crack (or break)

2. Something You Have

 **Definition :** The authentication methods based on "Something You Have" rely upon your possession of something.

- You could possess something that could let you authenticate using it. You often don't require to remember anything while using it for authentication purpose.
- Some of the examples of authentication methods based on "Something You Have" are
 - o Physical keys
 - o Badge
 - o Swipe Card (for example Debit or Credit Card)
 - o Digital Certificates

- o Security Keys (for example Private Key)
- o OTP (that you get via SMS)
- o Tokens

Advantages of "Something You Have" type authentication

- Easy to use
- Does not often require remembering secrets
- Chances of errors are low
- Not easy to crack
- Can be used by non-person entities (hardware devices, applications, OS, programs, processes, etc.)

Disadvantages of "Something You Have" type authentication

- Difficult to change
- Possibility of loss or theft
- Requires distribution methods (provisioning) to reach to the user securely

3. Someone You Are

 **Definition :** The authentication methods based on "Someone You Are" rely upon your physical characteristics.

- Your body has several physical characteristics that can be used to uniquely identify and authenticate you. These characteristics do not much change over time (as you age) and can serve authentication purpose for near lifetime.
- These characteristics are called Static Biometrics.

 **Definition :** Static Biometrics are physical characteristics that can be used for authentication.

- Generally speaking,

 **Definition :** The measurement and analysis of unique physical or behavioural characteristics is called biometrics.

- However, there can be scenarios where re-provisioning (re-calibrating) your biometric details might be required. For example, if you use a particular finger for fingerprint and your that particular finger is damaged permanently, you might have to choose another finger or another type of biometrics for authentication.
- Some of the examples of authentication methods based on "Someone You Are" are
 - o Fingerprint
 - o Palm Scan
 - o Hand Geometry
 - o Retina Scan
 - o Iris Scan
 - o Facial recognition

Advantages of "Someone You Are" type authentication

- Easy to use
- Does not often require remembering secrets
- Difficult to crack

Disadvantages of "Someone You Are" type authentication

- Difficult to implement correctly
- Chances of errors are high (recall you trying fingerprints several times at Aadhar enrolment centre?)
- Difficult to change (requires physical presence for re-provisioning)
- Cannot be used by non-person entities (hardware devices, applications, OS, programs, processes, etc.)

4. Something You Do

 **Definition :** The authentication methods based on "Something You Do" rely upon your way of performing a given task.

- This authentication method also collects biometric patterns but while performing a given task. Unlike static biometric patterns, these are dynamic biometric patterns which are used for authentication purpose.

 **Definition:** Dynamic Biometrics are job performing characteristics that can be used for authentication while an individual is performing a given task.

- Some of the examples of authentication methods based on "Something You Do" are
 - o Voice print (or pattern)
 - o Keystroke Dynamics (how hard you press the keys and how fast)
 - o Handwriting characteristics (remember old movies where handwriting matches were done?)

Advantages of "Something You Do" type authentication

- Easy to use
- Does not often require remembering secrets

Disadvantages of "Someone You Are" type authentication

- Difficult to implement correctly
- Not too difficult to crack (consider replaying a recorded voice)
- Chances of errors are high (have you tried voice to text yet?)
- Difficult to change (requires physical presence for re-provisioning)
- Cannot be used by non-person entities (hardware devices, applications, OS, programs, processes, etc.)

5. Somewhere You Are

 **Definition :** The authentication methods based on "Somewhere You Are" rely upon your physical location.

- Increasingly, the devices and systems have location awareness. Your mobile phone or laptops (via network connectivity) precisely know where you are located at a particular moment. "Somewhere You Are" uses the location information for authentication.

- For example, Google Smart Lock for Android allows you to set Trusted Locations. Say, if you are at home, your phone may not require you to unlock it (via PIN, pattern, password or fingerprint) before use.
<https://support.google.com/accounts/answer/6160273?hl=en>

Set your Android device to automatically unlock

You can keep your Android phone or tablet unlocked in some situations, like when your phone is in your pocket or you're near home. When you use Smart Lock, you won't need to unlock with your PIN, pattern, or password. The features you can use depend on your device.

If you want to change your screen lock, learn more about screen lock settings.

Note: Some of these steps work only on Android 9 and up. Learn how to check your Android version.

Turn on automatic unlock

1. Make sure you have a screen lock. Learn how to set a screen lock.
2. Open your device's Settings app .
3. Tap Security & location > Smart Lock.
4. Enter your PIN, pattern, or password.
5. Pick an option and follow the on-screen steps.

After setup, when you turn on your screen, you'll see a pulsing circle at the bottom around the Lock .

Important: When you don't use your device for 4 hours, and after it restarts, you'll need to unlock it.

Turn off automatic unlock

1. Open your device's Settings app .
2. Tap Security & location > Smart Lock.
3. Enter your PIN, pattern, or password.
4. Turn off On-body detection and remove all trusted devices, trusted places, trusted faces, and Voice Match voices.
5. Optional: If you want to turn off your screen lock, learn how to change your screen lock.

- "Somewhere You Are" is also quite widely used in corporate IT. In many environments, if you are on an office network (LAN or Wi-Fi), you can login using only a password, but if you are out of the office you must use VPN or an additional mechanism for authentication.

Advantages of "Somewhere You Are" type authentication

- Easy to use
- Does not often require remembering secrets
- Can be used for authenticating non-person entities (mobile, laptops or other location aware devices)

Disadvantages of "Somewhere You Are" type authentication

- Not too difficult to crack (consider theft and someone carrying the device to a trusted location)
- Cannot be used for authenticating individuals
- Requires network connectivity for location awareness

5.5.3 Comparison between the Authentication Types

Sr. No.	Type of authentication	Ease of use	Ease of Change	Ease of implementation	Error rate	Support non-person entities
1.	Something You Know	High	High	High	Low	Yes
2.	Something You Have	High	Low	Medium	Low	Yes
3.	Someone You Are	High	Low	Low	High	No
4.	Something You Do	Medium	Low	Low	High	No
5.	Somewhere You are	High	High	Medium	Medium	Yes

5.5.4 Factors of Authentication

Each type of authentication that you learnt in this section is called a factor of authentication. Based on the number of factors you choose for effectively carrying out and completing the authentication process, you have three types of authentication scenarios.

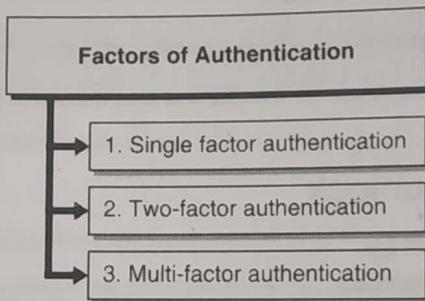


Fig. 5.5.3

1. Single factor Authentication

 **Definition :** Single factor authentication requires only ONE of the types of authentication for successfully carrying out the authentication process.

For example, you could just use password or token. This is most widely used. It is often treated as a weak form of authentication.

2. Two-factor Authentication

 **Definition :** Two-factor authentication requires you to use any TWO types of authentication, one after another, for successfully carrying out the authentication process.

- It is considered as a strong form of authentication. For example, for your online transactions, you are first required to give the account password and then you receive an OTP. You are required to put the correct OTP for successfully authenticating your account details and carrying out and completing your transaction.
- Another example could be ATM. You must possess your Debit Card (Something You Have) and put in the right PIN (Something You Know) for withdrawing money.

3. Multi-factor Authentication

Definition : Multi-factor authentication requires you to use MORE than two types of authentication.

It is often used in a high security environment. For example, you may be first required to give your fingerprint, after which you can access an application where you are required to provide username and password. For carrying out a transaction on that application, you might require an OTP.

Note : If two authentication techniques from the same type of authentication are used, it is not considered two-factor authentication. It would be considered a single factor authentication. For example, you cannot consider consecutive requirement of two passwords or a password and a PIN to be two-factor authentication. Two-factor authentication essentially requires two different ways to authenticate.

5.5.5 Password Based Authentication

Definition : A password is a protected sequence of characters that is used to authenticate an entity and provide access to a protected system.

- Passwords are the most widely used form of authentication. You can use it on computers, mobile devices, web portals, applications and nearly everything else that supports any form of user interface and requires authentication before use.
- Passwords fall into "Something You Know" type of authentication that you learnt earlier. The use of passwords requires effective password management that is strong enough to keep the passwords protected.

