Module 1

Cryptography

An original message is known as plain text, while the coded message is called the ciphertext.

The process of converting from plaintext to ciphertext is known as Enciphering or Encryption.

Restoring plaintext from ciphertext is deciphering or decryption.

Many schemes used for encryption constitute the area of study known as Cryptography. Such a scheme is known as a cryptographic system or a cipher.

Techniques used for deciphering a message without any knowledge of the enciphering details fall into the area of cryptanalysis.

Cryptanalysis is what layperson calls 'breaking the code'. The areas of cryptography & cryptanalysis together are called cryptology.

Cryptography, a word with Greek Origin, means SECRET WRITING.

We use the term to refer to the science & art of transforming messages to make them secure & immune to attacks.

A MOTHER Product

Although in the past cryptography referred only to the encryption & decryption of messages using secret keys.

Now, it is defined as involving three distinct mechanisms.

→ Symmetric-key encipherment
→ Asymmetric-key encipherment
→ hashing.

Symmetric key Encipherment

- also called Secret key Encipherment or Secret key cryptography. share this common key
- It uses Single Secret key for both encryption & decryption
- Encryption / decryption can be thought of as electronic locking.
- In this, Alice puts the message in a box & locks the box using shared secret key. Bob unlocks the box with the same key & takes out the message

Encryption: $C = E_K(P)$ — done by Sender

decryption: $P = D_K(C)$ — done by Receiver

Asymmetric key Encipherment

* also called public key encipherment/cryptography
* first, there are two keys instead of one:
  - one public key — user receives public key to encrypt.
  - one private key
* To send a secured message to Bob, Alice first Encrypt the message using Bob's public key.
* To decrypt the message, Bob uses his private key.

Send to everyone, then uses private key of sender & receiver decrypt the msg using public key of sender.

Hashing

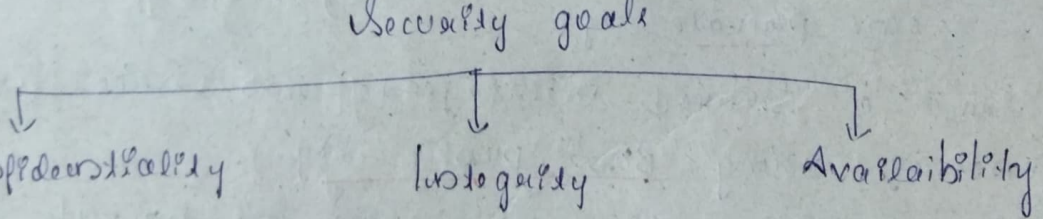
- In hashing, a fixed length message digest is carried out of a variable length message.

- The digest is normally much smaller than the message.
- To be useful, both the message & digest must be sent to Bob.
- Hashing is used to provide checkvalues, to verify the data integrity.
  - cannot retrieve original msg from message digest
  - change made in I/P value, it make drastic change in msg digest.

STEGANOGRAPHY

→ It means "Covered writing"
→ Cryptography means concealing the content of a message by enciphering.
→ Steganography means concealing the message itself by covering it with something else

SECURITY GOALS (CIA)



Confidentiality

done using encryption

* It not only applies to the storage of the information it also applies to the transmission of information.
* When we send a piece of information to be stored in a remote computer or when we retrieve

a piece of information from a remote computer, we need to conceal it during transmission.

Eg: In banking,

customer's account need to be kept Secret.

Integrity

done using hash Algorithm

- Integrity means that changes need to be done only by authorised entities & through authorised mechanisms.
- Integrity violation is not necessarily the result of a malicious activity.
- An interruption in the s/m, such as a power surge, may also create unwanted changes in some information.
- Eg: Info needs to be changed constantly. In a bank, when a customer deposits / withdraws money, balance of her account need to be changed.

Availability

- The third component of Info Security is availability.
- The info created & stored by an organisation to be available to authorised entities.
- Information is useless if it is not available.
- The unavailability of info is just as harmful

for an organisation as the lack of confidentiality or integrity.

