Information Security

EG3203CT

Sixth Semester

Notes

Prepared by

Laxmi Yadav & Sushant Sharma

Diploma in Computer Engineering

Unit-1 Introduction

1.1. Information System.

An information system (IS) is an interconnected set of components used to collect, store, process and transmit data and digital information. At its core; it is a collection of hardware; software, data, people and processes that work together to transform raw data into useful information. An IS supports a variety of business objectives such as improved customer service or increased efficiency.

People often use the term "information system" interchangeably with "computer system" but these systems are not the same. While computers systems are part of an IS, they do not encompass all the components and processes that make up an IS, such as people and processes. "Information Technology" (IT) is another similar term, but IT focuses on the technical aspects of the hardware and software that supports enterpise computing. An IS on the other hand, focuses on how people use IT and data to manage and make decisions within an organization.

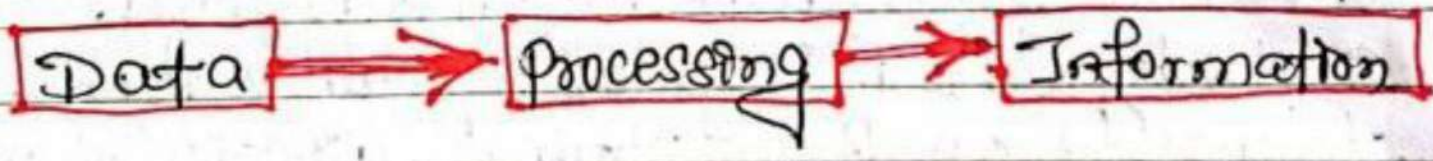
Dimensions of an information system,

There are various dimension of an information system:-
- Organizational dimension
- Management dimension
- Technology dimension.

1.2. Data and Information

Data:

Data is a raw material; it is a collection of facts and figures. Data does not have a significant meaning because of its raw nature. Data may include text, figures, facts, images, number, graphs and symbols and it can be generated from different sources like sensors, surveys, transaction; social media, etc.



A proper analysis of data plays an important role in fields like research, science, business, healthcare, agriculture and technology driving decision making and innovation

- Raw material
- Processed Data
- Structured information

- Unstructured information
- It has no context
- It has context

Information:

An information is a processed data. It is always useful and used in decision making. A person who has a lot of information about a particular thing is always considered a knowledgeable person. Hence, a good information base always makes a good knowledge base and a good knowledge base helps to make healthy & fruitfull decision.

Characteristics

- It is effective and complete to make decisions.
- True information is broad in scope
- It relates current situations and has acceptable level of integrity.
- Compatible with response time.
- concise and does not contain delicacy.
- Precise and accurate.
- Organized and stored for future reference.

Different between Data & Information

	Data	Information
①	Data is raw material.	Information is processed data.
②	It is meaningless	It is meaningful.
③	not use in decision making.	Used in decision making
④	It does not rely on information	It relies on data
⑤	Data is collection of facts.	Information kept facts in context.
⑥	Data is unorganized	Information is organized.
⑦	It can be considered as a single unit that is unprocessed.	It is a product and a collection of data.

1.3. Vulnerability & attacks

Vulnerability:

A security vulnerability is a weakness, flaw, or error found within a security system that has the potential to be leveraged by a threat agent in order to compromise a secure network.

Mistakes happen, even in the process of building and coding technology. What's left behind from these mistakes is commonly referred to as a bug. While bugs aren't inherently harmful, many can be taken advantage of by nefarious actors; these are known as vulnerabilities.

There are a number of security vulnerabilities but some common examples are.

- **Broken Authentication:**
  When authentication credentials are compromised, user sessions and identities can be hijacked by malicious actors to pose as the original user.

- **SQL injection:**
  It attempt to gain access to database content via a malicious code injection that

allow attackers to steal sensitive data, spoof identities.

- Cross site scripting:
  Like an SQL injection, Cross site scripting (XSS) attack also inject malicious code into a website which targets websites user, rather than the actual website itself.

- Cross- Site Request Forgery:
  A cross-site Request forgery (CSRF) attack aims to trick an authenticated user into performing an action that they do not intend to do. Paired with social engineering, can deceive users into accidentally providing a malicious actor with personal data.

- Security Misconfiguration:
  Any component of a security system that can be leveraged by attackers due to a configuration error can be considered a "security Misconfiguration".

Attacks:

An attempt to gain unauthorized access to system services, resources or information or an attempt to compromise system integrity, availability or confidentiality.

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permissions. It happens to both individuals and organizations. There are many different kinds of attacks, including but not limited to passive, active, targeted, clickjacking, brandjacking, botnet, phishing, spamming, inside and outside

Types of Cyber Attacks:

1. Malware:

Malware is malicious software designed to cause damage to computer network & servers. There are different form of malware including Trojan, viruses and worm and they all reproduce and spread through a computer network to steal data, cause damage to devices, render network inoperable

or take control of systems.

d. Phishing:

A phishing attack tricks a target into downloading malware or entering sensitive information into spoofed websites. These cyber-attack methods are typically launched via email, with the attacker creating messages that look legitimate and may appear to be from a trusted sender. However they will contain malware within an attachment or a malicious hyperlink that asks the recipient to enter their login credentials or banking details.

6. Ransomeware:

Ransomeware attacks are a financially fueled form of malware attack. Attacker send messages containing a malicious attachment that, when downloaded, encrypts specific data and files or entire computers. The attacker will then demand a ransom fee from the victim and will only release or restore

access to the data upon payment.

④ Man-in-the-Middle:

MITM attacks enable a malicious actor to position themselves between the target victim and an online service the user accesses. An example of this is an attacker creating a spoofed, free-to access Wifi network. When the user connects to or signs into the network, the attacker can steal the login credentials and data they use while on it.

⑤ Cryptojacking:

A cryptojacking attack occurs when a bad actor takes control of a computer, mobile device or server to mine for online currency or cryptocurrency. The attack either begins with malware being installed on a computer or by running code in JavaScript to infiltrate the user's browser.

⑥ DNS tunneling:

DNS tunneling is a cyber-attack method that targets the Domain Name System (DNS), a protocol that translates web addresses into Internet protocol (IP) addresses. DNS is

widely trusted and not intended for transferring data. This makes it an effective target to launch cyber-attacks against corporate networks.

1.4. Security Goals.

Information security is designed and required to secure the print, digital and some personal sensitive and private information from unapproved persons. It very well may be utilized to get information from being misused, affirmation, destruction, modification and interruption.

There are the major goals of information security which are:

* Confidentiality:

The goals of confidentiality is that only the sender and the pre-determined recipient should be adequate to approach the element of a message.

Date
Page

② Integrity: When the element of a message is transformed after the sender sends it but since it reaches the intended recipient and it can said that the principle of the message is lost.