Choosing a Password

- Passwords, even though are the easiest to use amongst other types of authentication techniques, are also weakest form of authentication. Why? Because, users usually choose weak passwords which are easily breakable or guessable.
- Passwords can either be user chosen or be automatically generated by a trusted system.

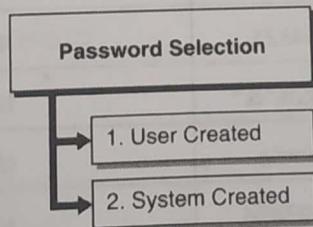


Fig. 5.5.4

1. User Created

- A user can typically choose her own password when signing up on a system. The problem here is that the users typically choose something that is extremely easy to guess.
- Some of the common and worst password choices of 2018 are as listed in Table 5.5.1.

Table 5.5.1 : Source : SplashData's Top 100 Worst Passwords of 2018

RANK	PASSWORD	CHANGE FROM 2017
1	123456	Unchanged
2	password	Unchanged
3	123456789	Up 3
4	12345678	Down 1
5	12345	Unchanged
6	111111	New
7	1234567	Up 1
8	sunshine	New
9	qwerty	Down 5
10	iloveyou	Unchanged
11	princess	New
12	admin	Down 1
13	welcome	Down 1
14	666666	New
15	abc123	Unchanged
16	football	Down 7
17	123123	Unchanged
18	monkey	Down 5
19	654321	New
20	!@#\$%^&*	New
21	charlie	New
22	aa123456	New
23	donald	New
24	password1	New
25	qwerty123	New

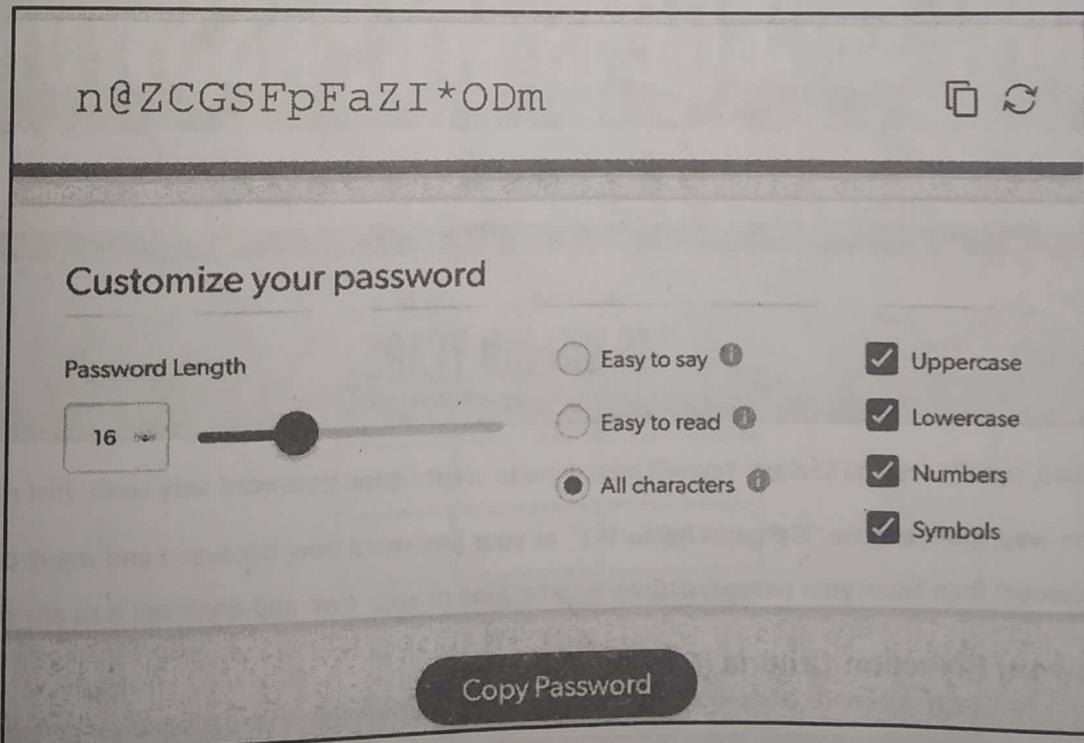
- Is your password on the list?
- Let's pick the first password from this list (123456) and find out how much time it would take a computer to break this password. <https://howsecureismypassword.net/> provides a good estimate of password cracking times with respect to the provided password.



- The provided password (123456) can be instantly broken. Would you choose that as your password still?

2. System Created

- Quite a few systems today offer passwords that are
 - o Randomly generated
 - o Difficult to crack and
 - o Easy to remember
- Such systems ensure that the important quality parameters for a good and strong password are matched in the suggested passwords.
- Here is a snapshot of LastPass password generator tool.



- It allows you to choose length, mix of characters and creates a random and strong password. Let's find the strength of the password it generated (n@ZCGSFpFaZI*ODm).

It would take a computer about
131 BILLION YEARS
to crack your password

- It would take 131 billion years for a computer to crack this password - n@ZCGSFpFaZl*ODm. Wow, now that is something called as a strong password! I would suggest choosing that if you are protecting something worthwhile!
- But, do you say that the password (n@ZCGSFpFaZl*ODm) is hard to remember? Ok, I hear you.
- Let me give you a tip. How about choosing an Indian festival as a password but slightly altering the characters? Let's take "Ganesh Chaturthi". I will replace "a" with "@" and "i" with "1". So, "Ganesh Chaturthi" would be "G@neshCh@turth1". Easy to remember? Ok, let's try this for a quality test.

It would take a computer about
16 BILLION YEARS
to crack your password

- Not bad, right? I see you smiling. You will learn how to create good password very soon. Just read on!
- By the way, don't choose "G@neshCh@turth1" as your password now because I and many other readers of this book would then know your password. Create something of your own and don't tell it to anyone.

5.5.6 Password Selection Criteria (Quality Guidelines)

SPPU – May 19

Q. Explain any two password management practices.

(May 19, 4 Marks)

Here are some general guidelines when choosing passwords.

1. Choose at least 12 characters in your password. The lengthier the password, the harder it is to crack it.

1. Use mix of characters.
 - a. At least one digit.
 - b. At least one uppercase letter.
 - c. At least one special character such as (@, #, \$, %, ^, &, *, (,), etc.).
2. Do not use the same password for all your accounts.
3. Do not use easy to guess passwords. Do not use your name, date of birth, school name etc. as your password.
4. Check your password quality before using it.
5. Do not use words found in the dictionaries. For example, avoid creating a password such as "Apple".

General Password Usage Guidelines

Here are some general guidelines to follow when working with passwords.

1. Do not send your password in cleartext. Avoid entering them on sites that do not use https.
2. Do not share your password with anyone in your family and friends.
3. Change your passwords periodically to avoid overuse.
4. Do not tell your password to anyone over phone or email howsoever the conversation may sound legitimate.
5. Wherever possible, use two-factor authentication with password.
6. Do not write down your password!

5.5.7 Storing Passwords on System

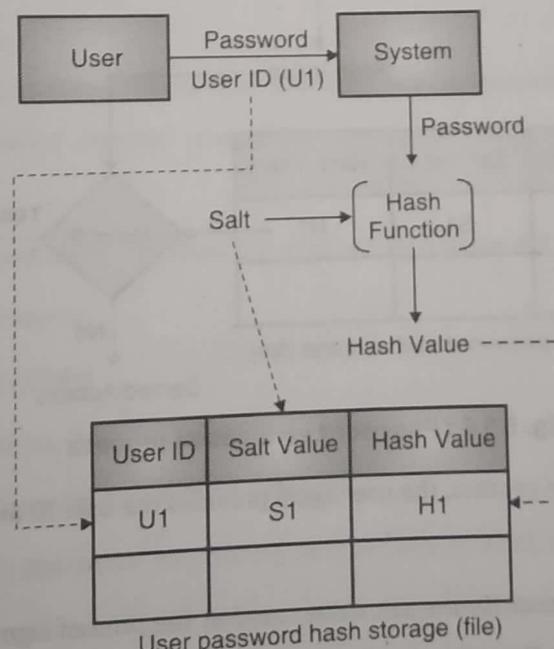


Fig. 5.5.5

When you enter your password on a Windows® or a Linux machine, how does the system know that you entered the right password? Does it compare your provided password, character by character, to the one previously stored on the system that you chose during sign up? No, it does not store your password in cleartext at anywhere on the system.

