STYUDY MATRIAL

OF

CRYPTOGRAPHY

AND

NETWORK SECURITY

Prepared by
Smt.Archana Tripathy
Sr.Lecturer in CSE
Govt.Polytechnic , Bhubaneswar

Chapter-1

POSSIBLE ATTACKS ON COMPUTERS

1.1 Need for Security

Computer security basically is the protection of **computer** systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your **computer** system. Cyber security is defined as protecting **computer** systems, which communicate over the **computer** networks.

Computer security is **important** because it keeps your information protected. It's also **important** for your **computer's** overall health; proper **computer security** helps prevent viruses and malware, which allows programs to run quicker and smoother**.**

1.2 Security Approaches

Trusted system:

A trusted system is a computer system that can be trusted to a specific extent to enforce a specific policy.

SECURITY MODELS An organization can take several approaches to implement its security model. Let us summarize these approaches.

No Security: In this simplest case, the approach could be a decision to implement no security at all.

Security through obscurity: In this model, a system is secure simply because nobody knows about its existence and contents. This approach cannot work for too long, as there are many ways an attacker can come to know about it.

Hot Security: In this scheme, the security for each host is enforced individually. This is a very safe approach, but the trouble is that it cannot scale well. The complexity and diversity of modern sites/organizations makes the task even harder.

Network Security: Host security is tough to achieve as organizations grow and become more diverse. In this technique, the focus is to control network access to various hosts and their services, rather than individual host security. This is a very efficient and scalable model**.**

INTRODUCTION

Computer data often travels from one computer to another, leaving the safety of its protected physical surroundings. Once the data is out of hand, people with bad intention could modify or forge your data, either for amusement or for their own benefit. Cryptography can reformat and transform our data, making it safer on its trip between computers. The technology is based on the essentials of secret codes, augmented by modern mathematics that protects our data in powerful ways.

- Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers

- Network Security - measures to protect data during their transmission

- Internet Security - measures to protect data during their transmission over a collection of interconnected networks Security Attacks, Services and Mechanisms To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One **Approach is to consider three aspects of information security:**

Security Attack – Any action that compromises the security of information owned by an organization.

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

Security Service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

Principle of Security:-

The classification of security services are as follows:

Confidentiality: Ensures that the information in a computer system a n d transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.

Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information.

Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages. Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

Access control: Requires that access to information resources may be controlled by or the target system.

Availability: Requires that computer system assets be available to authorized parties when needed.

Types of Attack:-

SECURITY ATTACKS There are four general categories of attack which are listed below.

Interruption:- An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

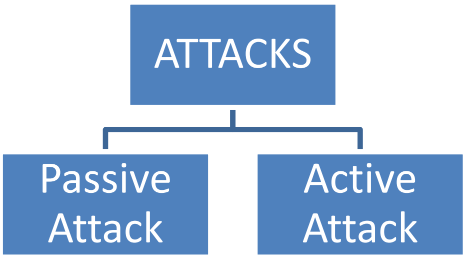
Interception:-An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer. e.g., wire tapping to capture data in the network, illicit copying of files Sender Receiver Eavesdropper or forger

Modification:- An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network. Sender Receiver Eavesdropper or forger

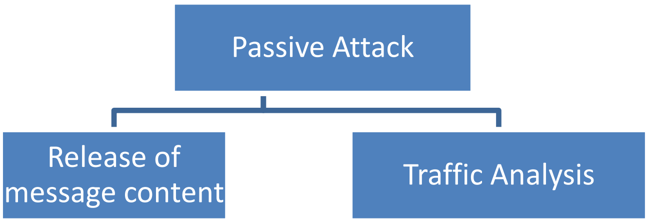
Fabrication:- An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file. Sender Receiver Eavesdropper or forger

Cryptographic Attacks

Types of Attack



Passive Attacks (Interception):-



Passive Attacks (Interception):-

Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Passive attacks are of two types:

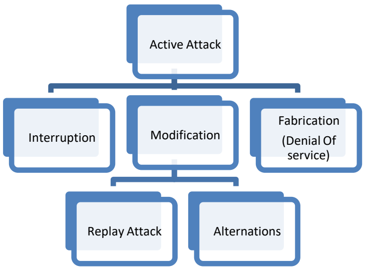
1. Release of message contents:

A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.

