SYSTEM SECURITY

EXTC – BE – DATA COMPRESSION AND CRYPTOGRAPHY

Ms. Vandana Sawant

Assistant Professor

Dept. of Electronics & Telecommunication Engineering,

SIES Graduate School of Technology

QUESTIONS

- Write short note on intrusion detection system
- What is intrusion detection system discuss the different techniques of implementing it ?
- Explain intrusion detection certificate
- Write a short note on secure electronic payment system
- Write short note on ethical hacking
- Write short note on digital immune system
- Write classification of firewall
- Write a need of firewall
- Explain operating process of biometric system
- Explain types of biometric system

OBJECTIVES OF LECTURE

- Students should be able to
  - Know about SYSTEM SECURITY

INTRUSION DETECTION SYSTEM

- An intrusion detection system is defined as a software that helps to find out if a system is breached
- In a nutshell IDS can help you to find out if there were undesired actions or attacks carried out on your information system
- 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

INTRUSION DETECTION SYSTEM

- Need for IDS :
- Defense in depth :
- Defense in depth of security designing ensure that even if one of the controls is to fail the overall security of the system would still be possibly healthy.
- IDS fulfills this need to bring an added layer of protection where any breaches or their possibilities can be identified quickly
- Automate intrusion detection:
- Corrective actions:

INTRUSION DETECTION SYSTEM

- Types of IDS:
- Based what it monitor :
- Network based IDS (NIDS):
- Host based IDS(HIDS):
- Based on how it monitors:
- Signature based:
- Anomaly based:

INTRUSION DETECTION SYSTEM

- Limitations and challenges of IDS:
- Does not prevent attacks:
- High rate of false alerts(noise):
- Complex systems:
- Bypassing IDS:

SECURE ELECTRONIC TRANSACTION

- Secure electronic transaction is a security technology proposed by VISA and MASTER CARD for secure credit card transaction (HTTPS)
- Issuer :
- User:
- Merchant:
- Acquirer:
- Payment gateway:

SECURE ELECTRONIC TRANSACTION

- User browses the merchant's website and decides the order
- She sends the order and payments information
- Merchant forwards the card information to its bank via the payment gateways
- The merchant's bank sends the credit card information to the issuer via the payment gateway
- Issuer verifies the credit card information and sends the authentication to the merchant's bank
- Merchant's bank sent authentication to merchant notifying that the payment is cleared
- Merchant completes the order and sends confirmation to the costumer

Ethical hacking

- Almost all organization are increasing their digital presence .it is hard to find any meaningful business without a website or an app and not using digital equipment within the organization to carry out various activities
- Attackers are continuously looking for easy target that they can exploit . How should organization protect themselves?
- You can say that purchase every security tool n the market have 10000 security professionals continuously watching digital systems and lock down everything.
- But, can you really do this? Will all organization have enough budget, skill, and resources to invest in security?
- Remember that business exit to make money and not lock down systems. but, at the same time it is important to ensure that such systems are not under attack.

Ethical hacking

- Definition:
- Ethical hacking involves carrying out attacks on systems in a non-destructive way to identify vulnerabilities.
- It is generally called penetration testing . It is one of the most effective methods of identifying the gaps in security and fixing those gaps before attackers gaps before attackers an discover them.
- The goal of penetration testing (or shortly called as Pentest) is to identify and fix the vulnerabilities before any threat can exploit those vulnerabilities.
- It involves thinking like n attackers and conducting test to find out vulnerabilities in system.
- These test are carried out by system experts who are deemed to be as skilled as the attackers.
- They are part of a team which is usually called as Red Team.

Ethical hacking

- Definition:
- In the industry the term ‘Red Team’ is generally used for any team that focuses on identifying improvement opportunities in the organization.
- Conducting penetration testing involves the following high-level steps.

Ethical hacking

- Create a plan :
- In this step, you first seek management approval. Getting approval is crucial to ensure that your tests are not consider unwanted and unexpected and you are not charged with any liabilities for damages, if and when occurred .once the approval is in place, you define a scope for the test .
- The scope should include:
- (a) symbol to be tested
- (b) specific dates and time
- (c) total time duration for which tests would be performed.
- (d)any business risk involved.
- (e)deliverable to be produced as part of testing
- (f)should you test with security controls turned off or on.

Ethical hacking

- Select tools:
- Conduct penetration tests:
- Evaluate the findings:
- Fix and findings:

Ethical hacking

- Definition:
- A bug bounty programme is an open offer from a company for anyone in the world from anywhere to conduct non-destructive penetration testing on its systems (websites, portals, application, etc.) and report the findings securely to it for appropriate fixing and handling of those findings.