The passwords are adequately protected using hashes.

A. Sign up Process

- During the sign-up process, the user creates an ID and chooses a password that she would like to use when authenticating to the system.
- The system chooses a random salt value (nonce or any other random value) and passes that along with the user provided password to a hashing function. The hashing function computes the hash value. Then, the hash value and the corresponding salt value with the user ID is saved on the system in the form of a file. The system does not store password in cleartext at anywhere on the system.
- The purpose of the salt value is to bring randomness to the hashing process. So, if any two users provide the same password, even then, the entries in the password hash table file would not be the same. The random salt value also serves a purpose of defending the passwords from attack as you would see later in the section.

B. Password Verification Process

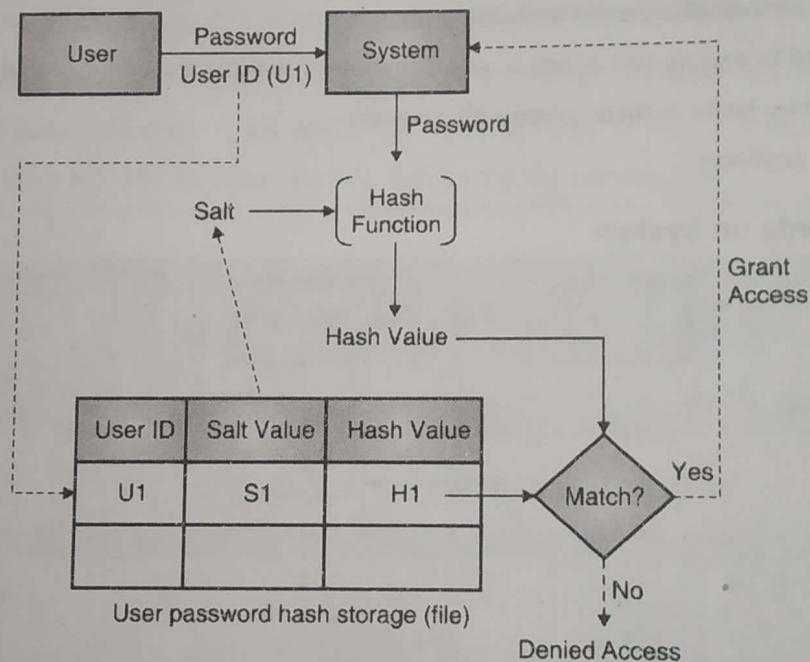


Fig. 5.5.6 : Password verification process

- During the password verification process, the user again provides the user ID and the password she set during the sign-up process.
- Corresponding to the provided user ID, the salt value, used at the time of sign up process, is picked up from the user password hash storage file. The salt value from the file and the user provided password are then fed to the same hashing function. The hashing function computes the hash value with the provided inputs.
- This hash value is then compared with the hash value stored in the user password hash storage file. If the two hash values match, the user provided the right password and is successfully authenticated to the system and is granted access. If the hash values do not match, the authentication process fails, and the user is denied access to the system. Fig. 5.5.6 explains the verification process.

5.5.8 Attacks, Limitations and Challenges on Password Based Authentication

As you know, password is the weakest form of authentication. There have been several mechanisms to attack on it. Let's learn about them.

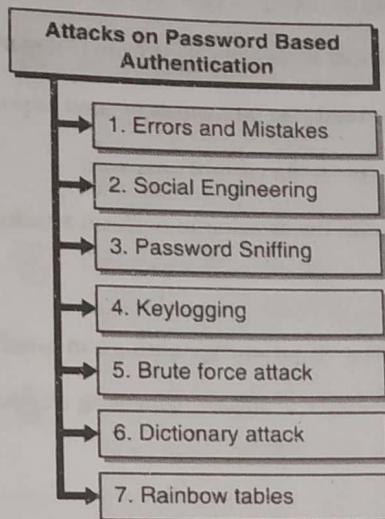


Fig. 5.5.7

1. Errors and Mistakes

- This is probably the most common reason due to which cracking passwords is not that hard. These are common pitfalls against the password creation and general password usage guidelines that you learnt earlier. The common mistakes are
 1. Choosing a weak password that does not align with the password selection guidelines
 2. Writing down passwords
 3. Sharing them with others
 4. Transferring or storing them in cleartext
 5. Using the same password for multiple accounts
 6. Choosing common passwords (something as in the top 25 worst passwords list that you saw earlier)
- Such errors and mistakes make it quite easy to crack password-based authentication and gain unauthorised access to the system.

Protection Mechanism

1. Avoid common pitfalls and adhere to the password selection and password usage guidelines.
2. Use two-factor authentication to ensure that the authentication is not processed only based on the provided password. Another form of authentication would be required before any access is granted to the system.

2. Social Engineering

As you learnt earlier, social engineering attacks can be carried out on the users. Users can be tricked to

1. Reveal the current password (say by posing as your manager needing access to something very quickly)
2. Reset the password (say by posing as someone calling from IT department and asking for quick reset)
3. Ask to install software that could read user passwords or send password hash storage file to the attacker
4. Click on links that could reset or reveal the current password
5. Or carry out anything else that helps the attacker to perform attacks on the password-based authentication

Protection Mechanism

1. Periodic user education and training on social engineering and cybersecurity.
2. Users should be repeatedly made aware of social engineering attacks and how not to get trapped.

3. Password Sniffing

- Passwords that are transferred without encryption (in cleartext) are prone to sniffing.

 **Definition :** *Packet Sniffing is the act of intercepting (capturing) of network traffic and logging it for further analysis.*

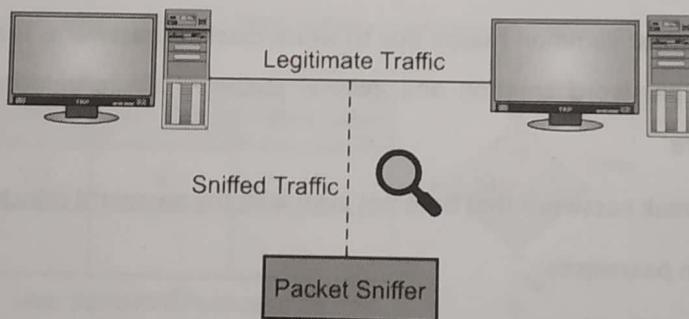


Fig. 5.5.8

- Packet sniffing is carried out using either software programs or hardware devices. These are called packet analysers or just packet sniffer. Wireshark is one of the most widely used Packet Sniffing program.
- Hence, as you see, as a best practice, never send or store your passwords in cleartext. These days browsers give you a warning when you are entering a password in a HTTP (and not HTTPS) site. The HTTP protocol sends information to the webserver in cleartext. You should not ignore such browser warnings. Avoid entering sensitive information such as password on such sites.

Login

username:

password:

login

Test with a dummy user
This demo contains a login page. Even though the form is secure (HTTPS) page, your credentials could be stolen.

More info at stealmylogin.com

Site Information for www.stealmylogin.com

Connection
Connection Is Not Secure
Logins entered on this page could be compromised.

Content Blocking
Strict
No blockable content detected on this page.

Permissions
You have not granted this site any special permissions.

- You cannot, to a great extent, avoid network sniffing attempts since it is external to the network and mostly beyond your control. For example, how do you protect someone with Wi-Fi analysing device to capture your Wi-Fi packets? However, some of the common protection mechanisms to reduce the impact from sniffing are as follows.

Protection Mechanism

1. **Encryption** : Use TLS, VPN tunnels or application level encryption wherever possible to avoid sending and receiving data in plaintext.
2. **Use secure protocols** : Discourage the use of protocols such as HTTP, FTP, TELNET, RPC and prefer using secure protocols such as HTTPS, FTPS, SSH, etc.
3. **Isolate and Segment Networks** : Design your network in such a way that the sensitive systems are adequately segmented from rest of the network.
4. **Keylogging**

- Keylogging is an old technique where the attacker installs a hardware device or a malware on your system that captures all your keystrokes.