Eg: What would happen to a bank if the customers could not access their accounts for transactions?

Although CIA triad define Security Objectives, Some in the Security field feel that additional concepts are needed to present a complete picture. Two of them are
* Authenticity
* Accountability.

Authenticity :-

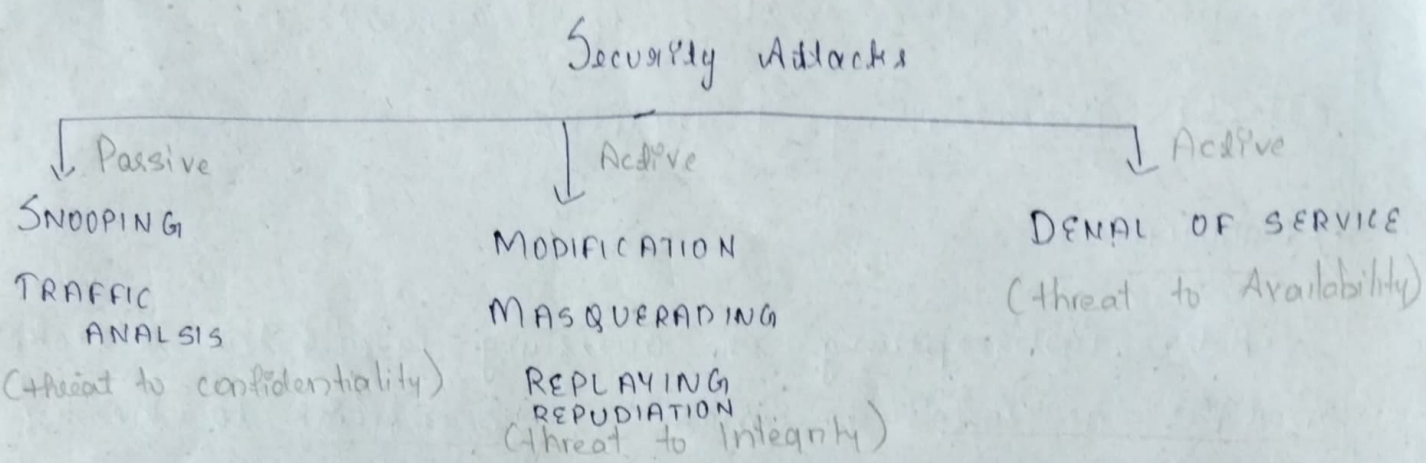
The property of being genuine & being able to be verified & trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are & that each input arriving at the s/m came from a trusted source.

Accountability :-

The Security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

ATTACKS

• Goals of Security can be threatened by Security attacks.



attacks threatening confidentiality

1) Snooping

• It refers to unauthorised access to or interception of data.

• A file transfered through the internet may contain confidential information.

• An unauthorised entity may intercept the transmission & use the contents for her own benefit.

• To prevent snooping, the data can be made non intelligible to the interceptor by using encipherment techniques.

2) Traffic Analysis

> Although encipherment of data may make it non intelligible for the interpreter, she can obtain some other type information by monitoring online traffic.

> Eg, she can find the email address of the sender or the receiver.

> She can collect pairs of requests & responses to help her guess the nature of transaction.

Attacks threatening Integrity

1) MODIFICATION

• After intercepting or accessing info, the attacker modifies the info to make it beneficial to herself.

• Eg, customer sends a message to a bank to do some transaction.

• The attacker intercepts the message & changes the type of transaction to benefit herself.

• Sometimes the attacker simply deletes or delays the message to harm the system or to benefit from it.

2) MASQUERADING

* Masquerading or Spoofing happens when the attacker impersonates somebody else.

* Eg: an attacker might steal the bank card & PIN of a bank customer & pretend that she is that customer.

* Sometimes the attacker pretends instead to be the receiver entity.

* Eg, a user tries to contact a bank, but another site pretends that it is the bank & obtains some information from the user.