2. Traffic analysis:

If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place. Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

Active Attacks:-



These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

Masquerade (Interruption):– One entity pretends to be a different entity.

Modification of messages: - Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect. Modifications are two types

Replay: - Involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

Alteration: - Alteration of message involves some changes to the original message. **Denial of service (Fabrication) (DOS)** – Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance. It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Model Questions

Chapter-1

Possible attack on computes:

1. What are the key principles of security? (10)
2. Define security? Explain the need of security. (6)
3. Explain different security model. (6)
4. Explain different security approaches available for security purpose. (10)
5. Describe the principle of security. (10)
6. What are the types of attack to a computer system? (10)
7. Define virus? (2)
8. Define worm? (2)
9. What do you mean trusted system? (2)
10. What do you mean by OSI standard for security model? (2)
11. Distinguish between identify theft and brand theft? (2)
12. Define Trojan horse? (2)
13. Define cookies? (2)

Chapter-2

CRYPTOGRAPHY CONCEPTS

Cryptography is the study and practice of techniques for secure communication in the presence of third parties called adversaries. It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.

OR

Cryptography is the study and application of techniques that hide the real meaning of information by transforming it into nonhuman readable formats and vice versa.

Cryptography – Benefits

Cryptography is an essential information security tool. It provides the four most basic services of information security −

Confidentiality − Encryption technique can guard the information and communication from unauthorized revelation and access of information.

Authentication − The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.

Data Integrity − The cryptographic hash functions are playing vital role in assuring the users about the data integrity.

Non-repudiation − The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.

All these fundamental services offered by cryptography has enabled the conduct of business over the networks using the computer systems in extremely efficient and effective manner.

The process of transforming information into nonhuman readable form is called **encryption.**

The process of reversing encryption is called **decryption**.

Decryption is done using a **secret key** which is only known to the legitimate recipients of the information. The key is used to decrypt the hidden messages. This makes the communication secure because even if the attacker manages to get the information, it will not make sense to them.

The encrypted information is known as a **Cipher**.

What is Cryptanalysis?

Cryptanalysis is the art of trying to decrypt the encrypted messages without the use of the key that was used to encrypt the messages. Cryptanalysis uses mathematical analysis & algorithms to decipher the ciphers. The success of cryptanalysis attacks depends

- Amount of time available
- Computing power available
- Storage capacity available

The following is a list of the commonly used Cryptanalysis attacks;

Brute force attack– this type of attack uses algorithms that try to guess all the possible logical combinations of the plaintext which are then ciphered and compared against the original cipher.

Dictionary attack– this type of attack uses a wordlist in order to find a match of either the plaintext or key. It is mostly used when trying to crack encrypted passwords.

Rainbow table attack– this type of attack compares the cipher text against pre-computed hashes to find matches.

Cryptanalysis:-

Cryptanalysis is the study of analyzing information systems in order to study the hidden aspects of the systems. Cryptanalysis is used to breach cryptographic security systems and gain access to the contents of encrypted messages, even if the cryptographic key is unknown.

What is Cryptology?

Cryptology combines the techniques of cryptography and cryptanalysis.

OR

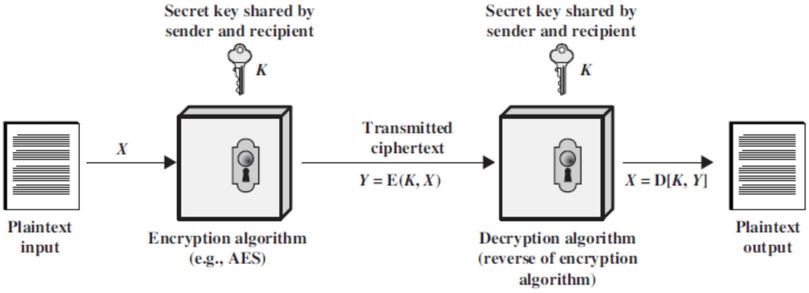
Cryptology: - Cryptology is a combination of Cryptography and Cryptanalysis:- Cryptanalysis is the technique of decoding messages from a non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format.

