Rusali 21/3/24 (A+)

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

Written Assignment - 1

Explain different services & mechanisms of security.

1. Various security measures are implemented to ensure the confidentiality, integrity & availability of assets.
2. Security mechanisms are a set of processes that deal with recovery from security attack.
3. Types of security mechanisms are:

a) Encipherment:
It deals with hiding & covering of data which helps data to become confidential. It is achieved by applying mathematical calculations or algorithms which reconstruct information into not readable form. It is achieved using cryptography & encipherement. The level of data encryption depends on the algorithm used.

b) Access control:
This is used to stop unattended access to data which you are sending. It can be achieve of using passwords, firewalls or adding PIN to data.

c) Notarization:
This involves using a trusted third party in communication. It acts as a mediator between sender & receiver so that any chance of conflict is reduced.

d) Data Integrity:
It is used to append value to data created by data itself. It is similar to sending a packet of information known to both sending & receiving parties which is

checked before & after data is received. when this packet or data which is appended is checked & is the same while sending & receiving, data integrity is maintained.

e) Authentication exchange:
It deals with identity to be known in communication. This is achieved at the TCP/IP layer where three way handshake mechanism is used to ensure data is sent or not

f) Bit stuffing:
It is used to add some extra bits to data which is being transmitted it helps data to be checked at the receiving end & is achieved by even parity or odd parity.

g) Digital Signature:
This is achieved by adding digital data that is not visible to the eyes. It is a form of electronic signature which is added by the sender which is checked by the receiver electronically. This is used to preserve data which is not more confidential but the sender's identity is to be notified.

- What are various types of attacks? Explain with example.

1) Active attacks:
Active attacks are a type of attacks in which the attacker attempts to alter, destroy or disrupt the normal operations of a system or network.
Types of active attacks:
a) Masquerade:
It is a cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data. This can involve impersonating a legitimate user or system to trick other users or systems into providing sensitive information or granting access to restricted areas.
b) Modification of messages:
It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of original data.
Eg: A message "Allow John to read file x" can be turned into "Allow Smith to read file x".
c) Repudiation:
An attacker attempts to deny or repudiate actions that they have taken such as

making a transaction or sending a message. These attacks can be a serious problem as they can make it difficult to trace down the source of the attack or determine who is responsible for a particular action.

d) Replay:

It involves the passive capture of a message & its subsequent transmission to produce an authorised effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network & later on use that data for personal use.

e) Denial of service

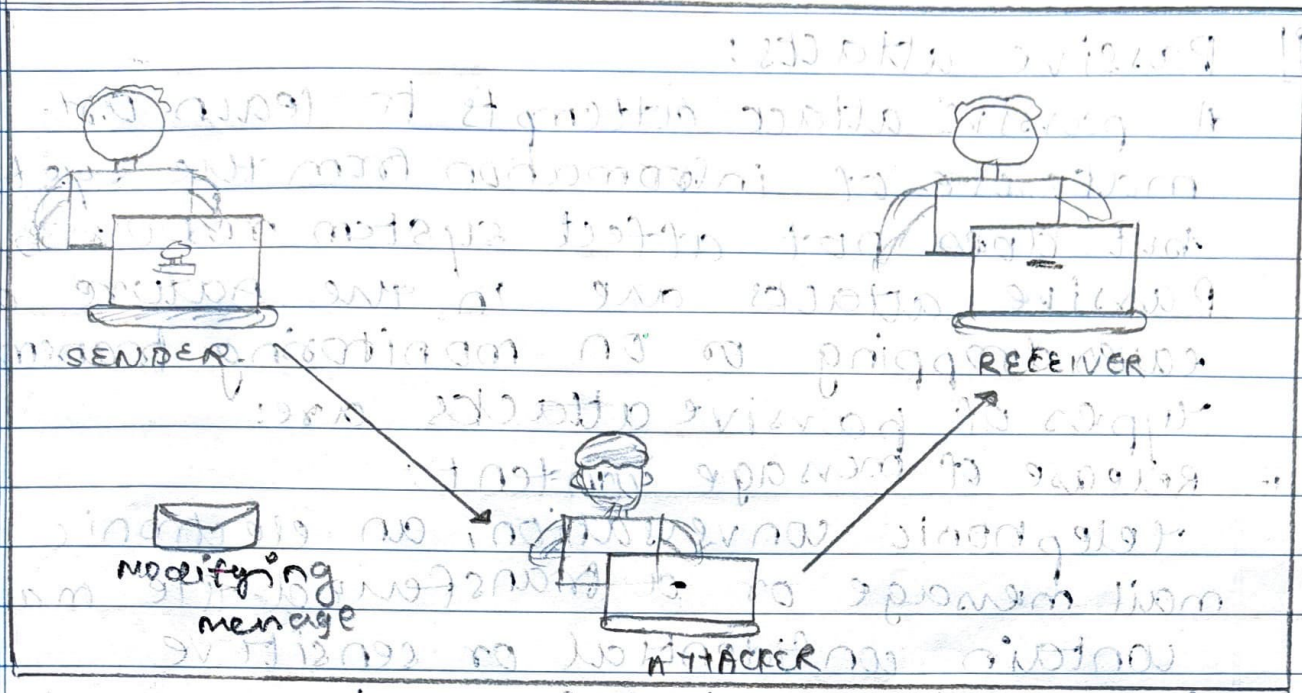
It is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests. In a DOS attacker floods a target system or network with traffic or requests in order to consume its resources such as bandwidth, CPU cycles or memory & prevent legitimate users from accessing it.