3) REPLAYING

- The attacker obtains a copy of a message sent by a user & later tries to replay it.
Eg: a person sends a request to her bank to ask for payment to the attacker, who has done a job for her.
- The attacker intercepts the message & sends it again to receive another payment from the bank.

4) REPUDIATION

> This type of attack is different from others because it is performed by one of the two parties in the communication: the sender or receiver.
> The sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.
> eg: of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request.
> An example of denial by the receiver could occur when a person buys a product from a manufacturer & pays for it electronically, but the manufacturer later denies having received the payment & asks to be paid.

Attacks threatening Availability

1) Denial of service

• DoS is a very common attack.

It may slow down or totally interrupt the service of a system.

- The attacker can use several strategies to achieve this.
- She might send so many bogus requests to a server that the server crashes because of the heavy load.
- The attacker might intercept & delete a server's response to a client, causing the client to send requests many times & overload the s/m.

Passive Vs Active Attacks

PASSIVE ATTACKS

* Attacker's goal is just to obtain information, i.e, the attack does not modify data or harm the system.
* The s/m continues with its normal operation. However, the attack may harm the sender or receiver of the message.
* Attacks that threaten confidentiality, snooping & traffic analysis are passive attacks.
* Revealing of the information may harm the sender or receiver of the message, but the s/m is not affected. For this reason, it is difficult to detect this type of attack until the sender or receiver finds out about the leaking of confidential info^{n}
* Passive attacks can be prevented by encipherment

ACTIVE ATTACKS

* An active attack may change the data or harm the s/m.

* Attacks that threaten the integrity & availability are active attacks.

* Active attacks are normally easier to detect than to prevent, because an attacker can launch them in a variety of ways.

Attacks	Passive/Active	Threatening
SNOOPING TRAFFIC ANALYSIS	PASSIVE	CONFIDENTIALITY
MODIFICATION MASQUERADING REPLAYING REPUDIATION	ACTIVE	INTEGRITY
DENIAL OF SERVICE	ACTIVE	AVAILABILITY

dialogs → open the interconnection

OSI SECURITY ARCHITECTURE

* The OSI security architecture focuses on
  1) Security attacks
  2) Security mechanism
  3) Services.

* SECURITY ATTACKS : Any action that compromises the security of info owned by an Organization.

* SECURITY MECHANISMS : A process that is designed to detect, prevent or recover from a security attack.

* SECURITY SERVICE : A processing or communication service that enhances the security of the data processing s/m & the info transfers of an org.

The services are intended to counter security attacks & they make use of one or more security mechanisms to provide the service.

→ To assess effectively the security needs of an organisation & to evaluate & choose various security products & policies, the manager responsible for security needs some systematic way of defining the requirements for security & characterising the approaches to satisfy those requirements.

→ This is difficult enough in a centralised data processing environment; with the use of local & wide area networks, the problems are compounded.

Following provides definitions taken from RFC 4949 (Request for comments)

* Threat : A potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security & cause harm i.e, a threat is possible danger that might exploit a vulnerability.

