Module
13
Network Security

Lesson

40

Network Security

13.1.1 INTRODUCTION

Network Security assumes a great importance in the current age. In this chapter we shall look at some of the security measures that are adopted in today's networks. The schematic below best explains these different techniques and their inter relationship.

Cryptography has been at the heart of security from time immemorial. Cryptography has always been performed using a secret key (code) shared between the sender and the receiver. However a new approach to cryptography involves the use of a public and private key. This concept will be explained in detail later.

HASHING MEANS CREATING A MINIATURE VERSION OF A MESSAGE THAT CAN BE USED, INSTEAD OF THE MESSAGE FOR SOME ASPECTS OF SECURITY.

Authentication of People and processes is required to let them access the resources of an organization.

There was also very little provision for security in the original TCP/IP model for the internet. A modified model has to be created to take care of security. This is done by adding *extra layers/sub-layers* at the application layer, the transport layer, the network layer and the data link layer.

Firewalls are necessary to prevent unauthorized people accessing the resources of the system. They filter the messages that are received by the system. Finally the use of a Virtual Private Network (VPN) allows an organization with offices at different geographic locations to keep their network secure and protected.

We shall now discuss some of these techniques in detail.

13.1.2 CRYPTOGRAPHY

The original message to be transferred is known as **plaintext.** After the message is transformed it is known as **ciphertext. Encryption** and **Decryption** algorithms transform plaintext to ciphertext and back. The algorithms are also known as **ciphers**. A **key** is the number that the cipher as an algorithm operates on.

☞ *IN CRYPTOGRAPHY, THE CIPHERS ARE PUBLIC, THE KEYS ARE SECRET.*

We have two groups of cryptography algorithms: symmetric-key algorithms and public-key algorithms.

SYMMETRIC KEY CRYPTOGRAPHY

In Symmetric key cryptography, the same key is used by both parties. In symmetric-key cryptography, the algorithm used for decryption is the inverse of the algorithm used for encryption. The same key is used in both the directions.

Symmetric-key algorithms are efficient. It takes less time to encrypt and decrypt a message using a symmetric-key algorithm.

However each pair of users must have a unique symmetric key. Thus for N people to use the symmetric-key algorithm we need N(N-1)/2 keys.

In the earliest and simplest symmetric-key ciphers, a character was substituted or transposed.

A cipher using the **substitution method** replaces one symbol with another. The substitution may be monoalphabetic, or polyalphabetic. In monoalphabetic substitution the relation between the character in the plaintext and ciphertext is always one-to-one. In polyalphabetic substitution, each occurrence of a character can have a different substitute, i.e. the relation is one-to-many.

☞ *AN EXAMPLE OF POLYALPHABETIC SUBSTITUTION IS THE* ***VIGENERE CIPHER***

Monoalphabetic substitution is very simple, but the code can be attacked easily. The method cannot hide the natural frequencies of characters in the language. A key created by polyalphabetic substitution is harder to break than a ciphertext created by monoalphabetic substitution. A good polyalphabetic substitution may as a mater of fact smooth out the frequencies. However even then attacking the code is not difficult.

In a **transpositional cipher**, the characters retain their plaintext form but change their position to create the ciphertext.

Source: http://nptel.ac.in/courses/Webcourse-contents/IIT%20Kharagpur/Communication%20network/pdf/13.1%20Lesson%2040%20.pdf