Passive attacks:

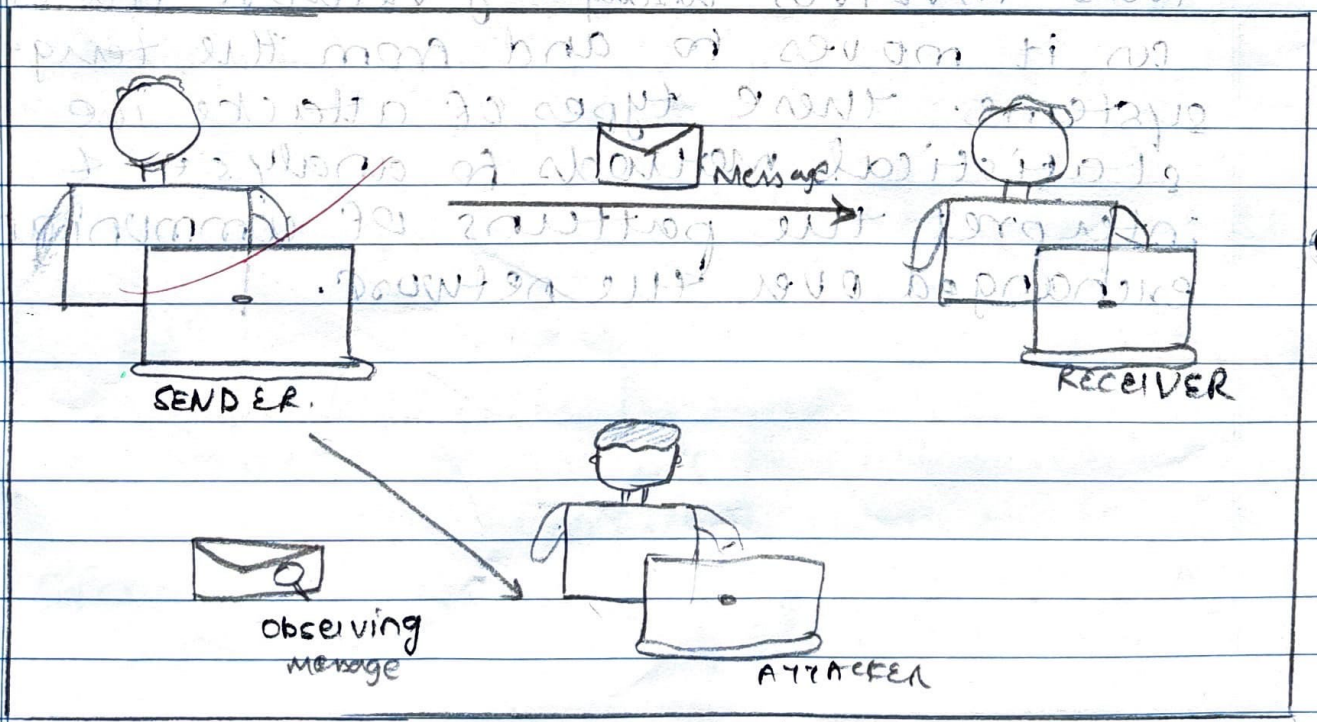
A passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive attacks are in the nature of eavesdropping or on monitoring transmission. Types of passive attacks are:

1. Release of message content:
Telephonic conversation, an electronic mail message or a transferred file may contain confidential or sensitive information. This information in the hands of an opponent would be dangerous.