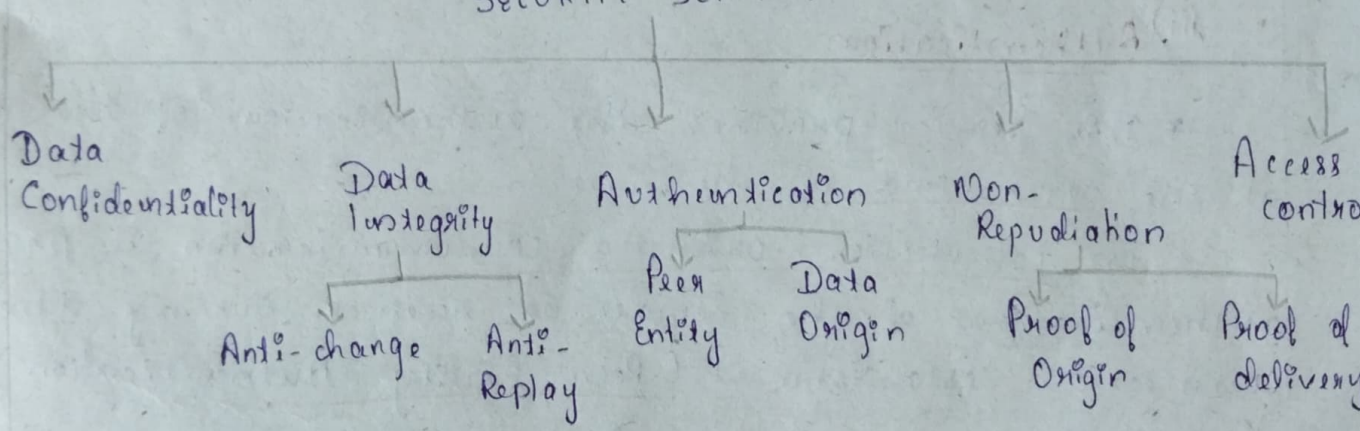
* Attack : An assault on s/m security that derives from an intelligent threat; i.e, an intelligent act that is a deliberate attempt to evade security services & violate the security policy of a s/m.

Security Services and Mechanisms

- The International Telecommunication Union - Telecommunication standardization Sector (ITU-T) provides some Security services mechanisms to implement those services
- Security services & mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.
- A mechanism can be used in one or more services

(1) Security Services

* It is easy to relate one or more of these services to one or more of the Security goals.
* It has been designed to prevent the Security attacks



i) Data Confidentiality

- It is designed to protect data from disclosure attacks
- Service as defined by X.800 is very broad & encompasses confidentiality of the whole message or part of a message & also protection against traffic analysis.
- It is designed to prevent snooping & traffic analysis attack.

ii) Data Integrity

- It is designed to protect data from
  * modification * insertion
  * deletion * replaying by an adversary
- It may protect the whole or part of the ~~mech~~ message.
- provide assurance that data received are exactly as sent by an authorised entity.
- It includes
  > Connection Integrity with recovery.
  > Connection Integrity without recovery.
  > Selective-field connection Integrity
  > Selective-field connectionless Integrity
  > connectionless Integrity.

iii) Authentication

* This Service provides the authentication of the party at the other end of the line.
* In connection-oriented communication, it provides authentication of the Sender or receiver during the connection establishment (Peer Entity Authentication)
* In connectionless com^n, it authenticates the source of the data (data Origin Authentication).

iv) non-repudiation

- It protects against repudiation by either the Sender or receiver of the data.
- With Proof of Origin, the receiver of the data can later prove the Identity of the Sender if denied.
- With Proof of delivery, Sender of data can later prove that data were delivered to the intended recipient

v) Access Control

→ Provides protection against unauthorised access to data.

→ The term 'access' in this definition is very broad & can involve reading, writing, modifying, executing programs & so on.

→ provides prevention of unauthorised use of a resources.

→ This service controls who can have access to a resource, under what conditions access can occur & what those accessing the resources are allowed to do.

② Security Mechanisms

Security Mechanisms
- → Encipherment (confidentiality)
- → Data Integrity
- → Digital Signature
- → Authentication exchange
- → Traffic Padding
- → Routing control
- → Notarisation
- → Access control

a) Encipherment

- Encipherment, hiding or covering data, can provide confidentiality.
- Used to complement other mechanisms to provide other services.
- Cryptography & steganography are used for enciphering.

into a form that is not readily intelligible.

- Transformation & subsequent recovery of the data depend on an algorithm & zero or more encryption keys.

b) Data Integrity

→ Data Integrity mechanism appends to the data a short check value that has been created by a specific process from the data itself.

→ Receiver receives the data & the checkvalue.

→ He creates a new checkvalue from received data compares the newly created check value with one recei

→ If two check values are same, integrity of data has been preserved.

c) Digital Signature

> It is a means by which the sender can electronically sign the data & receiver can electronically verify the sign.