2.1 Plain text and Cipher text

Plain Text:-

Clear text or plain text signifies a message that can be understood by the sender, the recipient and also by anyone else who gets an access to that message.

Cipher text:- When a plain text message is codifies using any suitable scheme, the resulting message is called as cipher text.


Secret key shared by sender and recipient
K
Secret key shared by sender and recipient
K
X
Transmitted ciphertext
Y = E(K, X)
X = D[K, Y]
Plaintext input
Encryption algorithm (e.g., AES)
Decryption algorithm (reverse of encryption algorithm)
Plaintext output

There are two types of techniques used to covert plain text to cipher text.

- **Substitution Techniques**
- **Transposition Techniques**

2.2 SUBSTITUTION TECHNIQUES

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with cipher text bit patterns.

Caesar cipher (or) shift cipher

The earliest known use of a substitution cipher and the simplest was by Julius Caesar. TheCaesar cipher involves replacing each letter of the alphabet with the letter standing 3 placesfurther down the alphabet e.g., plain text : pay more money

Cipher text: SDB PRUH PRQHB Note that the alphabet is wrapped around, so that letter following „z‟ is „a‟. For each plaintext letter p, substitute the cipher text letter c such that

C = E(p) = (p+3) mod 26

A shift may be any amount, so that general Caesar algorithm is

C = E (p) = (p+k) mod 26

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply

P = D(C) = (C-k) mod 26

Playfair cipher:-

The best known multiple letter encryption cipher is the playfair, which treats digramsin the plaintext as single units and translates these units into cipher text digrams. The playfairalgorithm is based on the use of 5x5 matrix of letters constructed using a keyword. Let thekeyword be „monarchy‟. The matrix is constructed by filling in the letters of the keyword(minus duplicates) from left to right and from top to bottom, and then filling in the remainder ofthe matrix with the remaining letters in alphabetical order. The letter „i‟ and „j‟ count as one letter. Plaintext is encrypted two letters at a time

According to the following rules:

Repeating plaintext letters that would fall in the same pair are separated with a Filler letter such as „x‟. Plaintext letters that fall in the same row of the matrix are each replaced by the letter to the right, with the first element of the row following the last. Plaintext letters that fall in the same column are replaced by the letter beneath, with the top Element of the column following the last. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter.

Plaintext = meet me at the school house

Splitting two letters as a unit => me et me at the as ch o x ol ho us ex

Corresponding cipher text => CL KL CL RS PD IL HY AV MP HF XL IU

2.3 TRANSPOSITION TECHNIQUES

All the techniques examined so far involve the substitution of a cipher text symbol for a plaintext symbol. A very different kind of mapping is achieved by performing some sort of permutation on the plaintext letters. This technique is referred to as a transposition cipher.

Rail fence Technique:-

Rail fence Technique is simplest of such cipher, in which the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

Plaintext = meet at the school house

To encipher this message with a rail fence of depth 2, we write the message as follows:

m e a t e c o l o s

e t t h s h o h u e

The encrypted message is

MEATECOLOSETTHSHOHUE

Row Transposition Ciphers-

A more complex scheme is to write the message in a rectangle, row by row, and read the message off, column by column, but permute the order of the columns. The order of columns then becomes the key of the algorithm.

e.g., plaintext = meet at the school house

Key = 4 3 1 2 5 6 7

PT = m e e t a t t

h e s c h o o

l h o u s e

CT = ESOTCUEEHMHLAHSTOETO

A pure transposition cipher is easily recognized because it has the same letter frequencies as the original plaintext. The transposition cipher can be made significantly more secure by performing more than one stage of transposition. The result is more complex permutation that is not easily reconstructed.