2. Traffic analysis.
This involves analysing network traffic as it moves to and from the target systems. These types of attacks use statistical methods to analyse & interpret the patterns of communication exchanged over the network.



ACTIVE ATTACK



PASSIVE ATTACK.

Rusari 21/3/24 (A+)

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

written Assignment - 2.

write short note on 'digital signatures & digital certificates.

→ Digital Signature

1) Digital Signatures are essential in today's modern world to verify the sender of a document & his identity.

2) A digital signature is represented in a computer as a string of binary digits & computer is using a set of rules & regulations (algorithms) to identify the person signing the document as well as the originality of the data can be verified.

3) A digital signature is defined, the signature generated electronically from the digital computer to ensure the identity of the sender & contents of the message cannot be modified during transmission process.

4) Digital signature techniques achieve the authenticity, integrity & non-repudiation of the data over the internet.

5) Concept of digital signature is that sender of a message uses a signing key (private key) to sign the message uses & send that message & its digital signature to receiver over insecure communication channel.

6) The receiver uses a verification key of the sender only to verify

the origin of the message & make sure that it has not been tampered with while in transit as transmitted.

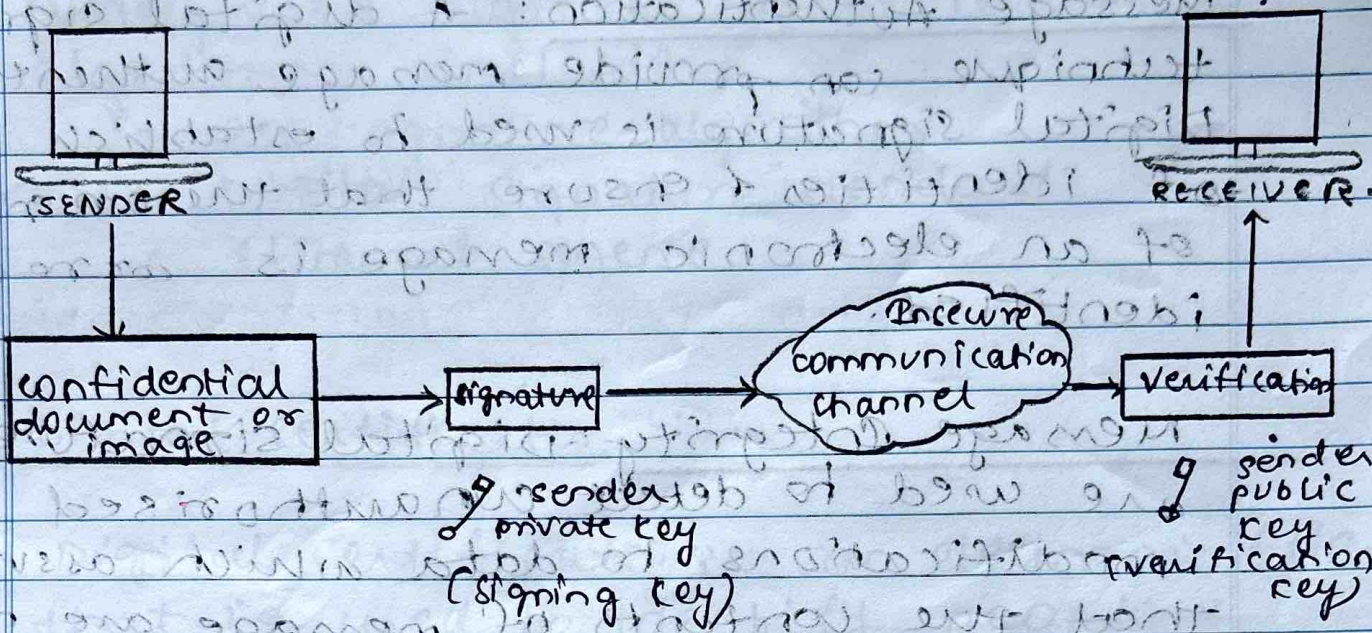
7) High value of a message when encrypted with the private key of a person is, his digital signature on that e-document.