> Sender uses a process that involves showing that she owns a private key related to the public key that she has announced publicly.

> Receiver uses sender's public key to prove that the message is indeed signed by the sender who claims to have sent the message.

d) Authentication Exchange

* Here, two entities exchange some messages to prove their identity to each other.

Eg: one entity can prove that she knows a secret that only she is supposed to know.

e) Traffic Padding

• It means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

f) Routing control

→ It means selecting & continuously changing different available routes b/w sender & receiver to prevent the opponent from evasdropping on a particular route.

g) Access Control

> It uses methods to prove that a user has access right to the data or resources owned by a s/m.

> Eg: Proofs are passwords & PINs.

h) Notarization

* It means selecting a third trusted party to control the communication b/w two entities. Can be done to prevent repudiation.

* The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.

* It involves use of trusted third party in communication. It act as a mediator b/w sender & receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

Security Services	Security Mechanism
→ Data Confidentiality	– Encipherment, Routing control
→ Data Integrity	– Encipⁿ, dig. sigⁿ, data integrity
→ Authentication	– Encipⁿ, dig sigⁿ, authⁿ exchange
→ Non-repudiation	– Dig. sigⁿ, data Integrity, notarizⁿ
→ Access control	– Access control mechanism.

Attacks

1) Ransomware
2) Phishing.
3) DoS

① Ransomware

- In recent years, ransomware has quickly become one of the most prevalent types of malware.
- The most common malware variants encrypt a s/m or specific files, pausing any work from being done until the victim pays a ransom to the attacker.
- Other forms of ransomware threaten to publicise sensitive infoⁿ within the encrypted data
- Ransomware is a form of malware that encrypts a victim's file.
- It is used by cyber criminals.
- The attacker then demands a ransom from the victim to restore access to the data upon payment.
- Users are shown instructions for how to pay a fee to get the decryption key.

• It uses asymmetric encryption.

• It uses a pair of keys to encrypt & decrypt a file. The public-private pair of keys is uniquely generated by the attacker for the victim, with the private key to decrypt the files stored on the attacker's server.

• Attacker makes the private key available to the victim only after the ransom is paid, but that is not always the case.

• Without access to the private key, it is nearly impossible to decrypt the files that are being held for ransom.

• The Wannacry ransomware attack was a worldwide cyberattack in May 2017 by the Wannacry ransomware cryptoworm.

• which targeted computers running the Microsoft Windows O.S by encrypting data & demanding ransom payments in the bitcoin crypto currency.

• If a comp or network has been infected with ransomware, the ransomware blocks access to the s/m or encrypts its data.

• Cyber criminals demand ransom money from their victims in exchange for releasing the data.

• In order to protect against ransomware infection, a watchful eye & security s/w are recommended.

• Victims of malware attacks have three option after an infection.

→ pay the ransom
→ Remove malware
→ restart the device.

• Attack vectors frequency used by extortion Trojans include the Remote Desktop Protocol, phishing emails & s/w vulnerabilities.

* It can therefore target both individuals & companies.

defend against Ransomware

* Often org^n can mitigate ransomware attacks by having up-to-date backups.

* If their files become ~~blocked~~ locked, they can simply wipe the s/m & reboot from an offline backup.

* Org^n should train users about the threat, patch their s/w as necessary & install all the usual security soln

Examples of Ransomware malware attacks

> With vendors & org^n increasingly moving online, more data is at risk of exposure.

> Attackers know this & often take advantage of small to mid-sized org^n with weaker n/w security, requesting an amount they know the org^n can afford.

> eg: Cryptolocker, locky, wannacry, Hermes, Grand Crab.

② PHISHING

- Phishing is a type of deception designed to steal valuable personal data, such as credit card numbers, passwords, a/c data or other info^n.

