Information Security

Module 1 : Introduction.

★ Vulnerability is a weakness that could be exploited to cause harm.

★ Threat is a set of circumstances that could cause harm.

★ Controls prevent threats from exercising vulnerabilities

★ Security Triad:-

CIA Triad: {
Availability - used by authorised parties.

Intregrity - modified only by authorised parties

Confidentiality - viewed only by authorised parties.

Authenticity - ability of a system to confirm the identity of a sender.

NonRepudiation or Accountability - ability of a system to confirm that a sender cannot convincingly deny having sent something.

★ Threats

Threats are caused both by humans and other sources.

Page No.
Date

Types of Threats.

1] Natural Causes – fire, power failure etc.

2] Human Causes – i] Benign intent – Errors.
ii] Malicious intent
- Random (any website)
- Directed. (Impersonation)

Advanced Persistente Threat (APT)

Type of attack carried out by organised, skilled, and well-financed groups often supported by the governments. They carefully plan their attacks, stay hidden for a long time, target only specific groups or companies. Uses smart tricks such as spear phishing. Once they gain access they quietly steal the information over time.

☆ Types of Attackers.

- Terrorist groups
- Hackers
- organised Criminal member /group
- Hired Criminal
- Cyber Criminal Groups.

★ Harm

Negative consequence of a threat is Harm.

Types of Harms & Attacks :-

1] Interception :- Attack on confidentiality
2] Interruption :- Attack on availability.
3] Modification :- Attack on integrity
4] Fabrication :- Attack on Authenticity

★ Control

Means to counter threats.

Method - Opportunity - Motive
(how) (when) (why)
Deny any of these to the attacker, the attack will not succeed.

Methods of Defense / Control Measures :-

1] Prevent - block the attack
2] Deter - make the attack harder
3] Deflect - make another target more attractive
4] Mitigate - making its impact less severe
5] Detect - when it happens
6] ~~Reflec~~ Recover - from its effects.

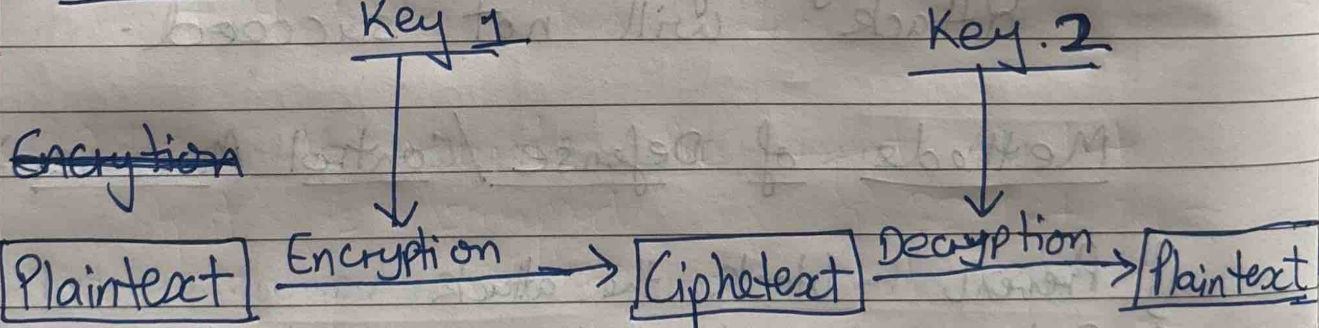
★ Encryption Terminology :-

Sender
Recipient
Transmission Medium
Interceptor / intruder
Encrypt / Encode / Encipher
Decrypt / Decode / Decipher
Cryptosystem
~~Par~~ Plaintext & Ciphertext

History of Encryption

Transposition → Caeser → Frequency Analysis → Polyalphatic → Jefferson Wheel → Enigma Machine → Cryptologic Bombe → DES (Data Encryption Standard)

Process



Symmetric – when Key 1 & Key 2 are same

Asymmetric – when Key 1 is the encryption key & Key 2 is the decryption key and both of them are different

★ Stream VS Block Ciphers:

Stream	Block.
• Each byte of data stream is encrypted separately	Encrypts a group of plain text symbols as a single block
• Low Diffusion	High Diffusion
• Susceptible to malicious insertions & modifications	Immune to insertion of symbols.
• Low Error propogation	Padding & Error propogation
• Speed of transformation	Slowness of Encryption

Diffusion hides relationship between the cipher text and the plaintext

Confusion hides the relationship between the ciphertext & the key.