8) Digital signature is an example of assymmetric key cryptography which uses three different algorithms to complete the process.

a) First step is key generation algorithm which generates private key & a corresponding public key

b) Next step signing algorithm which selects sending message & a private key generated in step 1, to produce a signature.

c) Third step is signature verifying algorithm which verifies the authenticity of sending message & public key.



10) As mentioned above the signature is generated with the help of private key. The private key, which is never shared, is used in signature generation, known to sender only.

11) Public keys, which are known by everyone, can be used to verify the signature of a sender. Every sender & receiver having a private & public key pair, a reason digital signature called public-key cryptography.

12) Digital signature Goals.

- 1. Message Authentication
- 2. Message Integrity
- 3. Non - repudiation.

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

- **Message Authentication**: A digital signature technique can provide message authentication. Digital signature is used to establish proof of identities & ensure that the origin of an electronic message is correctly identified.

- **Message Integrity**: Digital signatures are used to detect unauthorised modifications to data which assures that the contents of message are not changed after sender sends but before it reaches the intended receiver.

- **Non Repudiation**: There are situation where a user sends a message & later on refuses that he had sent that message. This is known as non-repudiation because the person who signed the document cannot repudiate the signature at a later time.

13. Widely used digital signature schemes/ algorithms include:
    a. RSA signature algorithm
    b. Digital signature standard
    c. ElGamal scheme.

Digital certificates:

1. Digital certificate is an electronic file that is used to identify people & resources over an insecure channel → a network called Internet. Digital certificate also enables secure, confidential communication b/w the sender & receiver using encryption
2. The role of certification authority (CA) is to issue certificates with authorised digital signature. Much like the role of the CA is to validate the certificate owners identity & to "sign" the certificate so that it cannot be tampered by unauthorised user.
3. Once a CA has signed a certificate the owner can present their certificate to people, websites & network resources to prove their identity for confidential communications over insecure channels
4. A standard called as X.509 defines structure of a digital certificate

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

certificate version number.
certificate serial number
Algorithm for signature identifier
certificate issuer name.
validity details
Name of the certificate owner
public key of certificate owner
Issuer unique identifier
owner unique identifier
extension to certificate.
certification Authority (CA)
Digital signature

Digital certificate contents

Structure of X.509 Digital certificate

A standard digital certificate typically includes a variety of information pertaining to its owner & to the certification Authority such as:

1. Certificate version Number:
Identifies a particular version of the X.509.

2. Certificate serial number:
Unique integer number generated by Certification Authority

3. Algorithm for signature identifier:
Identifies algorithm used by the certification authority to sign the certificate.

4. Certificate issuer name:
The name of the certification authority that issues the certificate.

5. Validity details:
The validity period of the certificate.

6. Name of the certificate owner:
The name of the owner & other identification information required for identifying the owner such as email.

7. Public key of certificate owner:
Certificate owner's public key, which is used to encrypt confidential information

of the certificate's owner.

8. Issuer unique identifier.
Identify the CA uniquely. i.e whether a single CA signed it or any CA using some details.

9. Owner unique Identifier:
Identify the owner uniquely if two or more owner has used the same name over a time.

10. Extensions to certificate:
This is an optional field which allows a CA to add additional private information to certificate

11. Certification Authority (CA) Digital signature
On creating the certificate, this information is digitally signed by the issuing CA. The CA signature on the certificates is like a tamper detection on packaging any tampering with the contents is easily detected.

Ishita Nandasmalani
THADOMAL SHAHANI ENGINEERING COLLEGE TSEC
C14
2103058

Bursari 22/12/24 (A)

Written Assignment - 3.

List software vulnerabilities. How are they exploited to launch an attack?.

Ans. Software vulnerabilities are weaknesses or flaws in a computer program or system that can be exploited by attackers to compromise the security, integrity, or availability of the software. These vulnerabilities can exist at various levels of software, including applications, operating systems, libraries & other components. Understanding & addressing software vulnerabilities is crucial for maintaining a secure computing environment. Software vulnerabilities can be mitigated through various measures, including regular software updates, patches, secure coding practices, input validation & the implementation of security best practices throughout the software development lifecycle.

- SQL injection: It is a type of cyber attack that exploits vulnerabilities in an application's software, allowing an attacker to manipulate the SQL queries executed by the application's database. This form of attack occurs when an application doesn't properly validate user inputs before incorporating them into SQL statements.