Ethical hacking

- The reporter is awarded and paid in proportion of the impact that the reported finding could have on the system and the company's business.
- The bug bounty programme leverages (get access to) worldwide talent pool of experts who can help the company to prevent cyberattacks . In return the recognition and compensation for their work from the company.
- You can read about Googl's bug bounty programme on
- htpp://www.google.com/about/appsecurity/reward-program/.

Digital immune system(DIS)

- With an exponential rise in the number of viruses and worms it is difficult to keep the system protected at all time using the traditional and anti -malware technology. There might be a significant delay between the discovery of a new malware and it reaching to anti-malware vendor for analysis.
- Vendor might take some more time to find a solution and update the malware detection signature.
- The user must download and update the new malware signature before the new malware detection and handling could be possible.

Digital immune system(DIS)

- The goal of digital immune system (DIS) is to reduce the cycle time between when a malware is first found and when a cure is deployed to all vulnerable systems
- DIS automates the several manual tasks involved in the submission , analysis, and distribution processes of malware.

Digital immune system(DIS)

- Characteristics of Digital Immune Systems(DIS):
- Following are the typical characteristics of Digital Immune System(DIS):
- 1.It helps to detect high percentage of new or unknown malware
- It is easy to scale to many systems.
- 1. it makes it easy to submit new malware samples to the anti-malware vendor.
- 2.it make it easy to distribute and update new malware signatures on the anti-malware software.
- 3.it reduces the time spent between discovery analysis and fix.
- 4.it removes various manual tasks and provide an opportunity for automation.

Digital immune system(DIS)

- How does digital immune system(DIS)work?
- DIS involves the following 4 steps:
- 1.new malware is detected:
- 2.sample sent to DIS:
- 3.DIS processes and find fix:
- 4.fix is distributed:

Firewalls

- Definition:
- Firewalls are network security systems that protect the computing resources on a trusted network from unauthorized access.
- component of a firewall rule:
- Typically, a firewall rule consists of the following parameter
- 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.]
- 8various optional parameters such as Rule Name, Evaluation, Order,etc.

Firewalls

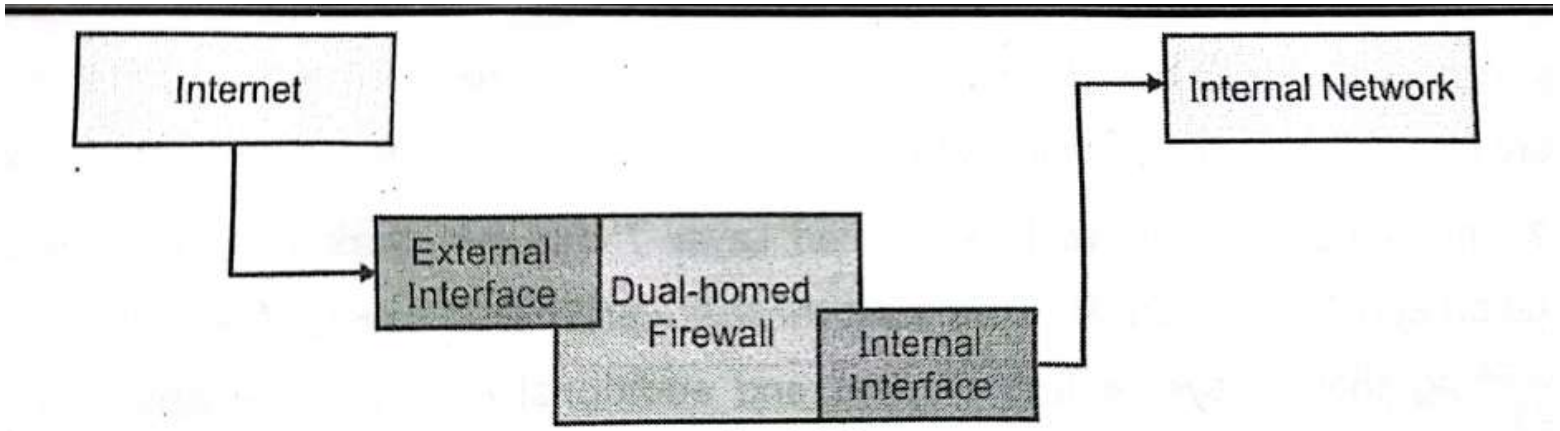
- Classification of firewalls:
- Based on OSI Layer:
- 1.Layer 2 Firewall: works at data link layer these firewall require MAC,VLAN or device hardware level information. It does not depend on IP
- 2.Layer 3 Firewall: these works at the network layer. Filter traffic based on source/destination IP, port and protocol. Also called as stateless firewall or first-generation firewall.
- 3.Layer 4 Firewall: works at transport layer do everything as that layer-3 and additionally track the active network connection and allow/deny traffic based on state of connection. these are also called as stateful firewalls or second-generation firewalls.
- 4.Layer 7 Firewall: can work at 3 layers –session, presentation and application. It does everything that a layer 4 does and additionally include the ability to intelligently inspect the content of the network packets.it is most advance type of firewall in use today. also called third generation firewall.