Definition : Keyloggers or simply keystroke loggers are malware programs that capture your keystrokes on the keyboard.

- The simple idea behind keylogging is that any user would definitely type sensitive information at some point in time. By identifying patterns in the key logged data, the attacker can search for sensitive information. Keyloggers are generally part of other virus or trojan malwares that secretly transmit logged key data to the attacker.

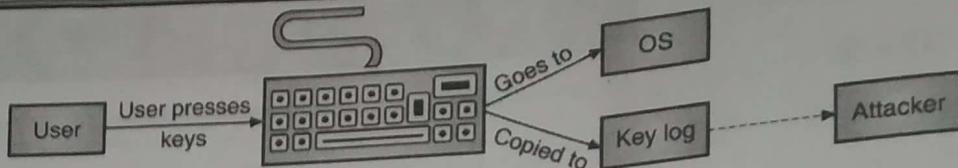
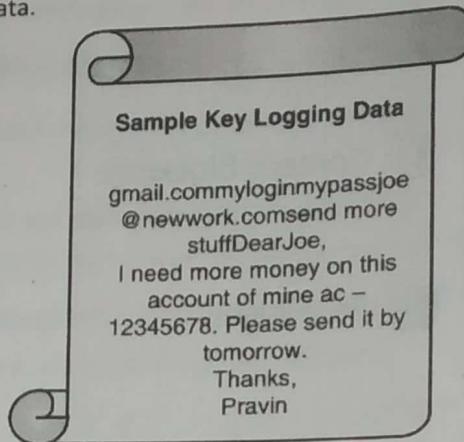


Fig. 5.5.9

- Here is a sample keylogging data.



- Can you identify some patterns and figure out some of my sensitive information? What If I told you that the data belongs to my activity of sending an email via my Gmail account to a friend? Can you figure out the sensitive information?
- Let me help you. Assume the following sequence of activities.
 1. I opened my favourite browser Mozilla and typed “gmail.com”.
 2. The Gmail login page appeared and then I typed my username “mylogin” and my password “mypass”.
 3. Then, I clicked on *compose* and typed the email address of my friend “joe@newwork.com”.
 4. Then, I typed my email subject “send more stuff”.
 5. Then, I composed my email and hit the *send* button.
- Does it sound simple but scary? That's precisely what keylogging is. All keys are captured as you press them. Some modern and advanced keyloggers also capture mouse clicks (x and y coordinates of the screen or pixel position information on the screen) along with screenshots.

Protection Mechanism

1. Regularly use anti-malware programs to scan your systems.
2. Set multi-factor authentication to avoid account hijack even if your password is compromised.
3. Use virtual keyboard specially when dealing with financial related logins.
4. Regularly check your installed program inventory to identify any potential malware.
5. Regularly check the services running on your system to identify any potential malware service.
6. Physically inspect your system wires and attachments to ensure that there are no unwanted hardware plugins.

5. Brute Force Attack

Definition : Bruce force attack is performed using tools that cycle through various combinations of characters until a successful combination of characters is found.

- These tools continuously send various character combinations in the hope of finding a successful combination. The time it takes to crack passwords this way is usually large.
- Some of the common tools to carry out the brute force attack are
 1. Brutus
 2. RainbowCrack
 3. Cain and Abel
 4. Wfuzz
 5. John the ripper
 6. Medusa
 7. Aircrack-ng

Protection Mechanism

1. Use lengthy and complex passwords. The more complex the password, the longer it takes to brute force it.
2. Introduce a time delay after a certain number of failed logins. For example, the system can lock the account after 3 failed attempts and requires administrator to unlock the account or wait for a period of 1-24 hours before automatically unlocking the account.
3. Send login notification. Whenever your account is attempted to log in, you could be notified via SMS or email. You could then take corrective actions if the login activity is not found to be legitimate.
4. Protect the password hash storage files from any unauthorised access or download. The attacks can be carried out on the files thus bypassing all forms of controls.

6. Dictionary Attack

Definition : Dictionary attack is a variation of brute force attack where instead of trying random character combinations, dictionary words and their variations are tried out for cracking the password.

- Dictionaries could be used from the user's natively spoken language or the multiple languages that a user may know. Apart from the regular dictionaries, there are other dictionaries which are collections from the hacker community.
- When a large user account database is stolen, such information is available with the hacker community that uses the information to form a listing of new passwords that people might be using.
- To give you a feel of how large a dictionary could be, take a look at the following snapshot.



The screenshot shows the homepage of CrackStation's Password Cracking Dictionary. At the top, there's a navigation bar with links for 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main title 'CrackStation's Password Cracking Dictionary' is prominently displayed. Below it, a message says 'I am releasing CrackStation's main password cracking dictionary (1,493,677,782 words, 15GB) for download.' A section titled 'What's in the list?' contains text about the list's origin, including wordlists, dictionaries, and password database leaks from various sources like Wikipedia and Project Gutenberg. It also mentions Project Gutenberg and eHarmony password database breaches. Another section discusses testing the list without download by giving SHA256 hashes to a free hash cracker or @PlzCrack on Twitter. A third section highlights the list's success in cracking LinkedIn and eHarmony password leaks.

- Imagine a text file of 15 GB!!! Impressive, isn't it?
- Dictionary attack might take lesser time than the actual brute force attack since not all combinations are tried. Also, if the user has not chosen a dictionary-based password, then the dictionary attack may not be able to crack it.

Protection Mechanism

1. Follow password selection guidelines and choose a complex and non-dictionary password.
2. Introduce a time delay after a certain number of failed logins. For example, the system can lock the account after 3 failed attempts and requires administrator to unlock the account or wait for a period of 1-24 hours before automatically unlocking the account.
3. Send login notification. Whenever your account is attempted to log in, you could be notified via SMS or email. You could then take corrective actions if the login activity is not found to be legitimate.
4. Protect the password hash storage files from any unauthorised access or download. The attacks can be carried out on the files thus bypassing all forms of controls.

7. Rainbow Tables

 **Definition :** Rainbow tables consist of passwords in the hash format.

- Rainbow tables are minor variations of dictionaries used in the dictionary attacks. Unlike dictionary attacks that use the pre-defined character combinations, rainbow tables contain pre-computed hash values for every possible character combination in those dictionaries.

(Copyright No. - 3673/2019-CO/L & 8811/2019-CO/L)

- That way, you need not waste system resources and time in computing the hash values (again and again) and then comparing with the hash value on the system (or the stolen user password hash storage file).
- Table 5.5.2 is a simplistic rainbow table.

Table 5.5.2 : A simple rainbow table

Character Combination	SHA-1 Hash
NewPassword	735b535bd8148743e2e19b08c7db8ea60142a0b3
MyPassword	daa1f31819ed4928fd00e986e6bda6dab6b177dc
Iamhappy	b0177566098815e0555830d7a68d2352614fe9bc
Apple@123	d88f1b3fb247e4ad3f6b821e4da902d1c91f0864

- Your problem is simplified. All you need to find then is any hash value in the rainbow table that could match with the system's hash value.
- When such a match is found, you can find the corresponding character combination from the rainbow table. This character combination is the cracked password.

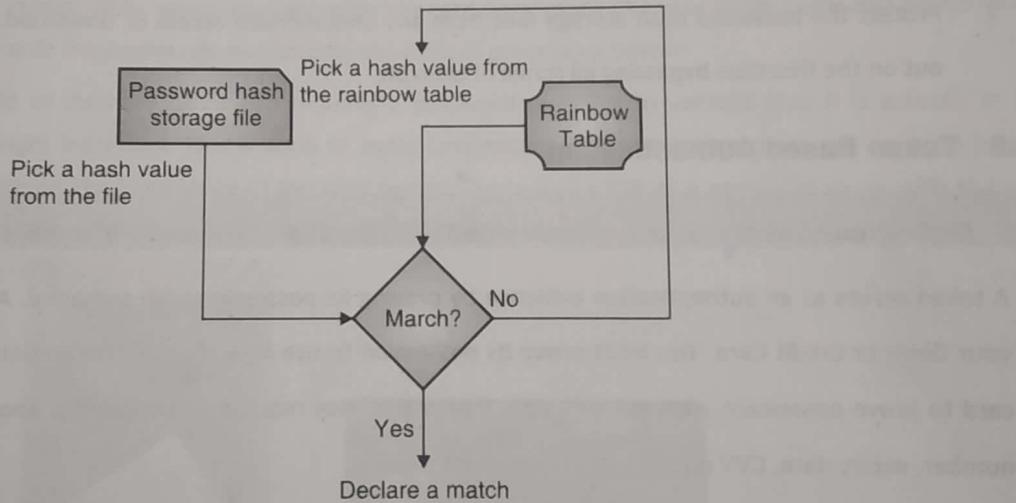


Fig. 5.5.10

- Rainbow tables are much faster when compared with the brute force or dictionary attacks. RainbowCrack is one of the tools that use rainbow tables to crack passwords.
- The rainbow tables are also huge in size as they contain several hash values for dictionary words.