☆ DES : Data Encryption Standard Algorithm.

Symmetric Block Cpher

Input key length = 64 bits

Final output Key = 64 bits.

Main key = 64 bits.
Subkey = 56 bits
Round Key = 48 bits

No. of Rounds = 16 rounds

Step1 :-

Initial Permutation ⇒ 64 bits input plain teact as the input, permutation happens & 64-bit output to the Round 1!

Step2 :- After 16 rounds, the ~~input~~ 64 bits output is swapped in a 32-bit swapper that swaps left 32-bits and right 32-bits.

Step3 What happens in each round ?

The 64-bit and divided into left & right 32 bits, then permuted ~~&~~ with the subkey to generate 48 bits round key.

The initial 64 bits input is also divided into left 32 & right 32 bits.

The 32 bits is then expanded to 48 bits in the Expansion P-box.

Then this 48 bits is XOR with 48-bit round key (Whitener)

Then this 48bits is acts as the input for S-boxes to do the real mixing i.e confusion. In this S-boxes there are 8 S-Box each with a 6-bit input and a 4-bit output; to total it to 32-bits.

~~Then this~~

This 32 bits is transpositioned in the P-Box

Then the output is XOR~~ed~~ with the left 32 bits again.

After this step we get our final right side 32 bits.

Strength of DES

- Timing attacks
- Analytic attacks

Weakness of DES

① Key Size (56 bits very easy to hack) ∴ Uses 3 DES
② Semiweak/Weak/Possible Weak keys.
③ Key Clustering

~~DES~~	DES	AES.
- Date designed	1976	1999
- Block Size	64 bits	128 bits
- Key length	56 ~~bits~~ bits	128, 192, 256 bits
- Operations	16 rounds	10, 12, 14 rounds, can be increased
- Encryption primitives	Substitution, permutation	Substitution, shift, bit mixing.
- Cryptographic primitives	Confusion, Diffusion	Confusion, ~~Diffu~~ Diffusion
- Design	Open	Open
- Design Rationale	~~Open~~ Closed	open
- Selection Process	Secret	Secret, but open to criticisms & comments

☆ Public Key Cryptography

Assymmetric Keys - i.e two keys;

① public key : encrypts messages, verify signatures.

② private key: only to ~~recip~~ recipient, decrypts messages and signs (creates) signatures.

Page No.
Date

Why ?

To address two issues :- ① Key distribution
② Digital Signatures

Applications

- Provides secrecy - effective encryption/decryption
- Provides authentication - through digital signatures
- Key exchange of session keys.

☆ Man - in - the - middle attack. (T B).

☆ Error - detecting codes. (EDC)

Simple :- Parity checks
Cyclic Redundancy checks.

Cryptographic EDC :- ① One-way hash function
② Crypographic Checksum
③ Digital Signatures.
④ Trust Certificates.

① One-way hash function

Function converts data into fixed-size value
Easy to compute
Impossible to reverse
Ideal for detecting changes in data.

2] Cryptographic Checksum

- Hash value encrypted with a secret key
- Ensures data integrity
- Prevents attackers from altering both data & verification code.

3] Digital Signatures

Cryptographic technique used to ensure the authenticity, integrity, non-repudiation and non-reusability

Key Components :- ① Original File
② Hash Code
③ Signer Identity - signs the file.
④ Encrypted Hash (Signature) - message authenticated by senders private key, proving authenticity.
⑤ Public Key Verification - decrypts using senders public key

Widely used for verifying softwares, secure communications, legal documents in digital form.

Efficiency - only hash is encrypted

~~Confidentit~~

Confidentiality - encrypted with symmetric key, which itself is encrypted with recipients public key.

4] Digital Certificates

- Electronic credentials used to verify ownership of the public key.
- Public key ~~is~~ and users identity are bound together in a certificate.
- A certificate authority (CA) issues and signs the certificate after verifying the identity of the requester.
- Certificates use digital signatures & hash functions to ensure authenticity & integrity
- Enables secure digital communication
- Chain of trust is formed when a certificate is signed by a higher authority (CA).