Firewalls

- Based on form factors: form factor or the footprint is the way the firewall is actually package and deployed
- 1. Software Firewall: software programmed and operating system to run them. can work at any of the OSI Layer
- 2.Hardware Firewall: may have better performance and they come packaged in a ready to use hardware device. You need to configure it as per your security requirement
- Based on the type of inspection:
- 1.Stateful Firewall: keep track of the state of connection apart from the defined firewall rules. These precisely understand various handshake protocol and can effectively top attacks that try to manipulate connection establishment or maintenance process
- 2.Stateless Firewall: typically work at layer 3 and take decision based on the defined rule parameters such as IP,Port and protocol.

Firewalls

- Based on architecture: based on deployment possibilities like one deployment type over the another
- 1.Dual-homed Firewalls: has two interfaces one facing the external networks and the other facing the internal network. It receives external packets at its one of the interface, evaluates firewall rules and passes on the traffic to the designated internal resources via the second interface



Firewalls

- 2.Screened Host: all internet traffic goes through the firewall no matter what . the internet router device first screen all the packets that are relevant to the network and then passes it to the screen host firewall for further inspection and applying rules

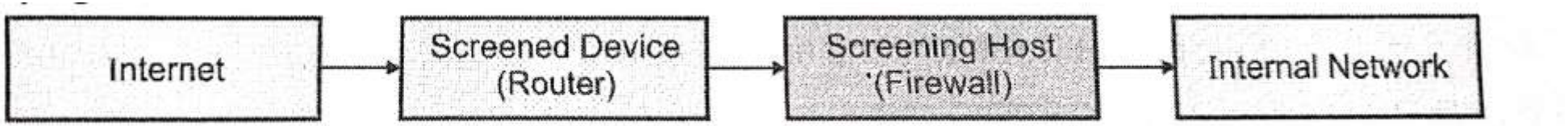


Fig. 6.8.3

Firewalls

- 3.Screened Subnet: two firewall are used.one just after the external network and the one just before the internal network. any network that lies between the two firewall is called a demilitarized zone(DMZ). You place your public facing server such as web servers, email servers etc. in DMZ . And 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.

Firewalls

- 3.Screened Subnet:

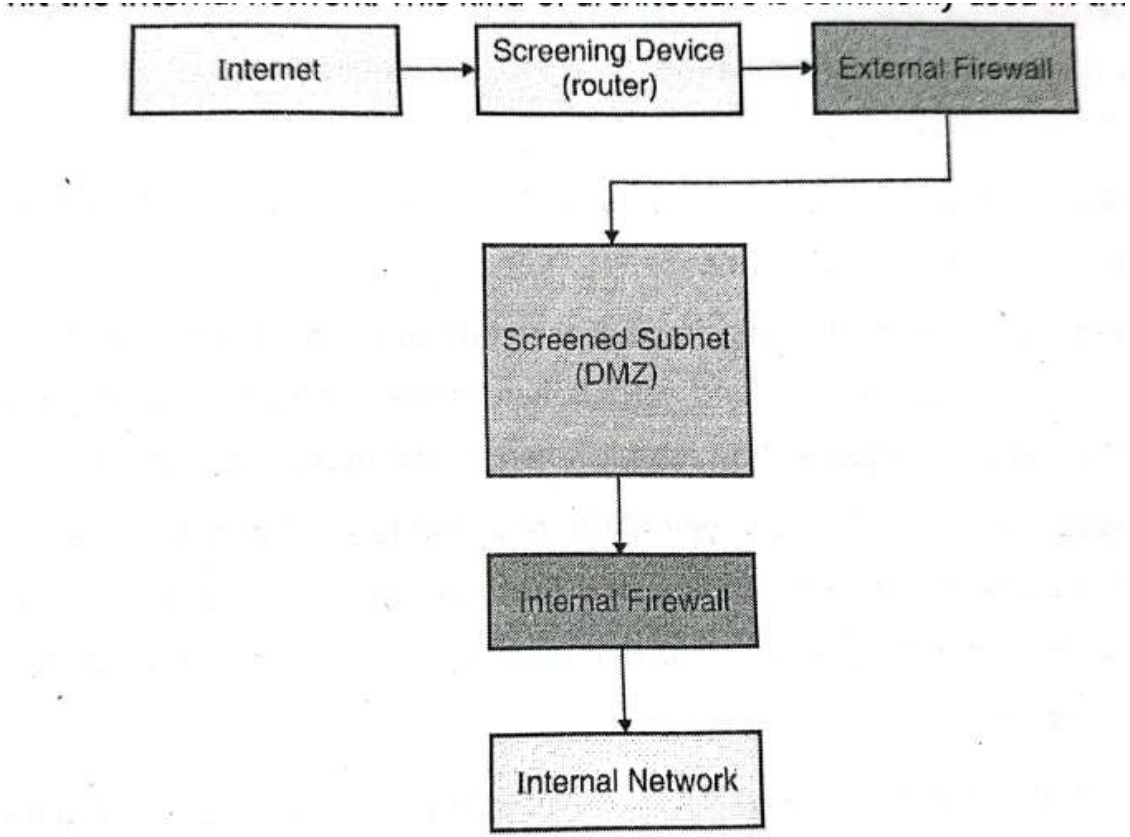


Fig. 6.8.4

Firewalls

- 4.Proxy: proxy firewall stands between the trusted and the untrusted networks and takes allow or denied decision after careful inspection of what is being passe along . Like a regular proxy, it breaks the connection between the sources and the destination. After examining the traffic, itself establishes a connection with the destination and passes the intended traffic to the destination, as if the packets were originating from it.

Firewalls

- 4.Proxy:

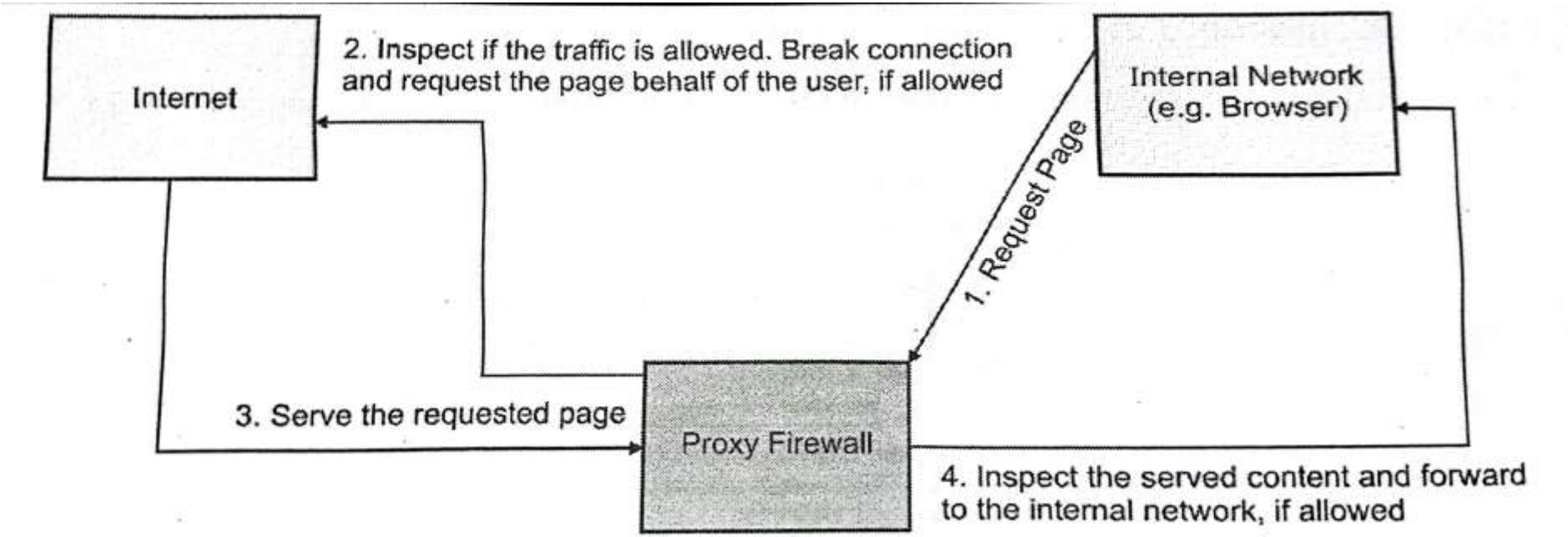


Fig. 6.8.5

Firewalls

- Challenges in managing and deploying firewalls:
- Performance: since the traffic needs to pass through the firewalls , there is a little performance degradation of the network
- 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 rule frequently .
- Costs : modern firewall that provide content and protocol level inspection may be cost prohibitive for small or medium size organization
- Insider attacks: firewall are usually designed and deployed to protect a trusted network from and untrusted networks. But if there were other vulnerabilities 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

Firewalls

- 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

Biometric based authentication

- Biometric based authentication relies upon someone you are and something you do utilizes physical characteristics of your body and your behavior characteristics. It is the most expensive way of authentication

Biometric based authentication

- Components of biometric system:
- User interface: input output devices it could the glass where you place your fingers or could microphone where you give voice print.
- Sensor :extracts the authentication related information. It should able to adequately read the information and should be error free
- If the sensor has a problem, it could either mean accepting unauthorized individuals or rejecting authorized individual