Rainbow Tables							
LM Rainbow Tables							
Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
lm_ascii-32-05-123-481-7	ascii-32-05-123-4	1 to 7	7,565,858,447,479	99.9 %	27 GB 32 GB	Perfect Non-perfect	Perfect Non-perfect
NTLM Rainbow Tables							
Table ID	Charset	Plaintext Length	Key Space	Success Rate	Table Size	Files	Performance
ntlm_ascii-32-05#1-7	ascii-32-05	1 to 7	70,570,841,626,496	99.9 %	52 GB 64 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_ascii-32-05#1-8	ascii-32-05	1 to 8	6,704,780,854,517,120	99.8 %	460 GB 576 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_mixalpha-numeric#1-6	mixalpha-numeric	1 to 8	221,919,451,578,090	99.9 %	127 GB 160 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_mixalpha-numeric#1-9	mixalpha-numeric	1 to 9	13,759,005,897,841,842	99.8 %	690 GB 864 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_loweralpha-numeric#1-9	loweralpha-numeric	1 to 9	104,461,669,716,084	99.9 %	65 GB 80 GB	Perfect Non-perfect	Perfect Non-perfect
ntlm_loweralpha-numeric#1-10	loweralpha-numeric	1 to 10	3,780,820,109,779,080	99.8 %	318 GB 396 GB	Perfect Non-perfect	Perfect Non-perfect

Protection Mechanism

- Follow password selection guidelines and choose a complex and non-dictionary password.
- Protect the password hash storage files from any unauthorised access or download. The attacks can be carried out on the files thus bypassing all forms of controls.

5.5.9 Token Based Authentication

Definition : Token is a form of authentication that utilizes "Something You Have" type of authentication.

- A token serves as an authentication evidence by proving its possession with someone. A simple example of token is your Debit or Credit Card. You must prove its possession to use it. A physical transaction may require a swipe of the card to prove possession whereas an online transaction may require various details about the card such as the card number, expiry date, CVV number and card holder's name.
- There are various types of token devices used in different ways to provide authentication.

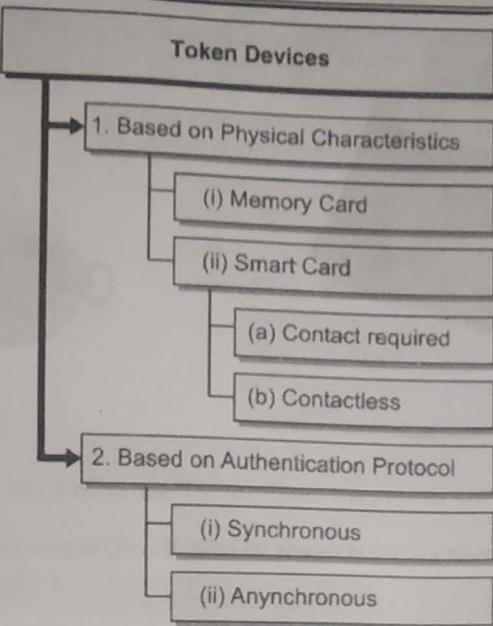


Fig. 5.5.11

A. Memory Card

 **Definition :** Memory cards physically contain the required authentication information.

- It usually has a magnetic stripe (or a chip) and the authentication information is contained in this stripe (or chip). You require a card reader using which you can swipe the card (very much like your Debit Card) and authenticate yourself. Memory cards themselves do not possess any form of processing power.
- Sometimes, the use of memory cards also requires a password or a PIN to validate that it is actually in the possession of the right individual. This is done to avoid circumstances where stolen cards can be used just by their possession without the knowledge of the card owner. The use of a PIN or a password along with the card possession, makes authentication as two-factor authentication.



B. Smart Card

 **Definition :** Smart card has processing capacity that can be used to provide authentication information.

- Unlike memory cards, smart cards have processing capacity and may also have display and buttons. It may or may not require a smart card reader.



- There are two types of smart cards.
 1. **Contact required** : The smart card needs to be inserted into the smart card reader for authentication.
 2. **Contactless** : The smart card just needs to be in the close proximity of the reading device.

C. Synchronous Tokens

Definition : A synchronous token device synchronizes (works tightly coupled) with the authentication service for providing authentication information.

- The synchronisation could be based on time or a counter. RSA SecurID is an example of time-based synchronous token.



- If the synchronization is time-based, the token device and the authentication service must hold the same time within their internal clocks.
- The time value on the token device and a secret key (pre-loaded in the token device and the authentication server also has a copy of it) are used to create the one-time password, which is displayed to the user.
- The user enters this value and a user ID into the computer, which then passes them to the server running the authentication service.
- The authentication service compares it to the value it expected. If the two match, the user is authenticated and allowed to use the computer and resources.
- If the token device and authentication service use counter-based synchronization, the user will need to initiate the creation of the one-time password by pushing a button on the token device.
- This causes the token device and the authentication service to advance to the next authentication value. The user enters this resulting value along with a user ID to be authenticated.

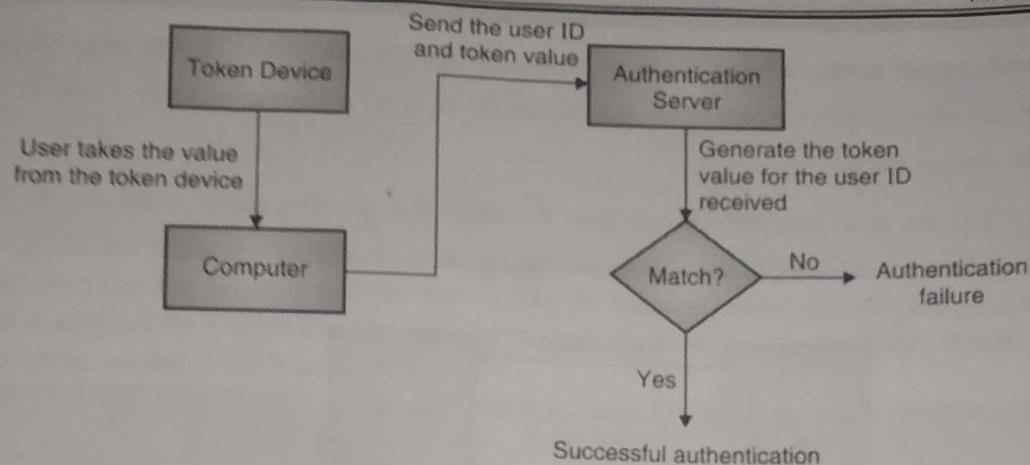


Fig. 5.5.12

D. Asynchronous Tokens

Definition : Asynchronous token device uses challenge-response mechanism for providing authentication information.

- Asynchronous token is not time dependent. It uses a challenge-response mechanism (very much like handshake protocols) for providing authentication information.
- The authentication server sends the user a challenge which is usually a random value. The user needs to enter this value into the token device. The token device encrypts the value entered and returns a value that the user uses as a one-time password. The user sends this value along with the user ID to the authentication server. If the authentication server can decrypt the value and gets the same challenge value that it sent earlier, the user is authenticated.