- Cross site scripting (XSS) is a type of security vulnerability found in web applications. XSS occurs when an attacker injects malicious scripts into web pages viewed by other users. These scripts are then executed in the context of the victim's browser, allowing the attacker to steal sensitive information, manipulate web content, or perform actions on behalf of the user without their consent.

- Cross site Request Forgery (CSRF) takes advantage of a user's authenticated session to perform unauthorized actions on a web application without their knowledge or consent. Attackers trick users into unknowingly submitting malicious requests.

- Security misconfigurations result from improper configuration settings, default settings, or unnecessary services. Misconfigurations can expose vulnerabilities that attackers may exploit to gain unauthorized access or compromise system integrity.

- Unvalidated input occurs when there is a failure to properly validate input data can lead to vulnerabilities like code injection, buffer overflows. Attackers exploit this weakness to manipulate the behaviour of the software.

- Denial of service (DOS) & Distributed Denial of service (DDOS): DOS attacks overwhelm a system or network, making it unavailable to legitimate users. DDOS attacks involve multiple compromised systems working together to launch a coordinated attack, causing service disruption.

- Insecure Direct Object References arises when an application provides direct access to objects (files, databases, etc) based on input without proper authorization. Attackers may exploit this to access unauthorized resources.

- Command injection: Command injection vulnerabilities arise when an application allows user input to be executed as a command by an underlying system shell. Attackers can inject malicious commands, leading to unauthorized access, & data manipulation or remote code execution.

THADOMAL SHAHANI
TSEC
ENGINEERING COLLEGE

- Buffer overflows.

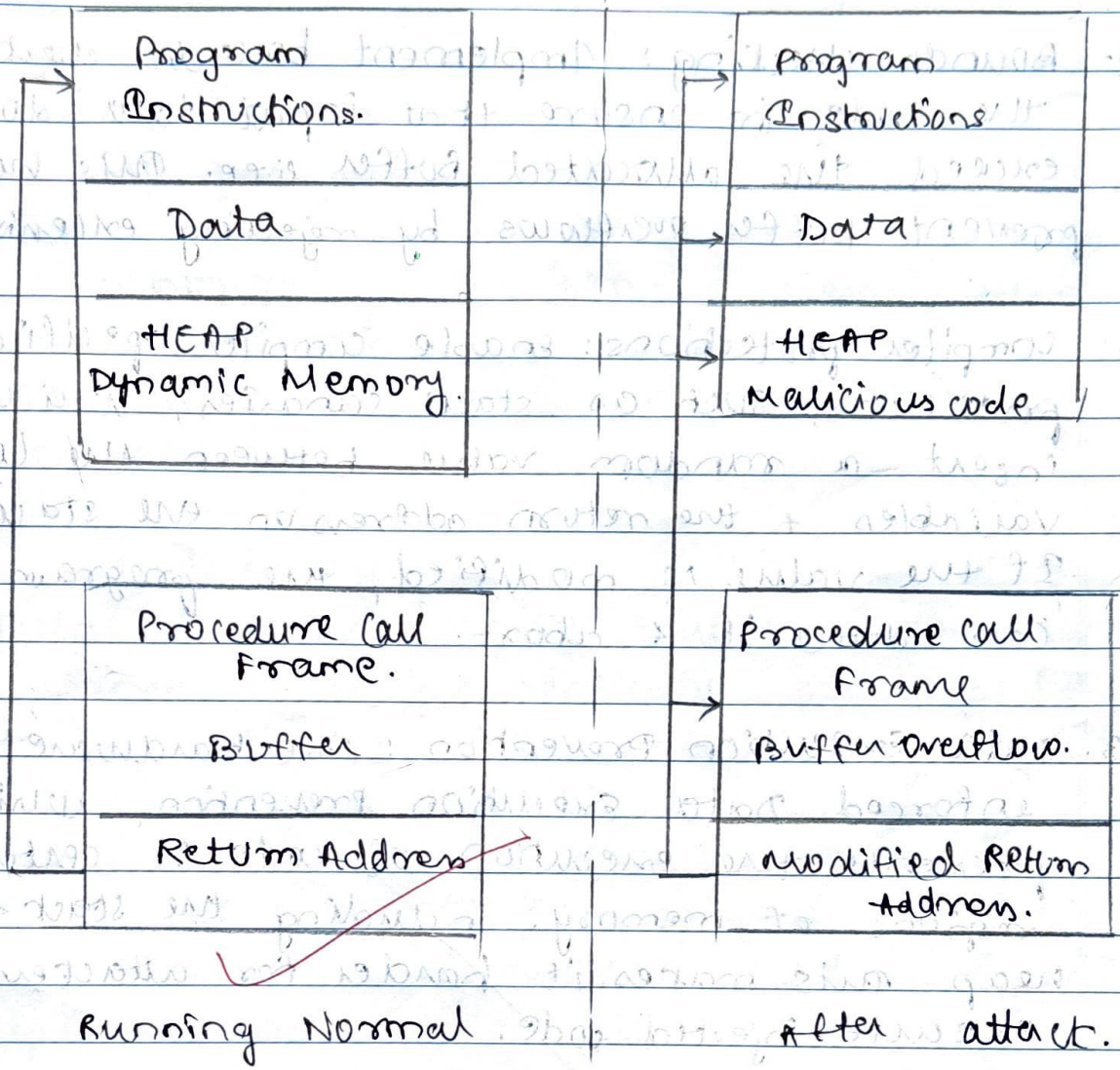
A buffer overflow occurs when a program writes more data to a buffer, which is a temporary storage area in the computer's memory, that it can hold. Attacker can insert malicious data values/ instruction codes into overflow space. This overflow can lead to overwriting adjacent memory locations, causing unexpected behavior & potentially leading to security vulnerabilities. Buffer overflow often result from improper input validation or unchecked buffers in the program's code.