Biometric based authentication

- Processing unit: evaluates the captured information and performs any processing required.
- Storage: required to keep the collected sample from the individuals for matching them as and when needed

Biometric based authentication

- Operating biometric system:
- Enrollment : it is a process involves collecting the biometric sample from individual
- Your physical presence is required to provide sample
- If it is fingerprint scanner, you provide your fingerprints
- If it is 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

Biometric based authentication

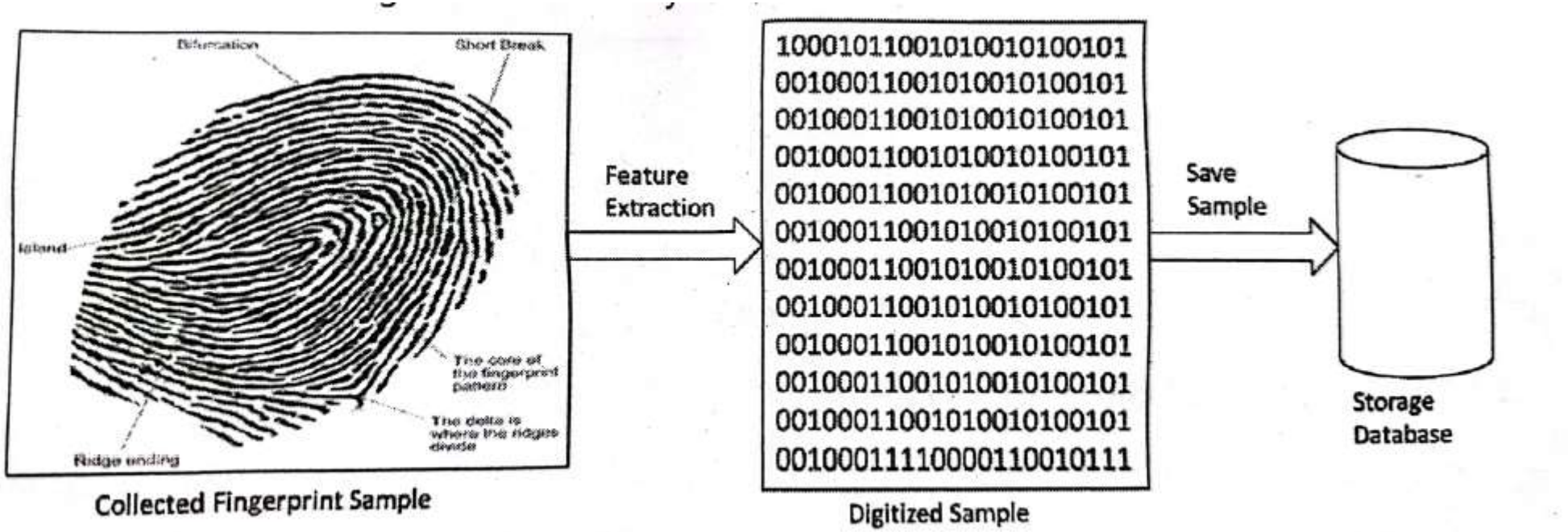


Fig. 6.9.2

Biometric based authentication

- You can understand the enrollment process using simplistic schematic diagram

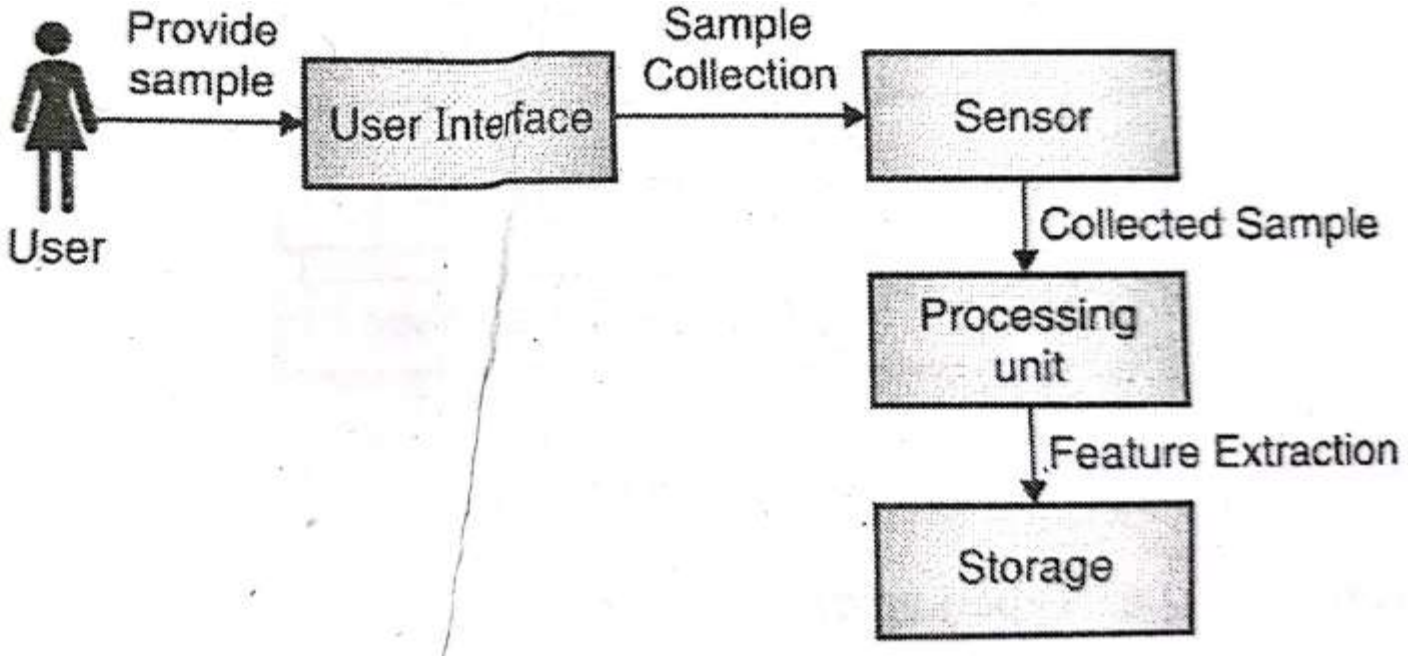


Fig. 6.9.3

Biometric based authentication

- Verification: your physical presence is again required.
- You offer the same type of sample that you provided during enrollment process
- Your provided verification sample is compared against the enrollment sample based on your identity .
- Once the two samples match , you are successfully verified .
- if the sample do not match authentication is rejected .
- This might be due to some error . In that case you can retry providing the sample again