③ Availability: The main goals of information security is availability. It is that resources must be available to authorized parties at all times.

④ Authentication:
It ensures that only authorized individuals or systems are allowed access. by verifying the identity of users & devices.

⑤ Non-repudiation:
It is achieved through digital signature and other cryptographic mechanism. It ensures that a sender should not manage to refuse sending a message that they send.

Security services and mechanisms

Security services:
A service that enhances the security of the data processing system and the information transfers of an organization.

Security mechanism:
A mechanism that is designed to detect, prevent or recover from a security attack.

Types of security mechanism are

① Access control:
It is used to stop unattended access to data which you are sending. It can be achieved by various techniques such as applying password, using forewalls or just by adding PIN for data

② Bit stuffing.
It is used to add some extra bits into data which is being transmitted. It helps data to be checked at the receiving

end and is achieved by Even parity or Odd parity.

④ Authentication exchange.
It deals with identity to be known in communication. It is achieved at the TCP/IP layer where two-way handshaking mechanism is used to ensure data is sent or not.

⑤ Data Integrity:
It is used by appending value to data to which is created by itself. If the packet or data which is appended is checked and is the same while sending and receiving then data integrity is maintained.

⑥ Digital signature

⑦ Notarization (प्रमाणित गर्ने प्रक्रिया).

⑧ Encipherment.

⑨ Routing Control.

⑩ Traffic-padding.

Unit-3. - Cryptographic Techniques....

A cryptographic techniques refers to a method or algorithm used to ~~creat~~ secure information by transforming it into an unreadable format known as cipher text, that can only be read by someone with the correct decryption key. It ensures the protection of data during storage and transmission against unauthorized access and tampering (छेडछाड).

* Conventional Cryptographic Techniques.

It refers to the traditional methods of encryption and decryption that primarily involve the use of symmetric key. In this techniques, the same key is used for both encrypting and decrypting data. This key must be kept secret and shared only between the communicating parties.

Characteristic

- Symmetric key usage.
  - Use same key for both encryption & decryption.

- Efficiency:
  Suitable for encrypting large amount data.
- key Management:
  Requires a secure method to share the key between parties.
- key length.
  Longer keys provide better security but may reduce performance.
- Security
  - Depends on the secrecy of the key.

Conventional Substitution and Transposition Ciphers:

Conventional Ciphers generally refer to classical techniques for encrypting text, primarily involving symmetric-key cryptography. These can be further divided into substitution ciphers and transposition ciphers.

Substitution Ciphers

Substitution ciphers involve replacing each letter or group of letters in

the plaintext with another letter or group of letters. The main goal is to obscure the original text by systematically substituting its characters

* Characteristics

- Character Replacement
Each character in the plaintext is replaced with another character.

- Fixed Mapping
substitution pattern is fixed and consistent throughout the message.

Examples
1. Caesar Cipher.
2. Atbash Cipher
3. Vigenere Cipher
4. Monoalphabetic Cipher.

Transposition Cipher.

It involves the rearranging the character of the plain text according to a certain system; without changing the actual character themselves.

Date
Page

* Characteristic.

1. Character Rearrangement.

Character are moved to different position based on a defined system.

2. Same Characters:

It contains the same character as the plain text, but in different order.

For example.

- Rail Fence Cipher.
- Columnar Transposition Cipher
- Route Cipher.

One time pad.

The one time pad (OTP) is a cryptographic techniques that offers theoretically perfect security when used correctly. It involves using a random key that is as long as the plaintext message. Each character or bit of the plaintext is combined with a character or bit from the key to produce the cipher text.

Characteristics.

1. Perfect security.
- If the key is truly random, used only once, and kept secret, the otp is unbreakable.

2. Key length.
The key must be at least as long as the plaintext.

3. Key Usage
Each key is used once and discarded after use.

4. Random key.
- The key must be completely random.

Operation

Encryption:
Each character / bit of the plaintext is combined with the corresponding character / bit of the key using a bitwise XOR operation for example.:
- plaintext : 01001100 (binary)
- key : 10101010 (random binary key)
- Ciphertext : 11100110 (result of XOR operation)

Date
Page

Decryption

The same process is applied to the cipher text with the same key to retrieve the plaintext.

- Cipher text : 11100110
- key : 10101010
- Plain text : 01001100.

Advantage

- Unbreakable
- Simplicity.
- No pattern.
- No computational limitation.

Disadvantage

- Key Management
- key distribution
- Single Use
- Storage Requirement
- Practicality.

Application

- Ensuring absolute security in operation.
- protecting confidential government exchanges.
- Securing sensitive information.
- Highly security system.
- Journalist source protection.

Block cipher and Stream cipher

Block cipher:

A block cipher is a type of symmetric key encryption algorithm that processes fixed size blocks of data typically 64 and 128 bits. It takes a block of plaintext and a key as input and produces a block of ciphertext of the same size. Common cipher-~~text block~~ include AES (Advanced Encryption Standard) and DES (Data Encryption Standard). They are used in various cryptographic protocols and applications to ensure data confidentiality. Block ciphers can operate in different modes, such as ECB (Electronic Codebook); CBC (Cipher Coded Block chaining) and CFB (Cipher Feedback) to provide additional security features.

Characteristics

- Fixed size blocks.
- Uses modes of operation,
- Requires padding for incomplete blocks.

- Example : AES, DES, 3DES.

Advantage.
- High security
- Versatile with different modes
- Errors contained within blocks

Disadvantage.
- More complex
- Paddings add overhead
- Can be slower.

Common modes of operation.

1. ECB (Electronic Code Book).
Simplest mode, but least secure because identical plaintext blocks result in identical ciphertext block.

2. CBC (Cipher Block Chaining).
- Each plaintext block is XOR-ed with the previous ciphertext block before being encrypted, improving security.

3. CFB (Cipher Feedback)
- converts a block cipher into a synchronous stream cipher, making it resistant

to transmission.

④ OFB (Output Feedback).
- converts a block cipher into a synchronous stream cipher, making it resistant to transmission errors.

⑤ CTR (counter).
- Turns a block cipher into a stream cipher by combining a counter value with a nonce ( ) providing high efficiency and parallelizability

Application.
- Data Encryption: securing files and sensitive data.
- Secure Communication: protecting data transmitted over networks
- Cryptographic protocols: Used in protocols like SSL/TLS for secure internet communication.

Stream Cipher.

An algorithm of encryption that processes data one bit or byte at a time, producing a continuous stream of encrypted data. It generates a stream of pseudo-random keys that are combined with the plaintext using bit wise operation like XOR (exclusive OR). This approach contrast with block ciphers, which encrypt fixed-size blocks of data.

Characteristics:

(1) Bit by Bit or Byte by Byte Encryption
- Processes data one unit at a time.

(2) Keystream Generation.
- Uses a pseudorandom keystream XOR with plaintext.