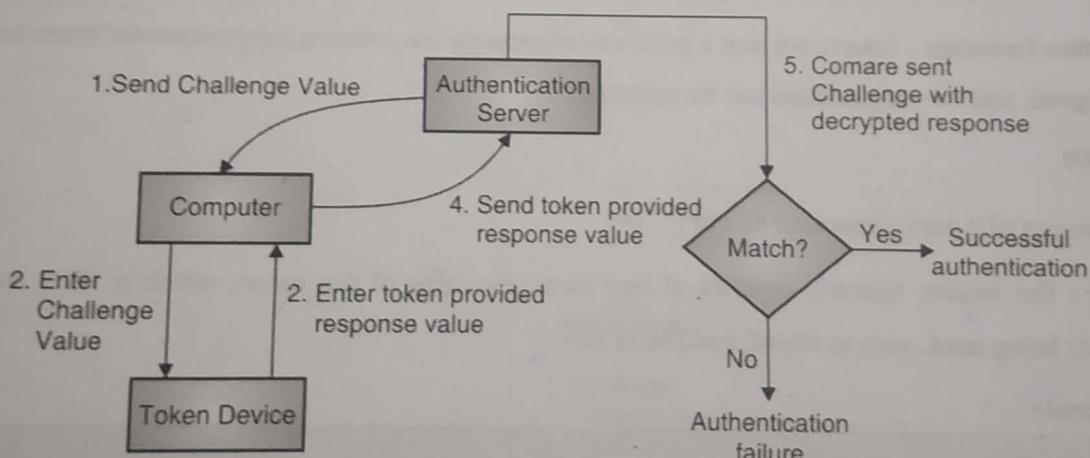


Fig. 5.5.13

E. Software Tokens

- Similar to physical tokens there also exist software-based tokens. Software tokens are used for security claims (authorisation) between two communicating parties. One such implementation, based on RFC 7519, is JSON Web Token or JWT (pronounced Jot).

Definition : JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties.

- The general concept behind a token-based authentication system is to allow a user to enter her user name and password in order to obtain a web token that allows her to fetch a specific resource - without using her user name and password again.
- Once her token has been obtained, she can offer the token that provides access to the specific resources for a time period. Tokens come with an expiry time and need to be refreshed periodically.

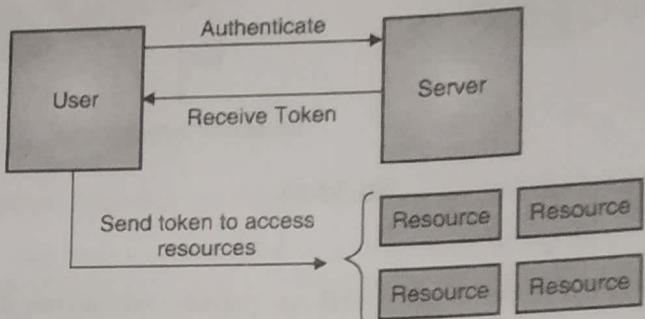


Fig. 5.5.14

Usage of software tokens

Two common scenarios where software tokens are used are

1. **Authorisation** : Once the user is logged in, each subsequent request will include the token, allowing the user to access resources that are permitted with that token. The user does not require re-authentication several times to continue accessing the permitted resources.
2. **Information Exchange** : Tokens are also a good way of securely transmitting information between parties. Tokens can be signed, and non-repudiation can be enforced.

F. JWT Structure

- A JWT consists of 3 parts separated by dot (".") –

 1. **Header** : The header typically consists of two parts: the type of the token, which is JWT, and the signing algorithm being used, such as HMAC SHA256 or RSA.

For example :

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

- Here algorithm is HMAC SHA 256 written HS256 in short. Token type is JWT.
- 2. **Payload** : The second part of the token is the payload, which contains the claims. Claims are statements about an entity (typically, the user) and additional data.

For example :

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "admin": true
}
```

3. **Signature** : To create the signature part you have to take the encoded header, the encoded payload, a secret, the algorithm specified in the header, and sign that. For example if you want to use the HMAC SHA256 algorithm, the signature will be created in the following way:

HMACSHA256(

```
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
secret)
```

- The signature is used to verify the message wasn't changed along the way, and, in the case of tokens signed with a private key, it can also verify that the sender of the JWT is who it says it is.
- All the 3 parts are Base64Url encoded. The following example shows a JWT that has the previous header and payload encoded, and it is signed with a secret.

The screenshot shows a JWT token being processed by jwt.io. On the left, under 'Encoded', the token is shown as a long string of characters: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.2pISfsEVqnkduM2tWciUIhDjNXXdQwaUQJcnfj-ZhyY. The right side, under 'Decoded', shows the token split into Header and Payload. The Header contains the algorithm (HS256) and type (JWT). The Payload contains the subject (sub), name, and an expiration timestamp (iat). Below the token, there's a section for verifying the signature using the provided secret and base64 encoding. A large green checkmark at the bottom indicates 'Signature Verified'.

ALGORITHM HS256

Encoded PASTE A TOKEN HERE

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.2pISfsEVqnkduM2tWciUIhDjNXXdQwaUQJcnfj-ZhyY

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYOUT: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239822
}
```

VERIFY SIGNATURE

HMACSHA256(
base64UrlEncode(header) + "." +
base64UrlEncode(payload),
fbwiuehfufwbfuiwbfi
) secret base64 encoded

SHARE JWT

Signature Verified

Note : You can go to <https://jwt.io/> and try out JWT.

5.5.10 Biometric Based Authentication

- The biometric-based authentication relies upon "Someone You Are" and "Something You Do". "Something You Are" utilizes physical characteristics of your body whereas "Something You Do" utilizes your behavioural characteristics.
- Biometric is the most expensive way of authentication. It requires specialized readers, processing, storage and comes with errors.

5.5.10(A) Components of Biometric Systems

Any typical biometric system comprises of the following components.

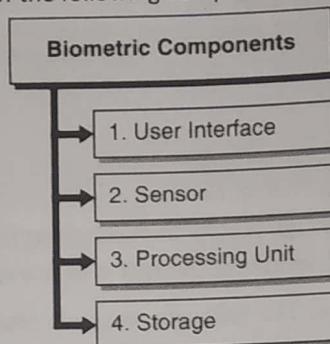


Fig. 5.5.15

1. User Interface

This is the equipment (or the part of the overall biometric system) which serves as the input and output device. The user interacts with it. It could be the glass where you place your fingers for scanning or could be a microphone where you give your voice print.

2. Sensor

Sensor is the most critical part of the biometric system. It extracts the authentication related information from the provided input and passes it to the processing unit. Sensor should be able to adequately read the information and should be error free as much as possible. If the sensor has problems, it could either mean accepting unauthorized individuals or rejecting authorized individuals. Both conditions are dangerous.

3. Processing Unit

The processing unit evaluates the captured information and performs any processing required for overall working of the biometric system.

4. Storage

A storage mechanism (or unit) is required to keep the collected biometric samples from the individuals for matching them as and when needed for authentication purpose.

5.5.10(B) Operating Biometric Systems

Like passwords, biometric systems also have two phases.

1. Sign up (or enrolment)
2. Verification

Enrolment

- The enrolment process involves collecting the biometric sample from the individual. Remember your Aadhar card enrolment? Your physical presence is required. You provide the biometric sample (one or multiple times) based on the type of the biometric device.
- If it is a fingerprint scanner, you provide your fingerprints. If it is a retina scanner, you look through an eye scanner. Once your sample is collected, the information that can be used for authentication is extracted from it. The information is digitized in the binary format and is stored for future use.

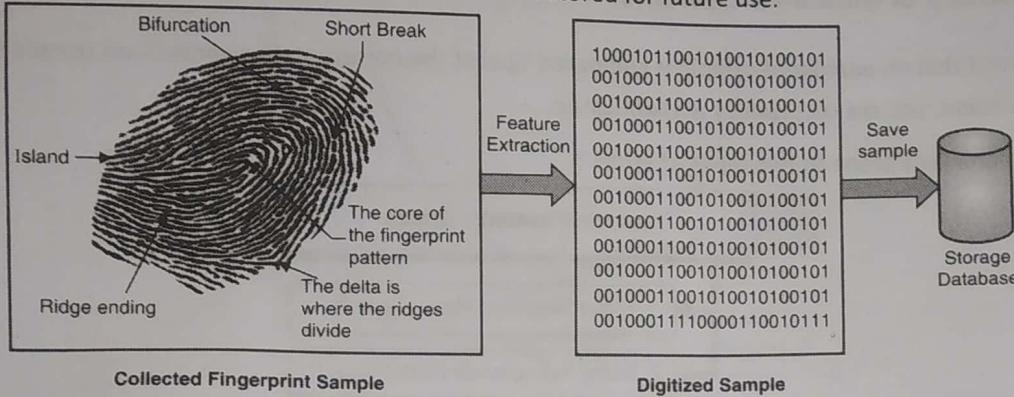


Fig. 5.5.16

- You can understand the enrolment process using a simplistic schematic diagram as shown in Fig. 5.5.17.