- It is a type of email attack that attempts to trick users into divulging passwords, downloading attachments or visiting a website that installs malware on their sm

- More targeted efforts at specific users or org^n are known as Spear phishing. Because the goal is to trick the user, attackers will research the victim to maximize trick potential, often using spoofing to make the email

seem legit.

- Millions of fraudulent email messages that appear to come from web sites you trust, like your bank or credit card company & request that you provide personal info.
- As scam artists become more sophisticated, so do their phishing e-mail messages & pop-up windows.
- They often include official-looking logos from real org^{n} & other identifying info^{n} taken directly from legitimate web sites.
- Phishing attacks are the practise of sending fraudulent communications that appear to come from a reputable source.
- It is usually done through email. The goal is to steal sensitive data like credit card & login info^{n}, or to install malware on the victim's machine.

defend against phishing

- Because phishing relies on Social Engineering - tricking users into doing something - employee training is one of the best defences against these attacks.
- Users should deploy anti-Spam & anti-malware solutions & staff should know not to divulge personal info^{n} or passwords in email messages.
- Training about downloading attachments or clicking website links in messages, even if they appear to come from a known source, is imperative given phishing attackers often pretend to be a company or person known to the victim.

Phishing malware attacks

1. Deceptive phishing
2. Spear phishing
3. Whaling
4. Vishing
5. Smishing
6. Pharming

① **Deceptive Phishing** : Most common type, using an email headline with a sense of urgency from a known contact. This attack blends legitimate links with malicious code, modifies brand logos, & evades detection with minimal content.

② **Spear phishing** : Spear phishing targets specific users or org^n by exploring social media, recording out-of-office notifications, compromising API tokens & housing malicious data in the cloud.

③ **Whaling** : Even more targeted than spear phishing, whaling targets chief officers of an org^n by infiltrating the n/w, exposing the supply chain & following up the malicious email with a phone call to give it legitimacy.

④ **Vishing** : Targetting victims over the phone, vishing is the use of voice over Internet Protocol (VoIP), technical jargon & ID spoofing to trick a caller into revealing sensitive information.

⑤ **Smishing** : It also targets phone users, but this one comes in the form of malicious text messages. Smishing attacks often include triggering the download of a malicious app, link to data-stealing forms & faux tech support.

⑥ Pharming : Moving away from trying to trick users pharming leverages cache poisoning against the DNS. using malicious email code to target the Server & compromise web user's URL requests.

③ DoS ATTACK

→ A Denial-of-Service (DoS) attack is an attack meant to shut down a machine or n/w, making it inaccessible to its intended users.

→ DoS attacks accomplish this by flooding the target with traffic, or sending it information that triggers a crash.

→ A DoS attack is a malicious attempt to overwhelm a web property with traffic in order to disrupt its normal Operations.

→ DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in DoS to addition users.

→ A DoS attack is characterised by using a single computer to launch the attack.

→ The primary focus of a DoS attack is to over-saturate the capacity of a targeted machine, resulting in DoS to additional requests.

→ The multiple attack vectors of DoS attacks can be grouped by their similarities.

→ DoS attacks typically exploited Security vulnerabilities present in the n/w, s/w & h/w design.

→ These attacks have become less prevalent as DDoS

attacks have a greater disruptive capability & are relatively easy to create given the available tools

→ In reality, most DoS attacks can also be turned into DDoS attack

→ DoS attacks fall in 2 categories:

* Buffer overflow attacks
* Flood attacks

a) Buffer Overflow attacks

- An attack type in which a m/y buffer overflow can cause a machine to consume all available hard disk space, m/y or CPU time.
- This form of exploit often results in sluggish behavior, s/m crashes, or other deleterious server behaviors, resulting in DoS.

b) Flood attacks

- By saturating a targeted server with an overwhelming amount of packets, a malicious ~~atto~~ actor is able to over saturate server capacity, resulting in DoS.
- In order for most DoS flood attacks to be successful, the malicious actor must have more available bandwidth than the target.

Types of DoS Attacks

1. Smurf attack
2. Ping flood
3. Ping of Death