(3) No padding Required.
- Handles data of any length without padding

(4) Encryption Variability.
- Same plaintext encrypted with different keystream yields different cipher text.

(5) Common Algorithms.
- RC4, Salsa20, ChaCha20,

Advantages.
- Efficiency in real-time encryption.
- Low complexity.
- No padding overhead.
- Flexibility.
- Stream processing.

Disadvantages.
- Single bit error can corrupt entire messages.
- Reusing keystreams can lead to security issues.
- Some ciphers have known vulnerabilities.
- Requires precise synchronization between sender and receiver.
- Weak keystream generation can make the cipher vulnerable.

Date
Page

Drawback of Steganography

- Requires a lot of overhead to hide a relatively few bits of information.
- Once the system is discovered, it becomes virtually worthless.

(2) Symmetric and Asymmetric Cryptographic Techniques

Symmetric cryptographic Techniques

In cryptography, "symmetric" refers to the use of the same key for both encryption and decryption. This means that both the sender and receiver use the same secret key to transform plaintext into ciphertext and vice-versa. Both individuals must have access to the same secret key and keep it confidential.

Asymmetric cryptographic Techniques

Asymmetric cryptography, also known as public key cryptography, involves the use of

two keys: a public key is used to encrypt data, while the private key is used to decrypt it. This method enhances security because even if someone intercept the encrypted data, they can not decrypt it without the private key.

2.2.1. Rivest, Shamir and Adleman (RSA)

RSA is a widely used asymmetric encryption algorithm that relies on the mathematical properties of large prime number to provide secure communication. It uses a pair of keys, a public key for encrypting data and a private key for decrypting it. It is also used for creating digital signatures that verify the authenticity and integrity of messages. For example: Encrypting a symmetric key for secure exchange.

Advantage.

- Strong security due to its mathematical basis on large prime numbers.
- Easy to implement RSA algorithm.
- Useful for secure key exchange and digital signatures.
- Safe & secure for transmitting sensitive data

Disadvantage
- Slower than symmetric encryption algorithm like AES.
- Slow data transfer rate due to large amount data.
- Require more computational power; making it less efficient for large volume of data.

DES (Data Encryption Standard).

DES is a symmetric-key encryption algorithm that was widely used for data encryption. It uses a single key to both encrypt & decrypt data. DES transforms plaintext into cipher text using a series of complex permutations and substitutions through multiple round of processing. Due to its 56 bit key size, it is no longer considered secure against modern brute-force attacks. It is used to protect sensitive data by converting it into a secure format. For example, Encrypting "HELLO" using an 8-byte key.

Advantage.
- Faster encryption and decryption compared to RSA.
- Simpler to implement.

Disadvantage.

- considered insecure today because its 56-key can be broken with modern computing power.
- Replaced by more secure algorithm like AES

AES (Advanced Encryption Standard)

AES is a symmetric key encryption algorithm that replaced DES due to its superior security and efficiency. It encrypts and decrypts data using a single key, with key sizes of 128, 192, or 256 bits. AES processes data in block and applies multiple round of transformation, making it highly secure and efficient for modern application. It is the standard encryption algorithm used today. For example: Encrypting the text "HELLO" with a 128 bit key.

Advantage

- Stronger security compared to DES.
- Efficient and fast, suitable for both hardware and software implementations.

Date
Page

disadvantage
- Requires proper key management and secure key storage
- While very secure, it still needs careful implementations to avoid vulnerabilities.

Review Questions.

1. What is cryptography? write its importance.
2. What is conventional substitution and transposition ciphers.
3. Differentiate Block cipher and Stream cipher.
4. What is Steganography.?
5. Explain symmetric and asymmetric cryptography with example
6. Explain RSA, DES, IDEA with example.
7. Define one-time pad.

Unit 5

Authentication and Digital signatures.

Authentication:

- Authentication is the process of verifying the identity of a user, device or a system.
- It ensures that only authorized users or system are allowed to access a system or application is who they claim to be.
- Common methods of authentication include passwords, biometric data & security token.

Uses of cryptography for authentication.

- Cryptography is used for authentication by ensuring that only authorized users can access certain data or services.
- It provides data to be transfered in such a way that no outsider can interpret the data or change it.
- There are the primary way in which cryptography is used,
  1. Password Hashing
  2. Secure Socket Layer
  3. Digital signature

- Biometric Authentication.
- Two-factor Authentication.

Digital signature.

A digital signatures is a type of electronic signatures that encrypts document with digital codes that are particularly difficult to duplicate. The main purpose of a digital signatures is to secure a document so that it is not tampered by people without authorization. It serves several key purpose such as:

(i) Authentication.

It confirm the identity of the signer, ensuring that the document or message was indeed sent by the claimed sender.

(ii) Integrity - Ensures the document has not been altered.

(iii) Non-Repudiation:

Prevents the signer from denying their signatures.

Date
Page

Secure Hash Function

A secure hash function is a cryptographic algorithm that generates a fixed-size output (hash) from an input (message) of any size. These hash values are used in various application such as integrity, verification & digital signature.

It works by transforming the data using a hash function : an algorithm that consists of bitwise operations, modular additions and compression function.

Common hash function:

- MD5 (Message Digest Algorithm 5) (128 bit)
  considered insecure due to vulnerability collision.
- SHA-1 (Secure Hash Algorithm 1). (160 bit)
  More secure than MD5 but being phased out in favor of stronger algorithms.
- SHA-256. (256 bit)
  widely used for its strong security properties
- SHA-3.
  offers improved security and flexibility. compared to SHA-2

Date
Page

Key management kerberos

Kerberos is a network authentication protocol designed to provide secure authentication for users and services in a network. Key management in kerberos involves several components:

1. **Key distribution center (KDC)**
   A central server that manages authentication and key distribution. It consists of two main components:
   - Authentication server (AS).
     Issues Ticket Granting Ticket (TGT) after validating user credentials.
   - Ticket Granting Server (TGS)
     Issues service tickets based on a TGT to allow access to specific services.

2. **Tickets:**
   Secure tokens issued by the KDC that prove a user's identity. There are two main types
   - Ticket-Granting Ticket: used to obtain tickets from the TGS.
   - Service Tickets: used to access specific services within the network.

3. Session keys.
- They are created for each session to ensures that the data exchanged is kept private and unaltered. There are temporary keys used to keep communication between user and services secure.

4. Key Exchange.
Kerberos uses secret keys that are shared between the server and users to keep information safe. This means that when data is sent, it's encrypted so that only the intended recipient can read it.

* Digital certificate.
A digital certificate is an electronic document used to prove the ownership of a public key. It includes information about the key, the identity of its owner, and digital signatures of an authority that has verified the certificate contents.

Unit 4 Application security

Date
Page

Application security -

It refers to the process of developing, adding and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification.

It describes the security measures at the application level that aim to prevent data or code within the app from being hijacked.