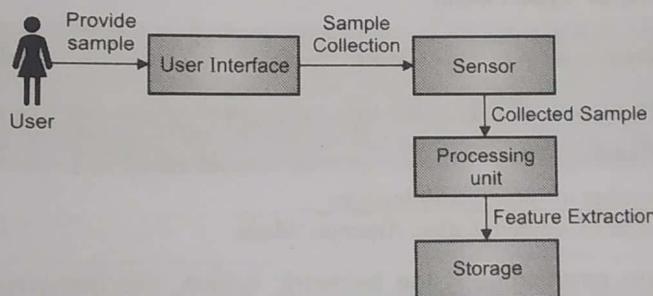


Fig. 5.5.17

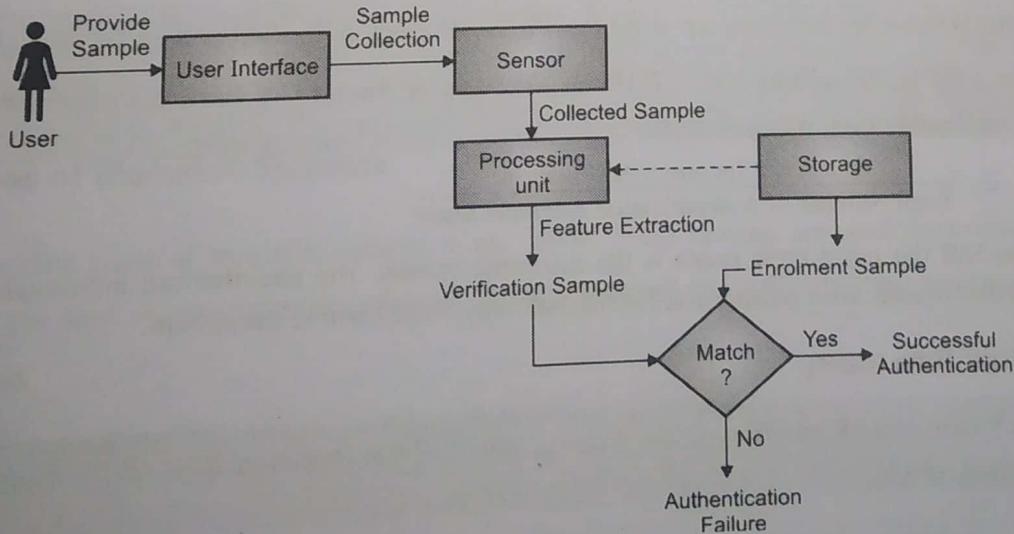
2. Verification

Fig. 5.5.18

- The verification process is quite straightforward. Your physical presence is again required. You offer the same type of sample that you provided during the enrolment process. For example, if you enrolled with fingerprints, you would need to provide fingerprints again for verifying.
- Your provided verification sample is compared against the enrolment sample based on your identity. Once the two samples match, you are successfully verified. If the samples do not match, the authentication is rejected. This might be due to some error. In that case, you can retry providing the sample again.

5.5.10(C) Accuracy of Biometric Systems

- You understand that an enrolment sample is compared against the corresponding verification sample to find a match. If a match is found, you are successfully authenticated.
- Biometric systems are prone to two types of errors :

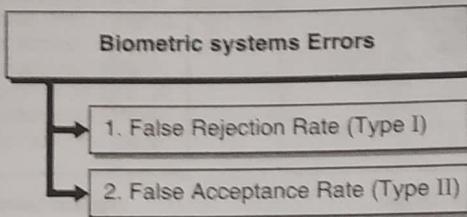


Fig. 5.5.19

1. False Rejection Rate (FRR) or Type I error

- Definition :** When a biometric system rejects an authorised individual it is called Type I error.
- Definition :** False Rejection Rate (FRR) is the ratio of number of incorrect rejections to the total number of authentication attempts made.

$$FRR = \frac{\text{Number of Incorrect Rejections}}{\text{Total Number of Authentication Attempts Made}}$$

The higher the FRR the more error prone is the biometric system. The authorised individuals would likely get frustrated from repeated attempts required to pass authentication.

2. False Acceptance Rate (FAR) or Type II Error

- Definition :** When a biometric system accepts an unauthorised individual it is called Type II error.
- Definition :** False Acceptance Rate (FAR) is the ratio of number of incorrect acceptances to the total number of authentication attempts made.

$$FAR = \frac{\text{Number of Incorrect Acceptances}}{\text{Total Number of Authentication Attempts Made}}$$

The higher the FAR the more error prone is the biometric system. The unauthorised individuals would likely get successfully authenticated. Such unauthorised individuals may cause harm to the system.

3. Crossover Error Rate (CER)

- Definition :** Crossover Error Rate is the point at which False Rejection Rate (FRR) is equal to the False Acceptance Rate (FAR).

This means that the biometric system is not more likely to produce one type of error than the other type. If the system rejects too many authorised individuals the FRR would be high. Similarly, if the system accepts too many unauthorised individuals the FAR would be high. CER is also called as Equal Error Rate (EER).

When comparing various biometric systems, choose the one with lower CER value. The lower the CER value the more accurate the biometric system is. For example, a biometric system having CER value 3 would be more accurate than the biometric system having CER value of 5.

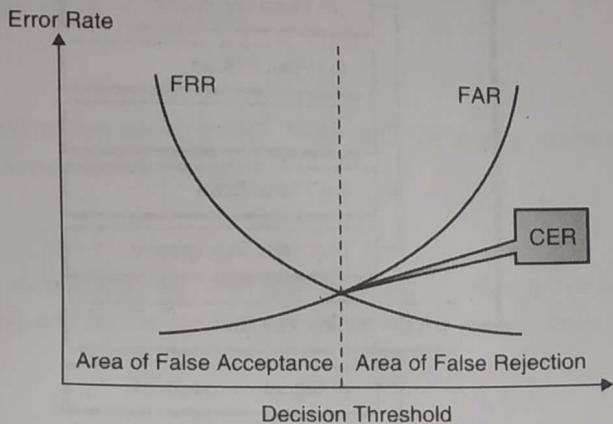


Fig. 5.5.20

Ex. 5.5.1 : A biometric system rejects 2 authorised attempts out of 10. Calculate its FRR.

Soln. :

$$\text{FRR} = \frac{\text{Number of Incorrect Rejections}}{\text{Total Number of Authentication Attempts Made}}$$

$$\text{Hence, FRR} = 2/10 = 0.2$$

Ex. 5.5.2 : A biometric system accepts 4 unauthorised attempts out of 10. Calculate its FAR.

Soln. :

$$\text{FAR} = \frac{\text{Number of Incorrect Acceptances}}{\text{Total Number of Authentication Attempts Made}}$$

$$\text{Hence, FAR} = 4/10 = 0.4$$

5.5.10(D) Types of Biometric Systems

- There are several types of biometric systems in use today. These systems are used depending upon the type of application, the level of authentication required, processing speed and authentication accuracy (Type I errors and Type II errors).
- Let us learn about some of the most commonly used biometric systems.

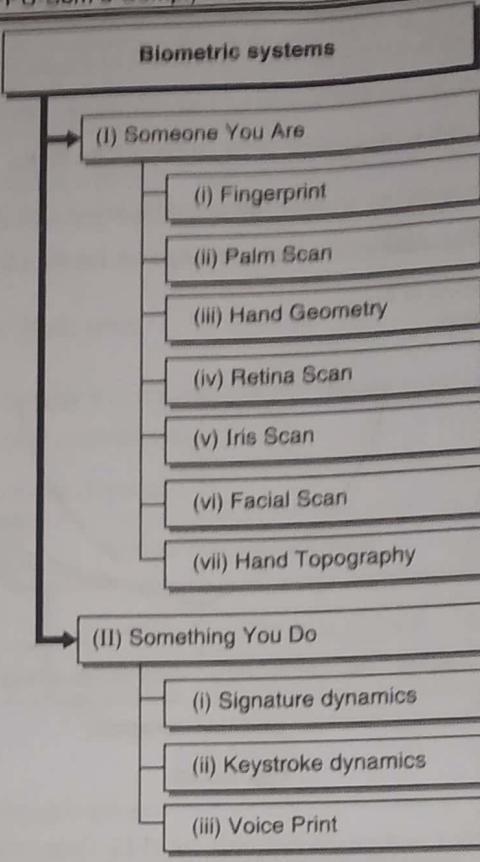


Fig. 5.5.21

1. Fingerprint

Fingerprint is one of the most commonly used type of biometric system. Your fingerprint is made up of several curves and endpoints. These when combined together are unique enough to identify you.