Example: int B[15];

Here the array bound is (0 to (4) ;i.e B[0] to B[14] If anything inserted after that bound then the adjacent data is overwritten. Attacker can overwrite users data, changes user instruction, overwrite OS data, changes OS instructions. This can get complete control of a program or OS. This is also known as aliasing.

By carefully crafting the input, an attacker may overwrite critical data with values that point to malicious code. When the program tries to execute this manipulated data, it unwittingly executes the attacker's code.

Buffer overflows can lead to arbitrary code execution, unauthorized access, privilege escalation, denial of service, etc.



→ Protecting against Buffer Overflow:

1. Bounds checking: Implement bounds checking in the code to ensure that input data doesn't exceed the allocated buffer size. This helps prevent buffer overflows by rejecting excessive input.

2. Compiler protections: Enable compiler specific protections, such as stack canaries, which insert a random value between the local variables & the return address on the stack. If the value is modified, the program can detect it & abort.

3. Data Execution Prevention: Use hardware enforced Data Execution Prevention, which prevents the execution of code in certain regions of memory, including the stack & the heap. This makes it harder for attackers to execute injected code.

4. Input validation: Always validate & sanitize user inputs. Ensure that the input data conforms to expected formats and doesn't contain unexpected characters or excessively long values.

5. Regular code audits & penetration testing to identify & address potential buffer overflow vulnerabilities in the software.

Authentication & Authorization are critical components of ensuring the security of a system.

Authentication issues: It is the process of verifying the identity of a user, system, or entity. Weaknesses in authentication can lead to unauthorized access. Common issues can be use of weak passwords, lack of multi-factor authentication (MFA), & improper storage of credentials.

Overcome this by:

1. Regular security training: Educate users about the importance of strong authentication practices. Raise awareness about attacks & attempts.

2. User account lockout policies: Implement account lockout mechanisms to temporarily lock accounts after a certain no. of failed login attempts. This helps prevent brute-force attacks.

3. Secure storage of credentials: Employ secure password hashing & encryption techniques to protect stored passwords. Avoid storing plaintext passwords & use strong encryption algorithms.

4. Implement Multi-factor authentication allow users to authenticate using multiple factors such as OTP, biometrics. It adds an extra layer of verification.

Authorization issues: It involves granting or denying access rights to authenticated users based on their roles & permissions. Authorization issues can arise when users are granted excessive privileges or when there are vulnerabilities that allow unauthorized access.

Overcome this by:

1. Role-Based access control: Implement RBAC to assign roles to users & grant permissions based on those roles. It simplifies the management of permissions & reduces the risk of over authorization.

2. Audit & Monitoring: Implement robust logging & monitoring systems to track user activities & access attempts. Regularly review logs to identify any suspicious or unauthorized access.

3. Apply the principle of least privilege, users should have the minimum level of access necessary to perform their duties. Regularly review & update permissions based on job roles.