Importance of application security.

- Application security is important because today's applications are often available over variety and connected to the cloud, increasing vulnerabilities to security threats and breaches. Hackers target apps more frequently, securing application is essential. Application security testing helps identify and address threats, preventing potential attacks. So, Application security is essential.

(4.1) Types

There are different types of application security

such as..:

(i) Authentication:
It ensures that only authorized users can access an application. It typically involves users providing a username & password. Multi-factor authentication adds extra security by requiring additional verification such as a mobile device or biometric data like finger print.

(ii) Authorization:
After a user has been authenticated, the user may be authorized to access and use the application. Authentication must happen before authorization so that the application matches only validated user credentials to the authorized user list.

(iii) Encryption:
After a user has been authorized, and is using the application, other security measures can protect sensitive data from being seen or even used by a cybercriminal so they are encrypted to keep the data safe.

Logging:

If there is a security breach in an application, logging can help identify who got access to the data and how. Application log files provide a time stamped record of which aspects of the application were accessed and by whom.

Application security testing:

An necessary process to ensure that all of there security controls work properly.

Security in cloud:

Security in cloud refers to the measures and practices used to protect applications hosted on cloud platforms from cyber threats and vulnerabilities. It involves ensuring that cloud-based applications are secure through access control, data encryption, secure configuration, regular updates, threat detection and compliance with relevant regulations. Because cloud environments provide shared resources in which

data is transmitted across the internet from the user to the application and back. Sensitive data is more vulnerable in cloud based application.

Mobile application security.

Mobile application security refers to the measures and practices used to protect mobile apps from threats and vulnerability. Mobile devices also transmit and receive information across the internet as opposed to a private network, making them vulnerable to attack. Key elements include secure coding, data encryption, strong authentication, secure API and regular updates. This ensures that the app data, code and communication are secure from unauthorized access and attacks.

Advantages

- protection of sensitive Data
- Enhanced user Trust
- prevention of Unauthorized Access
- Reduced risk of financial loss

Disadvantage
- Implementing robust security increased development time.
- Investing in security tools can be expensive.
- Complex and harder to manage.
- Decreased app performance & affect experience.

Web Application Security

Web application security refers to the measures and practices used to protect web application from security threats and vulnerabilities. It applies to web application - apps or service that users access through a browser interface over the internet. Because web applications live on remote servers, not locally on user machines, information must be transmitted to and from the user over the internet. It involves safeguarding application from attack and ensuring the confidentiality, integrity & availability of data and functionality. This includes secure coding practices, regular vulnerability assessment, encryption and access control.

Date
Page

Advantage.

- Protects against various cyber threats.
- Keep data accurate and secure.
- Maintains user privacy.
- Ensures regulatory requirements.
- Enhances user confidence

Disadvantage.

- Implementation may be expensive
- Makes development more complex.
- May slow down the application.
- Requires continuous updates.
- May lead to over-reliance and neglect of other aspects.

Unit-5

Program Security

Program security refers to the measures and practices designed to protect software program from unauthorized access and attacks.

It includes writing secure code, controlling user access, encrypting data, regularly updating the program, and testing for vulnerabilities.

The goal is to keep the software safe and functioning properly, without being compromised.

Types of program security

(1) Authentication:
- Ensuring only authorized users can access the program.

(2) Authorization:
- ~~Offers~~ Manages authority permission and access level.

(3) Data Encryption:
- protects data to prevent unauthorized access.

(4) Input validation:
- checking and sanitizing user inputs which protects from performing cyber attacks.

(5) Secure Codings
- Implementing practices to avoid vulnerabilities during development.

(6) Error Handling:
Managing errors without exposing sensitive information.

Program Errors

Program errors are flaws or issues in software code that cause the program to behave incorrectly or fail.

It generally includes syntax errors, runtime errors, logical errors, and semantic errors.

Identifying and correcting these errors ensure the software operates correctly and reliably.

There are 2 types of program errors. ie.
① Malicious program error
② Non-malicious program error

* Malicious program error
↳

- Malicious program error are intentional flaws or vulnerabilities introduced into software with harmful intent. (जान-बूझकर) (बनाइएको)
- These errors are deliberately crafted by attackers or insiders to compromise the security and integrity of a system or application.
- These errors are designed to :
  - Exploit :
    - Create opportunities for unauthorized access or control over the system.
  - Damage :
    - Disrupt, corrupt or destroy system data.
  - Steal :
    - Extract sensitive or confidential information illegally.
  - Deploy Malware :
    - Enable the installation and execution of viruses, spyware or ransomware.

Non-malicious program error

Non-malicious program errors are unintended mistakes or flaws in software that occur without harmful intent. (3624).

These errors are typically due to oversight or coding mistakes and need debugging and correction to ensure the program function as intended.

Many such errors cause program malfunction but do not lead to more serious security vulnerability.

Clever attacker uses flaws as common building blocks to build a complex attack.

- A few classes of error have been more serious errors for programmers and security professional.
  - Buffer Overflow
  - Incomplete mediation.
  - Time-of-check to Time of use error.

Buffer Overflow

Buffer overflow is a software coding error or vulnerability that occurs when the amount of data in the buffer exceeds its storage capacity. This extra

data overflows into adjacent memory locations and corrupts or overwrites the data in those locations.

A buffer overflow attack involves violating programming languages and overwriting the bounds of the buffer they exist on.

It lead the system being crashed or put it into an infinity loop.

There are several types of buffer overflow such as:

(1) Stack-based buffer overflows.

- A stack based buffer overflows occur when a program writes more data to a buffer located on the stack than it can hold.
- This overflow can overwrite adjacent memory on the stack, leading to various problems such as program crashes, data corruption or security vulnerabilities.

(2) Heap-based buffer overflow:

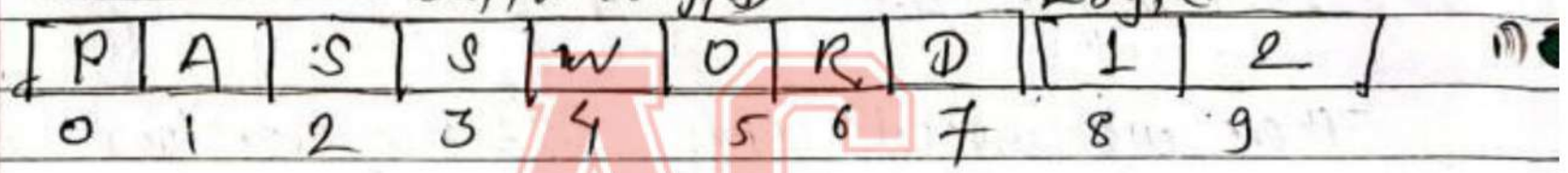
- A heap based attack is more difficult to carry out than the stack-based approach. It involves the attack flooding a programs memory space beyond the memory it uses for current runtime operations.