Biometric based authentication

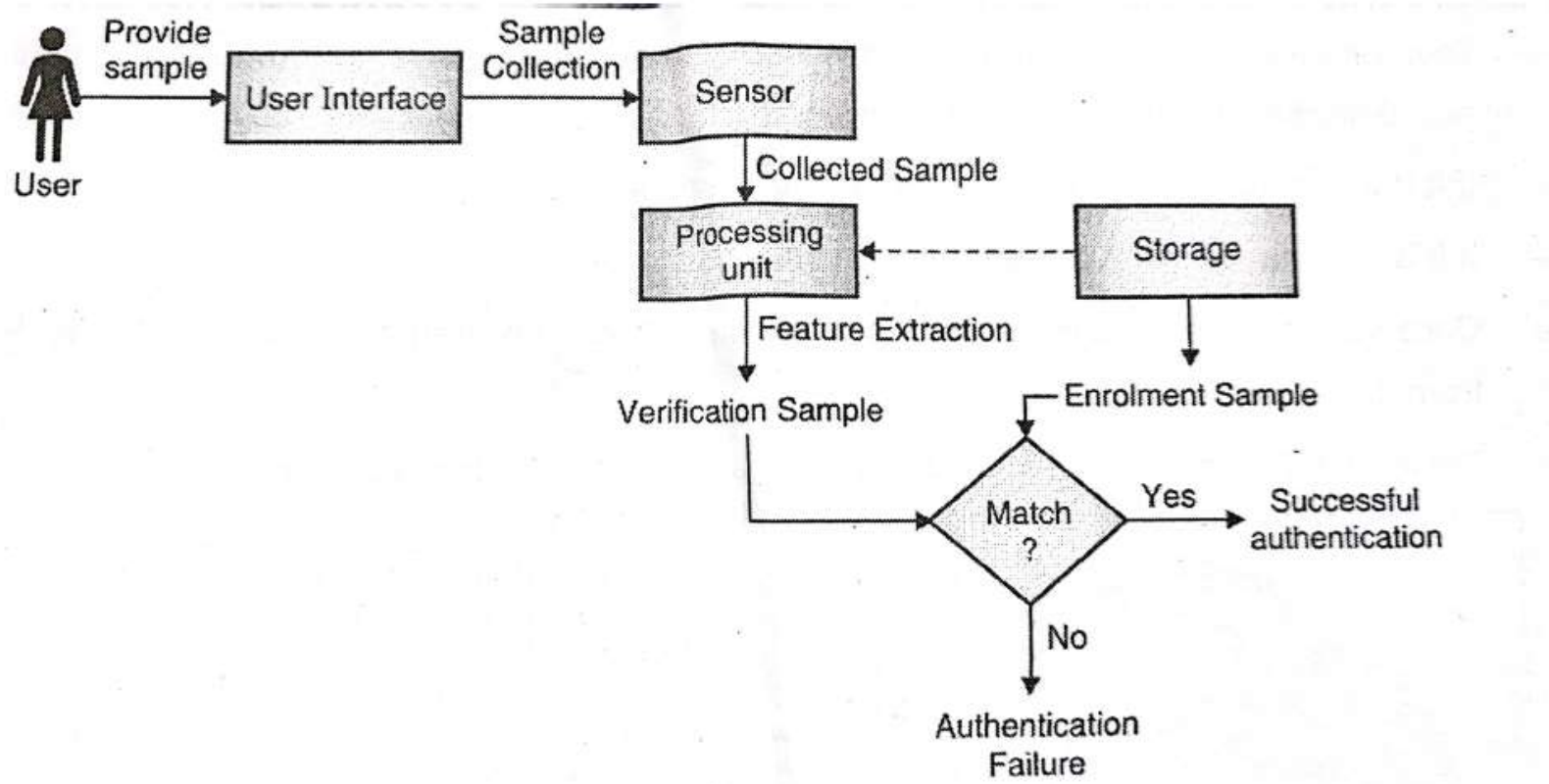


Fig. 6.9.4

Biometric based authentication

- Accuracy of biometric system:
- Biometric systems are prone to two types of error
- 1.false rejection rate(FRR) or type 1 error:
- When a biometric system rejects and authorized individual it is called type 1 error
- False rejection rate is the ratio of number of incorrect rejection to the total number of authentication attempts made
- $FRR=\frac{NUMBER\ OF\ INCORRECT\ REJECTIONS}{TOTAL\ NUMBER\ OF\ AUTHENTICATION\ ATTEMPTS\ MADE}$

Biometric based authentication

- 2.false acceptance rate(FAR) or type 2 error:
- When a biometric system accepts and an unauthorized individual it is called type 2 error