Feistel cipher structure

The input to the encryption algorithm are a plaintext block of length 2w bits and a key K.the plaintext block is divided into two halves L0 and R0. The two halves of the data passthrough „n‟ rounds of processing and then combine to produce the ciphertext block. Each round „i‟has inputs Li-1 and Ri-1, derived from the previous round, as well as the subkey Ki, derived from the overall key K. in general, the sub keys Ki are different from K and from each other. All rounds have the same structure. A substitution is performed on the left half of the data (as similar to S-DES). This is done by applying a round function F to the right half of the data and then taking the XOR of the output of that function and the left half of the data. The round function as the same general structure for each round but is parameterized by the round sub key ki. Following this substitution, a permutation is performed that consists of the interchange of the two halves of the data. This structure is a particular form of the substitution-permutation network.

The exact realization of a Festal network depends on the choice of the following parameters and design features:

Block size - Increasing size improves security, but slows cipher

Key size - Increasing size improves security, makes exhaustive key searching harder, but may slow cipher

Number of rounds - Increasing number improves security, but slows cipher

Sub key generation - Greater complexity can make analysis harder, but slows cipher

Round function - Greater complexity can make analysis harder, but slows cipher

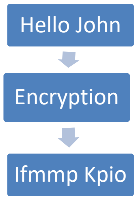
Fast software en/decryption & ease of analysis - are more recent concerns for practical use and testing.

Vernam Cipher (One-Time Pad):-

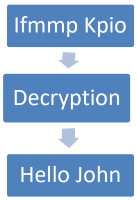
Vernam cipher uses a one-time pad, which is discarded after a single use and therefore is suitable for short messages.

2.4 Encryption and Decryption:-

Encryption:- The process of encoding plain text messages into cipher text messages is called as encryption.



Decryption:- The reverse process of transforming cipher text messages back to plain text messages is called as decryption.



2.5 Symmetric and Asymmetric Key Cryptography:

Symmetric key Cryptography:-

Symmetric key cryptography (or symmetric encryption) is a type of encryption scheme in which the same key is used both to encrypt and decrypt messages.

Asymmetric key Cryptography:-

Asymmetric encryption uses the public key for the encryption, and a private key is used for decryption.

Or

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys -- one public key and one private key

Diffie-Helman key Exchange/Agreement Algorithm

Diffie Hellman (DH) key exchange algorithm is a method for securely exchanging cryptographic keys over a public communications channel. ... If Alice and Bob wish to

communicate with each other, they first agree between them a large prime number p, and a generator (or base) g (where 0 < g < p).

ALICE	**BOB**
Public Keys available = P, G	Public Keys available = P, G
Private Key Selected = a	Private Key Selected = b
Key generated =	Key generated =
Exchange of generated keys takes place	
Key received = y	key received = x
Generated Secret Key =	Generated Secret Key =
Algebraically it can be shown that	
Users now have a symmetric secret key to encrypt	

Example
Step 1: Alice and Bob get public numbers P = 23, G = 9
Step 2: Alice selected a private key a = 4 and Bob selected a private key b = 3
Step 3: Alice and Bob compute public values Alice: x =(9^4 mod 23) = (6561 mod 23) = 6 Bob: y = (9^3 mod 23) = (729 mod 23) = 16
Step 4: Alice and Bob exchange public numbers
Step 5: Alice receives public key y =16 and Bob receives public key x = 6
Step 6: Alice and Bob compute symmetric keys Alice: ka=y^a mod p = 65536 mod 23 = 9 Bob: kb = x^b mod p = 216 mod 23 = 9
Step 7: 9 is the shared secret.

Model Questions

Chapter-2 Cryptography Concepts

1. Define cryptography. (2)

2. What do you mean cryptanalysis? (2)

3. Distinguish between plain text and cipher text? (2)

4. Explain the substitution technique? (10)

5. Describe the transposition technique? (10)

6. What do you mean by symmetric &asymmetric cryptography? (10)

7. Explain poly alphabetic substitution cipher? (6)

8. What do you mean by rail fence technique? (6)

9. Explain Diffie-Helmans Key exchange /Agreement algorithm with suitable example. (6)

10. Define encryption? (2)

11. Distinguish between encryption & Decryption? (2)

12. What are the differences between encryption processes to decryption process? (6)

13. What is algorithm Mode? Explain various types of algorithm Modes. (10)