Date
Page

Format string attack:

A format string attack exploits a vulnerability where user inputs is used as a format string in function like printf. It occurs when attackers use format specifiers like %.x or %.n to manipulate or extract sensitive information.

Example



Incomplete mediation.

It means that data is exposed somewhere in the pathway ~~data is exposed~~ between submission and acceptance. The ultimate problem is the successful submission and acceptance of bad data. The cause of the problem is the break, or lack of security in the pathway. Inputs to program are often specified by untrusted users. The most serious concern about this flow was the length of time that it could have run undetected.

Consequences of incomplete mediation includes

unresolved disputes, ongoing conflict and potential escalation of issues. To address excomplete mediation, parties may:

- Schedule additional sessions to continue the mediation process.
- Seek more comprehensive information or clarification.
- Consider alternative dispute resolution methods if mediation fails.

Time-of-check to Time-of-use errors.

Access control is a fundamental part of computer security; we want to make sure that only those who should access an object are allowed that access. Every requested access must be governed by a mediated access policy enforcement agent.

The "Time of check to Time of use (TOCTOU) error is a type of a race condition that occurs in computer system. It arises when a system checks the state of a resource and

then uses that resource later, but the state of the resource may have changed between the check and the use. This time gap can lead to inconsistencies or security vulnerabilities.

For example,
consider a scenario where a program checks if a file exists and then opens it. If an attacker changes the file between the check and the open operation, the program might open a different file than expected, potentially leading to unintended behavior or security issues.

TOCTOU errors are important to manage in secure programming practices to ensure that resources are used safely and consistently.

The problem is called time of check and time of use flaw because it exploits the delay between the two times. ie between the time the access was checked and the time the result of the check was used; a change occurred, invalidating the result of check.

Viruses

- A program that can pass on malicious code to other non-malicious program by modifying them.
- It infects a program by attaching the program.
- It can be transient or resident.
- Transient virus life depends on the life of its host: the virus runs when the host does.
- A resident virus locate itself in memory. A good program, once infected becomes a carrier and infects other program.

Types of viruses

① File Infector Virus:
Attaches itself to executable files. It activate when the infected file is run. eg: Chernobyl virus

② Macro virus:
Targets macro function in application like Microsoft word or Excel. It spreads through documen t that use macros. eg Melissa virus.

③ Boot sector virus:
Infects the boot sector of a hard drive or removable media: It activates when the system startup. for eg. Stone virus.

(4) Polymorphic virus:
Changes its code or appearance to evade detection by antivirus software. for eg. Storm virus.

(5) Metamorphic virus:
Completely rewrites its own code each time it infects a new system, making it harder to detect for eg. Simile virus

(6) Resident virus
Installs itself into the system memory and can infect files or system processes. for eg. Kondex virus.

(7) Non-Resident virus:
Does not stay in memory but instead attaches itself to file or program. for eg. Vienna virus.

Function of virus.

1. Replication.
- A virus replicates itself to spread to other files or systems

2. Infection :
It modifies or corrupt files, program or system areas.

③ Activation:
Triggers malicious action when certain condition are met.

④ Payload Delivery:
Executes its payload, which could range from data destruction to stealing sensitive data.

⑤ Dependency on host:
Viruses need a host file or system to execute and spread.

Trap Door

Trapdoor is defined as a secret backdoor hidden within an algorithm or individual piece of data. It can gain access to the system without using security access ~~produre~~ procedure. It is often built into the system by the original developers or introduced by malicious code actors. They are often harder to detect because they are embedded within the systems design or code by developer or attackers.

→ Backdoor is a method of bypassing normal authentication method.

→ Programmer uses trapdoor legally to debug and test program.

Salami Attack

→ A salami attack is a type of cyber attack in which an attacker make small incremental changes or theft to a system or data.

→ The name "salami attack" comes from the idea of slicing off small "pieces" of data or resources, like.

→ It is only a strategy for gaining an advantage over time by accumulating small increments.

→ Series of small attacks that are not detectable.

→ It is also known as salami-slicing.

~~Man in the middle attacks.~~

Types of salami attack.

1.) Financial Salami Attack.

This is the most common type, where attackers steal small amounts of money from multiple accounts or transactions. They round down transaction or manipulate bank accounts balances to avoid immediate detection.

(a) For example:

A bank employee programs a system to round down interest calculations and deposits the fraction of cents into personal account.

(b) Data Salami Attack.

Attackers gradually steal or manipulate small pieces of data from the database that are not immediately noticeable but lead to large-scale breaches or long-term issues.

Forexample: A cybercriminal hacks into a company database and extracts small portions of customer data to build a spam list or launch targeted phishing attack.

(3) Resource Salami Attack.

Attacker consume small amount of computing resources or network bandwidth from multiple users or organization to create a larger network for malicious purposes. For example

A botnet operator uses thousands of infected device to launch distributed Denial of service (DDoS) attack on a website, consuming a small portion of each devices bandwidth.

Man-in-the-Middle-Attack.

⇒ Man-in-the-Middle (MITM) attack occur when an attacker intercepts and potentially alters communication between two parties without their knowledge.

- Attacker can capture or manipulate the transmitted data by positioning themselves between send & receiver.

Types of MITM attack

① Email hijacking.
↳ Email hijacking is a type of cyber attack where an attacker gains unauthorized access to an email account. This can be achieved through phishing, credential theft, or exploiting security vulnerabilities.

② Wi-Fi Eavesdropping.
↳ Attackers set up rogue wi-fi network or intercepts traffic on public wi-fi networks to capture unencrypted data. For example! using a fake wi-fi network named to lure user.

③ Session hijacking.
↳ Attacker steal session cookies or tokens to take over an active user session, gaining unauthorized access. For example! Intercepting cookies from a web session.

④ SSL Stripping!
↳ Attacker downgrade HTTPS connections to HTTP, making the data transmitted between the user and the website unencrypted if accessible. For eg. redirecting user from HTTPS site to HTTP site for capturing sensitive data.

⑤ DNS spoofing (DNS cache poisoning)

↳ Attacker corrupt DNS cache entries to redirect users from legitimate websites to malicious ones. For example redirecting users to fake site by corrupting DNS cache

⑥ MITB (Man-in-the-Browser).
↳ Attacker use malware installed in the victim's browser to intercept and alter communication between the user and web application. For example, a Malware alters data in web transaction; like changing bank transfer details.

⑦ Bluetooth spoofing:
Attacker sets up a fake Bluetooth device to intercept data between paired devices.

Covert channel

A covert channel is a method used to transfer information in a way that is not intended or is hidden from regular monitoring or detection systems. It exploits unintended or unauthorized means to transmit data, often bypassing security measures.

Covert channels can pose significant security risks, particularly in environment where data confidentiality and integrity are paramount, as they can be used to filtrate sensitive information or execute unauthorized communication between system.