- False acceptance rate is the ratio of number of incorrect acceptances to the total number of authentication made
- $FAR=\frac{NUMBER\ OF\ INCORECT\ ACCEPTANCE}{TOTAL\ NUMBER\ OF\ AUTHENTICATION\ ATTEMPTS\ MADE}$

Biometric based authentication

- 3 crossover error rate(CER):
- Crossover error rate is the point at which false rejection rate =the false acceptance rate
- 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 authorized individuals the FRR would be high.
- Similarly, if the system accepts too many unauthorized 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

Biometric based authentication

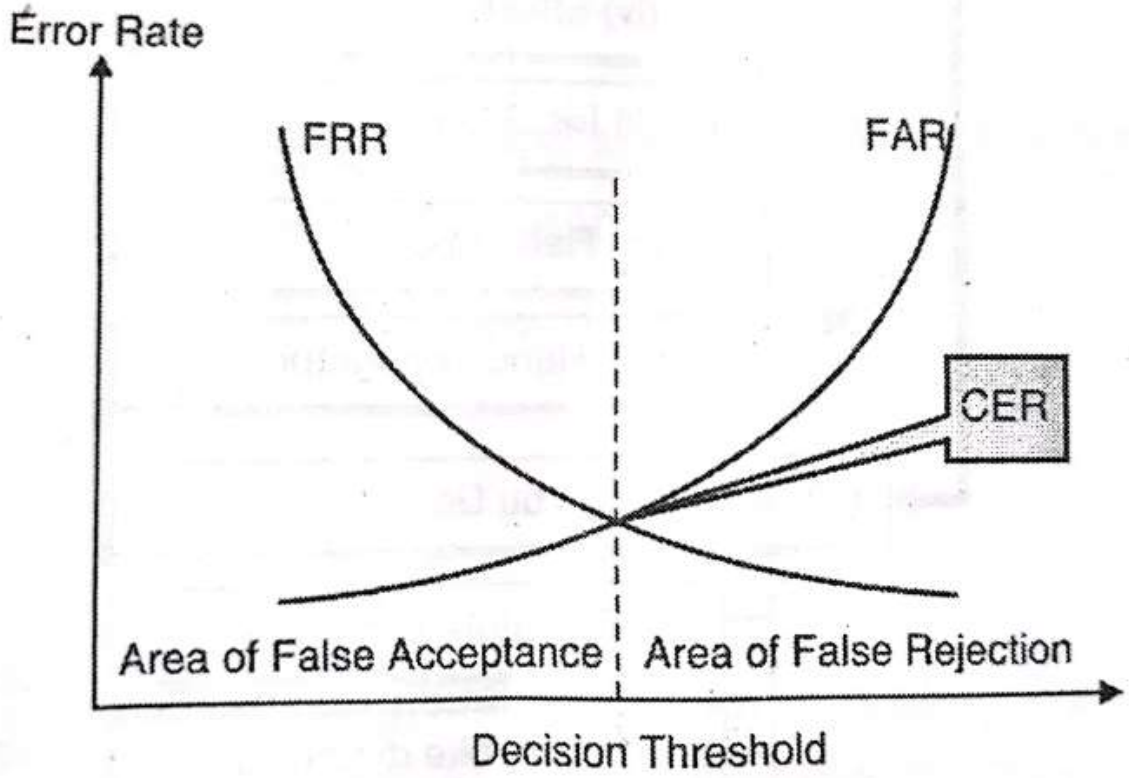


Fig. 6.9.6

Biometric based authentication

- Types of biometric system:

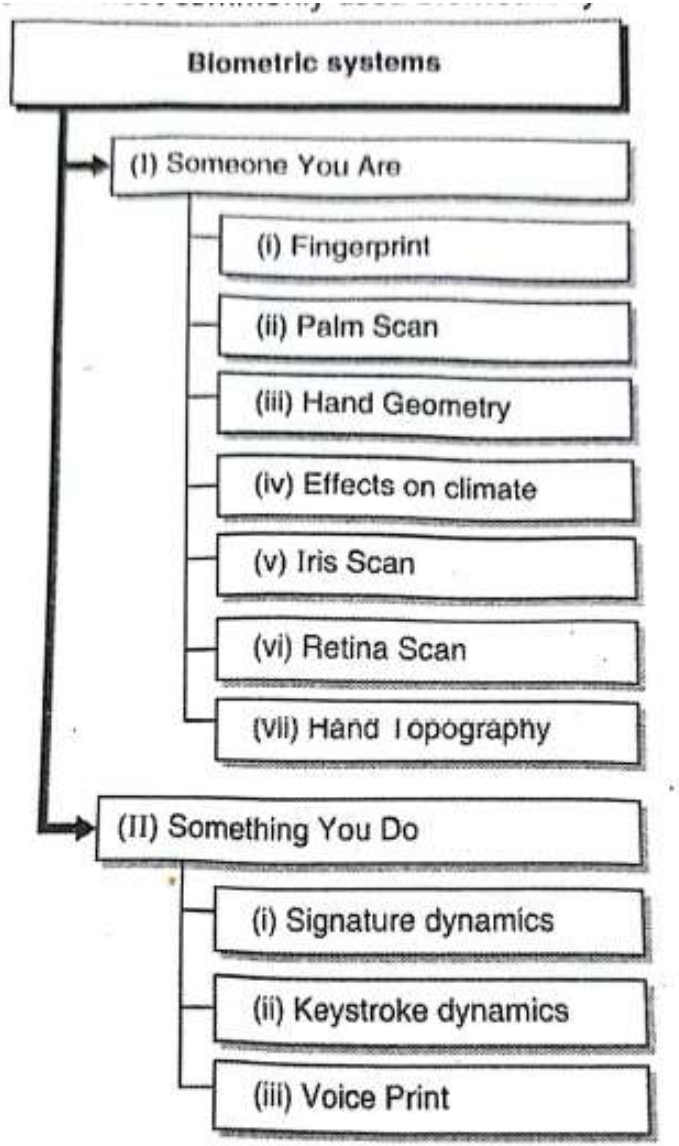


Fig. 6.9.7 : Biometric systems

Biometric based authentication

- Types of biometric system:
- 1.someone you are:
- A fingerprint
- B palm scan
- C hand geometry: your hand holds several key attributes such as shape, length, width, size etc. these attributes could fulfill biometric requirement to provide authentication information
- D retina scan involves reading the blood vessel pattern of retina on the backside of the eyeball. you are required to look into an eye scanner.

Biometric based authentication

- E iris scan: the iris has unique, colors, pattern ,rifts , rings, coronas, furrows.
- You need to look an eye scanner
- F facial scanner: it has got several key features such as nose ridges, eyewidth, chin shape, forehead size, bone structured etc
- G hand topography: it captures overall handshape and structure. The peaks and valleys in your hand biometrics traits that can be used for authentication.

Biometric based authentication

- 2 something you do :
- A 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
- B key stroke dynamics: keystrokes dynamics captured electrical signal 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.

Biometric based authentication

- C voice print:
- Alexa , siri or ok google yet
- Your voice pattern has a 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.

Biometric based authentication

- Comparison of biometric system:

Table 6.9.1

Biometric System	Processing Speed	Accuracy	Ease of Enrolment
Fingerprint	High	High	High
Palm Scan	Medium	High	Medium
Hand Geometry	Low	Medium	Low
Retina Scan	Medium	High	High
Iris Scan	Medium	High	High
Facial Scan	Medium	Low	Medium
Hand Topography	Low	Low	Low
Signature dynamics	Medium	Medium	Medium
Keystroke dynamics	Medium	Medium	Medium
Voice Print	Medium	Medium	Medium

Thank You!

(vandanas@sies.edu.in)