2. Palm Scan

You would have seen this in several movies. Your palm contains several curves, lines, endpoints, folds and textures that can uniquely identify you. Unlike fingerprints, you need to place your entire palm on the biometric sensor to enroll and verify yourself.

3. Hand Geometry

Your hand holds several key attributes such as shape, length, width, size etc. These attributes could fulfil biometric requirements to provide authentication information.

4. Retina Scan

Retina scan involves reading the blood-vessel pattern of retina on the backside of the eyeball. This pattern is unique enough to identify you. You are required to look into an eye scanner (fitted with a high-resolution camera). The scanner captures the pattern and stores it for authentication.

5. Iris Scan

The iris is the coloured portion of the eye that surrounds the pupil. The iris has unique patterns, rifts, colours, rings, coronas, and furrows. When you look into an eye scanner, these characteristics are captured and stored for authentication. Iris scan is the most accurate form of biometric system.

6. Facial Scan

Your face can be digitally identified as well. It has got several key features such as nose ridges, eye widths, chin shape, forehead size, bone structures, etc. These features are extracted during a facial scan and stored for authentication.

7. Hand Topography

Hand topography captures overall hand shape and structure. The peaks and valleys in your hand provide biometric traits that can be used for authentication. The entire hand is placed on a scanner and there are several cameras that capture the hand information from various angles.

8. Signature Dynamics

You sign at a particular speed making similar strokes each time. The signing process generates electrical signals that can be captured to provide biometric authentication.

9. Keystroke Dynamics

Keystroke dynamics capture electrical signals when you type using a keyboard. You type at a particular speed applying a specific key pressure, timing and rhythm for each key that you press. These dynamics can be captured and used for authentication.

10. Voice Print

Aren't you using Alexa, Siri or Ok Google yet? How does that work? Basically, you train the device to recognize your voice pattern. Your voice pattern has specific pitch, tone, amplitude and frequency that can be used to create a voice print (similar to fingerprint). These attributes are stored and when you are required to authenticate you are asked to speak a set of words or sentences to capture your voice print and compare it with the previously stored voice print information.

Comparison of Biometric Systems

Sr. No.	Biometric System	Processing Speed	Accuracy	Ease of Enrolment
1.	Fingerprint	High	High	High
2.	Palm Scan	Medium	High	Medium
3.	Hand Geometry	Low	Medium	Low
4.	Retina Scan	Medium	High	High
5.	Iris Scan	Medium	High	High
6.	Facial Scan	Medium	Low	Medium
7.	Hand Topography	Low	Low	Low
8.	Signature dynamics	Medium	Medium	Medium
9.	Keystroke dynamics	Medium	Medium	Medium
10.	Voice Print	Medium	Medium	Medium



Review Questions

Here are a few review questions to help you gauge your understanding of this chapter. Try to attempt these questions and ensure that you can recall the points mentioned in the chapter.

Firewall

- Q. 1** What are the components of a firewall rule? [4 Marks]
- Q. 2** Classify firewalls based on the OSI Layer. [4 Marks]
- Q. 3** Classify firewalls based on Form Factor. [4 Marks]
- Q. 4** Classify firewalls based on the type of Inspection. [4 Marks]
- Q. 5** Classify firewalls based on architecture. [8 Marks]
- Q. 6** What are some of the major challenges in managing and deploying firewalls? [6 Marks]

Computer Intrusions and Intrusion detection systems (IDS)

- Q. 7** Your boss is asking you why we need IDS if we already have firewalls. He is not convinced that IDS is required. How do you convince him? [4 Marks]
- Q. 8** Explain the types of IDS. [6 Marks]
- Q. 9** List the limitations and challenges of IDS. [4 Marks]

Access Control

- Q. 10** Describe how DAC systems use access control matrix to determine access policies. [6 Marks]
- Q. 11** With a flowchart, explain how access decisions are taken on a MAC system? List advantages and disadvantages of MAC-based systems. [6 Marks]
- Q. 12** Your supervisor is proposing that we should move to RBAC in the organisation. What is RBAC and what advantages he has in mind by proposing such a move? [6 Marks]
- Q. 13** With a block diagram, describe how access decision are taken in ABAC-based systems. [6 Marks]
- Q. 14** List advantages and disadvantages of an ABAC-based system. [7 Marks]
- Q. 15** With a block diagram, explain any two rules of the Bell-LaPadula (BLP) Model. [4 Marks]

Trusted Systems

- Q. 16** Write a short note on Discretionary Security Property of the Bell-LaPadula (BLP) Model. [6 Marks]
- Q. 17** What is the focus of the Bell-LaPadula (BLP) Model and how do Simple Security and Star Property rule help? [6 Marks]
- Q. 18** The Bell-LaPadula model suggests "No-read up" but reading down is allowed. The Biba model suggests "No-read down" but reading up is allowed. Are these two rules conflicting each other? [6 Marks]
- Q. 19** The Bell-LaPadula model suggests "No-write down" but writing up is allowed. The Biba model suggests "No-write up" but writing down is allowed. Are these two rules conflicting each other? [6 Marks]

- Q. 20 With a block diagram, explain Star Integrity Property Rule.
- Q. 21 Give a practical example of the application of Biba model.
- Q. 22 Write a short note on the Invocation Property Rule.

[4 Marks]

[6 Marks]

[4 Marks]

Authentication Methods

- Q. 23 What is "Something You Know" type of authentication? Give examples.
- Q. 24 List the advantages and disadvantages of "Something You Have".
- Q. 25 Define the term biometric. Give examples of static and dynamic biometrics.
- Q. 26 Write a short note on location-based authentication.
- Q. 27 Alex is proposing that we should at least use two-factor authentication these days to secure our accounts. John says "Come on Alex, don't you know that we already require a PIN followed by a strong password to authenticate on our application. We are good here". Alex says, no, that is not what I mean. What could Alex mean here?
- Q. 28 You should choose simple and easy to remember passwords so that you don't have hard time recalling them. For example, your name or your birth date can be a good password. Simple and easy to remember. Isn't it?
- Q. 29 Your supervisor is worried that not everyone in the organisation is using strong passwords for securing their accounts. You suggest her that we should enforce password quality criteria in the organisation. Confused, she asks you, what does password quality criteria mean and what are some of the suggested quality criteria we should adopt in the organisation?
- Q. 30 Describe how passwords are typically stored and verified on a system.
- Q. 31 Explain any three attacks on Password Based Authentication.
- Q. 32 Write a short note on Synchronous tokens.
- Q. 33 Write a short note on Asynchronous tokens.
- Q. 34 What are the components of a biometric system?
- Q. 35 Explain the enrolment process in a biometric system with a block diagram.
- Q. 36 Explain the verification process in a biometric system with a block diagram.
- Q. 37 Explain FRR, FAR, and CER with respect to a biometric system. How do you choose these parameters?
- Q. 38 Compare any 6 biometric methods of your choice on the basis of
- Processing Speed
 - Accuracy and
 - Ease of Enrolment

[4 Marks]

[6 Marks]

[4 Marks]

[4 Marks]

ure our accounts. John says
sword to authenticate on our
mean here?

[4 Marks]

hard time recalling them. For
member. Isn't it?

[4 Marks]

passwords for securing their
organisation. Confused, she asks
quality criteria we should adopt

[6 Marks]

[8 Marks]

[6 Marks]

[4 Marks]

[4 Marks]

[6 Marks]

[6 Marks]

[6 Marks]

use a biometric system based on

[6 Marks]

[8 Marks]