Types of covert channel.

(1) Storage channels:
There channel communicate by modifying the storage location ; Unused fields in communication protocols like TCP/IP stack can be used as storage channel.

(2) Timing channels.
Attackers use these channels to modify the system resources and send messages over a set period, "Interpacket delay refer to the delay between the transfer of continuous data packet.

How covert channels are created

- Creating a covert channel is complicated and requires advanced level of programming.

- The entity creating the channel must also have access to the file system.

- The main ways covert channels are created are through viral infection or programming efforts by someone with admin access to the system.

Unit 7 Database security

Database security refers to the range of tools, controls, and measures designed to protect databases from unauthorized access, attacks, theft and misuse. It include access control, encryption, auditing, backup and recovery and compliance with legal and regulatory requirement. The goal is to ensure the data is only accessible to authorized user and application.

Security Requirement

A security requirement is a rule or guideline that tells you what needs to be done to keep something safe. It is important for protecting system and data from being hacked or misused.

Some security requirements are given,-

① Reliability:
- work properly, available when needed and handle failures without data loss.

② Integrity.
- Accurate, consistent and protected from unauthorized access.

- Confidentiality.
  - Only authorized user can access data.
- Availability.
  - Have minimum downtime, with backup ready for recovery.
- Authentication
  - Ensure user that they are who they claim to be
- Audit & Logging.
  - Track and record all database activities for monitoring and trouble shooting.
- Compliance
  - Ensure that database meets legal and regulatory standard for data protection.

Reliability and Integrity.

Reliability ensures that the database operates correctly and is always accessible when needed, with the ability to handle failure or errors without losing data. This means the

system consistently provide accurate results, has minimal down time and can recover from issues without compromising the integrity of data.

Integrity

It ensures that the data within the database is accurate, consistent and protected from unauthorized modification. It focuses on maintaining the correctness and trustworthiness of data, ensuring that only authorized changes are made, and that the data remains consistent across the entire system.

Sensitive data:

- Sensitive data refers to information that must be protected due to its confidential nature. If exposed or accessed by unauthorized individuals, it could lead to privacy violation, financial loss or hard to individuals or organizations. It requires strong security measures such as encryption, access control, and regular monitoring to prevent misuse.

For example: Name, address, social security number, credit card or bank account number, etc.

Inference.

- Inference refer to the process of drawing conclusion or making assumptions based on available information or data. In database, protecting against inference means ensuring that even if data is combined or analyzed, it does not lead to the exposure of sensitive information. In context of data security, inference involves.

- Predicting or Extrapolating.

Using existing data to make prediction or derive insight that were not explicitly provided.

- Identifying pattern.

Analyzing data to find pattern or correlation that might reveal sensitive information or lead to unintended conclusions.

- Risk of disclosure,

It occur through data breaches, improper access control, or combining datasets in ways that reveal hidden details.

Multilevel database

A multilevel database is a type of database system designed to support multilevel of access and control, allowing different users or groups to view or interact with the data according to their access right. They are used to enhance security and manage access in complex systems where different users need varying levels of data visibility and interaction. This can include:

* Hierarchical levels:
Organizing data in a hierarchy - where different levels of access are granted based on user roles or security clearance.

* Security policies.
Implementing policies to ensure that users only access data appropriate for their level, often seen in military or government application.

* Seperation of Data.
Maintaining different data layers or views, such as confidential data at a higher level and general data at a lower level, to prevent unauthorized access.

Proposal of multilevel security.

(i) Establish security level and classificate.
(ii) Implement access control mechanism.
(iii) Develop and enforce access policies.
(iv) Enhance Data protection measures.
(v) Audit and monitoring.
(vi) Regular review and updates.
(vii) Conduct user training and awareness program

Security in network refers to the measures and protocols implemented to protect, data, resources and communication within a network from an unauthorized access, misuse and threats. Network security also provide a variety of tools and practices such as firewalls, encryption, intrusion detection system (IDS), and access control, to defend against potential attacks like hacking, malware and data breaches.

* Threats in Network.

Threats in network are dangers that can compromise the security, functionality and integrity of a network and its data. They targets the network's infrastructure, communication channel, and data aiming to disrupt services, steal information or cause damage. Some common threats of network include;

① Malware :
- Malicious software such as viruses, worms, Trojan and ransomeware that can infect and damage system within a network.

⑪ Man-in-the-Middle (MITM) attack.
- An attacker intercepts and alter communication between two parties without their knowledge.

③ SQL Injection:
A code injection technique where an attacker exploits a vulnerability in a web application's database layer by inserting malicious SQL code

④ Brute Force Attacks:
Repeatedly trying different combination of passwords or encryption keys to gain unauthorized access to a network or system.

⑤ Zero-Day Exploits:
An attack that exploits a previously unknown vulnerability in software or hardware before the vendor has released a patch.

Network Security Control

"Network security control are measures and mechanism put in place to protect network and its data from unauthorized access, attack and other security threats. These controls are designed to ensure the confidentiality, integrity and availability of network.

Types of network security control

1) Preventive Controls:
Block threats before they happen (eg. firewall, encryption).

2) Detective Controls:
Identify and alert on security incident (eg. intrusion detection system, SIEM).

3) Corrective Control:
Respond to and mitigate threat (eg. intrusion prevention system, patch management).

4) Deterrent Control.
- Discourage security breaches (eg. security policies, warning banners).

5) Compensating Control:
provide alternative protection when primary control are inadequate (eg. network segmentation, redundancy).

6) physical control:
protect the physical infrastructure (eg. locks, surveillance cameras).

Architecture

The architecture of network security involves designing and implementing a framework to protect network infrastructure and data from breaches and other security threats. It includes:

(i) Perimeter security.
→ Firewalls and DMZs to filter traffic and protect the network boundary.

(ii) Internal security.
→ Network segmentation and intrusion detection systems to monitor and isolate threat.

(iii) Access control.
→ Authentication and role-based access to restrict unauthorized access.

(iv) Data security:
→ Encryption and data loss prevention (DLP) to protect sensitive data.

(v) Monitoring and Response:
→ SIEM systems and incident response plans for detecting and responding to threats.

(vi) Endpoint security.
Antivirus and EDR - to secure devices connected to the network.

(vii) Cloud security.
VPN and CASBs - to secure cloud resources.

Encryption

In network security, encryption is a tool that protect your data by turning it into a code that only someone with the right key can read. This means if someone tries to intercept your information like during online banking or sending an email, they won't be able to understand it without the key.

Uses of encryption.

→ Protect data sent over the internet

→ Secure stored data.

→ Secure remote connections.

Date
Page

Content Integrity

Content integrity refers to the accuracy, consistency and reliability of data or information throughout its lifecycle. It ensures that data has not been altered or tampered with during transmission or storage. Organizations can make accurate decisions and protect against data breaches. If the data remains reliable and unaltered.

Strong Authentication

Strong authentication means using more than one method to prove your identity when accessing a network or system. This goes beyond just a simple username and password by adding additional layer of security. This makes it much harder for anyone else to access your account, even if they know your password.

Key elements of strong authentication.

1. Multifactor Authentication.
2. Two-factor Authentication
3. Public key Infrastructure
4. Bio-metric Authentication.

Access control

Access control is a data security process that enables organizations to manage who is authorized to access corporate data and resource. Secure access control uses policies that verify user are who they claim to be and ensures appropriate control access levels are granted users. It is categorized into two types based on how accessed is managed.

Physical Access Control.

physical access control restricts access to physical spaces, such as buildings, rooms or other areas where sensitive assets are stored.

Types of physical Access control.

- Key cards / Badges.

  Access is granted using key cards or badges, which are swiped or tapped at a reader to unlock doors.

- Bio-metric systems.

  Access is controlled using bio metric data, such as fingerprints, facial recognition, iris scans, etc.

- Locks and keys.
  Traditional method where physical keys are used to lock and unlock doors.
- Surveillance Cameras:
  While not directly controlling access, cameras are used to monitor and deter unauthorized physical entry.

② Logical Access control.
→ It restricts access to digital resources, such as computer system, network, files and data.

Types of logical access control

① Passwords and PINs.
The most basic form of logical access control, where users enter a password or personal identification number to gain access.

② Two-factor Authentication (2FA)
Requires users to provide two forms of identification before access is granted, sometime the password and sometimes one time code (OTP) in mobile device.

*Firewalls:
Regulates network access by controlling incoming and outgoing traffic based on predefined security rules.

- Access Control Lists:
Used to define users or system who has ~~gro~~ of access to objects, such as file or directories on a computer.

Wireless network security

It refers to the measures and practices designed to protect wireless network and the devices connected to them from unauthorized access and data breaches. It is a subset of network security that ads protection for a wireless network.

There are 4-types of wireless network security they are WEP, WPA, WPA2 and WPA3, the latest ones with increasing levels of security. While WPA2, which uses AES encryption, is commonly used, WPA3 provides additional security features such as stronger encryption and attack defenses. These protocols determine the users and device's access level.

Honeypots

A honeypot is a network attached system used as a trap for cyber-attackers to detect and study the tricks and types of attacks used by a hacker. Honeypots are mostly used by large companies and organizations involved in cyber security. It help cyber security researchers to learn about the different types of attacks used by attackers. It is a fake system or network designed to look like a real one, but its purpose is to lure in attackers.

Types of Honeypots

① production Honeypots:
Act as decoy in real network to distract hacker.

② Research Honeypots:
Used by experts to study hacker techniques and cyber threats.

③ Pure Honeypot:
- Large systems that closely monitor all hacker activity

④ Malware Honeypots:
Attract malware to study how viruses or worms behave.

⑤ Spam Honeypot
collect and analyze spam emails or bots to improve anti-spam defenses.

Traffic Flow Security:

Traffic flow security refers to technique used to hide or disguise the patterns of data moving across a network. Even if an attacker can't read the data, they might still learn something by watching how much data is being sent, when it's being sent or to whom.
To prevent this, traffic flow security methods mix up or hide these patterns by:

① Adding fake traffic.
- Sending extra meaningless data to confuse observers about how much real data is being sent.

④ Delaying data:
- Randomly delaying messages so it's harder to figure out the timing of the communication.

⑤ Splitting traffic:
Breaking message into smaller pieces and sending them over different routes to hide the full picture.

⑥3 Firewalls

A firewall is a security system that monitor and control the incoming and outgoing network traffic based on predefined rules. It acts like a barrier between a trusted internal network and an untrusted external network, blocking or allowing traffic based on security settings. It helps to protect computers and networks from unauthorized access, malware and cyber attack.

Date
Page

Design and Types of Firewall.

Firewall Design principle

- Designing an effective firewall strategy requires careful consideration of various principle: such of them are:

① Defense in Depth.

Employing multiple layers of security ensures that even if one layer is breached, others remain intact.

② This principle reduces the risks of a single point of failure compromising the entire network.

③ Default deny

This minimizes the attack surface and ensures that only necessary and trusted traffic is permitted.

④ Regular updates:

- Keeping rules sets and firmware up to date ensures that emerging vulnerabilities are addressed promptly.

(v) Testing and Validation
— Conduct regular security assessments and firewall rule review to validate the effectiveness of firewall configuration, and ensure compliance with security policies and regulatory requirements.

Types of firewall.

(1) Packet filtering Firewalls.
— Filters traffic based on basic information like IP addresses and port number. It blocks or allow data packets based on predefined rules. It is simple and fast; but does not check data content. For example:
A packet filtering firewall may be configured to block incoming traffic on port 80 (HTTP) to prevent unauthorized access to web services

(2) Stateful Inspection Firewall.
— It tracks the state of active connection and decides whether to allow or block packets based on the context of

a connection. For example: A Stateful inspection firewall monitors TCP connection ~~3. Proxy Firewall~~ ensuring that incoming packets belong to established, legitimate session.

3. Proxy Firewalls
- It acts as an intermediary between users and the internet. Instead of direct communication, the proxy handles all requests, checking for security. Very secure because it checks all data in detail, but it can slow things down. For example,
- A web proxy firewall intercepts and inspects web requests from clients.

4. Next-Generation Firewalls. (NGFW).
- It combines traditional firewall features with more advanced features like deep packet inspection, intrusion prevention and malware detection. For example,
- An NGFW inspects not only packet headers but also packet payloads to detect and block advanced threats such as zero-day exploits and malware

Personal Firewall.

A personal firewall is software designed to protect a single computer or device from unauthorized access. It monitors and controls the data coming in and going out of your device based on security rules. They are often used on home computers and personal devices to block unwanted connections, like hackers or malware trying to enter.

Features of personal firewall.

→ Easy-to-use interface
→ Make device less visible to external scans.
→ Alerts users to suspicious activity
→ Integrate VPN for secure internet access
→ provide real time notification for blocked attempts.
→ Allows users to set their own security preferences.

Date
Page

Intrusion detection system and its types.

An intrusion detection system (IDS) is a security tool that monitors a computer network or systems for malicious activities or policy violations. It monitors the traffic on a computer network to detect any suspicious activity. It analyze the data flowing through the network to look for pattern and sign of abnormal behavior. If the IDS detect something that matches one of these rules or patterns, it sends an alert to the system Administrator. The system Administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Types of IDS

① **NIDS: (Network Intrusion Detection System).**
→ It is a security solution that monitor and analyzes network traffic for sign of malicious activity or policy violation. NIDS alerts network administrator when suspicious activities are identified, helping to protect the network from unauthorized access and cyber attacks. For example

"NIDS is installing it on the subnet where firewalls are located. in order to see of someone is trying to crack the firewall.

(2) HIDS ('Host IDS).

- HIDS is a security tool installed on individual devices, like computers or server. to monitor and protect them from unauthorized access and malicious activities. An example of HIDS usage can be seen on mission critical machines. which are not expected to change their layout.

(3) PIDS (Protocol Based IDS).

A PIDS monitors and analyzes specific network protocol. to detect unusual or malicious activity. It focuses on ensuring that the communication between system follows proper protocol rules and does not contain any suspicious behavior. It can detect attacks that exploits weaknesses in these protocols.

(4) APIDS (Application protocol Based IDS).

↳ An APIDS is a system or agent that generally resides within a group of servers. It identifies the intrusion by monitoring and interpreting the communication on application specific protocol. For example: this would monitor the SQL protocol explicitly to the middleware as it transacts with the database in the web server.

IPS (Intrusion prevention system).

↳ An IPS is a security tool that monitor network traffic to detect and prevent cyber threats. Unlike an IDS, IPS takes an immediate action to block or stop attacks in real time. It works by analyzing network traffic in real time and comparing it against known attack pattern and signatures. When the system detect suspicious traffic; it blocks it from entering the network.

Types of IPS:

(1) Network Based IPS
(2) Host Based IPS.

① Network-Based IPS:
→ It is installed at the network perimeter and monitors all traffic that enters and exits the network. It monitors the entire network for suspicious traffic by analyzing protocol activity.

② Host-Based IPS
→ It is installed on individual hosts and monitors the traffic that goes in and out of the host. It is also an built software package which operates a single host for doubtful activity by scanning events that occurs within that host.

6.4) Email security.
Email security is the process of preventing email-based cyber attacks and unwanted communications. It spans protecting inboxes from takeover, protecting domains from spoofing, stopping phishing attack, preventing fraud,

Date
Page

, blocking malware delivery, filtering spam and using encryption to protect the content of emails from unauthorized persons. Security and privacy were not built into email when it was first invented.

PGP (Pretty Good Privacy).

PGP is a method used to encrypt emails, ensuring only the intended recipient can read them. It uses a combination of public and private keys for encryption and decryption. It also provides digital signatures to verify the identity of the sender and ensure the message hasn't been altered. It's popular because it offers strong encryption. but user need to manually share their public keys.

S/MIME

Secure / Multipurpose Internet Mail Extension is another standard used to encrypt and digitally sign email. It uses certificates for encryption

and authentication. It is widely supported by email clients like outlook and Apple Mail and works automatically if the sender and recipient have certificates. It ensures confidentiality and authenticity. It relies on trusted certificate Authorities.

Transport Layer Security (TLS)

Different from PGP and S/MIME, TLS is an encryption protocol used to secure network communication. This includes securing web browsing, email and transferring files. This functions as a way to protect any transfer of data between two end points devices. TLS is regarded as the successor to SSL; together there are two of the most popular encryption protocols available to users and businesses.

Security administration refers to the management and protection of an organization's security. It involves using methods and policies designed to safeguard data, networks and systems from unauthorized access and threats. It includes tasks such as setting up and maintaining security protocols, monitoring systems for vulnerabilities; managing user access rights, enforcing security policies and responding to security incidents. Security administrator ensure the protection of data, network and IT system, maintaining integrity, confidentiality and availability.

Security Administrator.

A security Administrator is a professional responsible for implementing, managing and monitoring an organization security measures to protect its information systems, networks and data from security threats.

Skills and Qualification of Security Administrator.

→ Technical knowledge related with the use of security tool and software to protect system.

→ Ability to look at problem and figure out what went wrong with security.

→ Good at explaining security rules and procedure to others.

→ Skilled in fixing security issues and responding to threats quickly.

→ Careful about monitoring systems and following security rules.

→ Aware of laws and rules about data protection.

Security planning.

Security planning is the process of figuring out how to protect an organization important information and assets from potential threats or risks. It involves creating a plan that outlines what needs to be done to keep everything safe.

Necessity of security planning

→ Helps the organization to avoid security issues before they happen.

→ keeps sensitive data and resources safe.

→ keeps the organization running.

→ keeping up with evolving regulations can be challenging.

→ Balancing security and ease of use.

Risk Analysis

Risk analysis is the process of figuring out what could be go wrong in a project or a business and how seriously those problems could be. It helps organization prepare for unexpected events. It help business avoid surprises and stay on track with their goals.

Common Tools and Techniques

① SWOT Analysis

— Identifies strengths, weaknesses, opportunities and threats,

② Risk Matrix:
A visual tool that categorizes risks based on their likelihood and impact.

③ Scenario Analysis:
Explores different scenarios to asses potential risks and responses.

Organizational security polices

- They are formal documents that outline an organizations approach to managing security risks and protecting it's assets, information and people. These polices help establish a framework for maintaining security and ensure everyone in the organisation understands their roles and responsibilities.

Importance of security polices.

→ Help to keep important data safe from threats.

→ Makes sure it meet legal and regulatory requirements, avoids penalties.

→ Reduces the risk of costly security incident and recovery effort.

→ Promotes awareness among employees regarding security issues.

→ Define roles and responsibilities, ensuring everyone knows their part in security.

Common types of security policies

① Acceptable Use policy:
- Defines acceptable behavior for using company resources like computers and internet access.

② Data protection policy:
- Outlines how to handle, store and share sensitive information securely.

③ Incident response policy:
- provides guidelines for responding to security incidents and breaches effectively.

(4) Access control policy:
- Specified who can access specific information and systems and what access is granted.

(5) physical security policy.
- Covers measures to protect physical premises, including access control & surveillance.

(6) Password policy:
Establishes rules for creating, managing and changing passwords to enhance security.

(7) Email security policy:
- Outlines practices for safely using email to prevent phishing and malware attacks.

(8) Remote work policy:
- sets security standards for employees working from home or outside the office.

(9) Mobile device poly:
Define rules for using personal and company mobile devices, focusing on data security.

Date
Page

Physical Security.

Physical security refers to the protection of people, property and physical assets from action that could result in damage, theft or harm. It involves strategies, policies and measures to safe guard facilities, equipment, resources and individuals against unauthorized access, misuse or destruction. The physical security framework is made up of three main components: access control, surveillance and testing.

1) Access control:

Managing who can enter and leave a facility. This involves using systems like key, cards, security codes or biometric scans to ensure only authorized individuals can access certain areas.

2) Surveillance:

Monitoring activities using cameras (CCTV), motion detectors and alarm systems. This helps detect and record any unauthorized behavior or suspicious activities.

② physical barriers:

Using physical structure like fences, gates, walls, locks and doors to prevent unauthorized access and protect sensitive areas. These barrier create layer of protection that make it harder for intruder to get in and easier to control who has access.