Computer & Network Security

Anshuman Thakur [1], Deepak Pandey [2], Khatri Mrunal Mohan [3], Mrs. Ajina A [4],

[1][2][3] *Computer Science Engineering Department,*
Sir M. Visvesvaraya Institute of Technology
Bangalore, India
[4] *Asst. Professor, Computer Science Engineering Department,*
Sir M. Visvesvaraya Institute of Technology
Bangalore, India

ABSTRACT: In modern world, our entire life moves around Computers. Most of our tasks are dependent on the Computers, like Communication, Ticket Reservations, Researches, Printing, Education, etc. When we communicate with each other by using Computers through E Mails, a number of Computers are used for this purpose and the collection of these computers forms a network, which is called a Computer Network. As more and more peoples are going to be connected through the general network (INTERNET), the problem of security arises. Now a day, a number of security issues occur in networks which include Sniffing, Spoofing, Security Attacks, Malwares, Unauthorized Access, etc. This will create havoc for the users, who wants to communicate with each other through these Networks. So, to make the communication between two users via the Computer Networks, we have to follow some security measures, which include using the Firewalls, Anti Malicious Software, Intrusion Detection Systems, Cryptography Techniques, etc. This paper is basically focused on how the communication between two users has been performed by using Computer Networks and how to make such a communication safe and secure.

KEYWORDS: Network Security, Security Attacks, Intruders, Malwares, Cryptography, Encryption, Password Protection, Firewalls, etc.

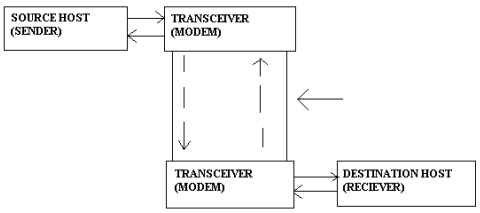
INTRODUCTION to COMPUTER NETWORKS:

A Computer has become an integral part of our modern lifestyle. We can do almost anything by using it. Even, now the Communication is almost dependent on the Computers. When a group of Computers are connected together via a common medium and transfers data and information from one system to another system, then such a collection of Computers is called a Computer Network.

For the establishment of a simple Computer Network, we require two users with their Computer Systems, a transmission medium between these two users, data / information to be transmitted and a common protocol between them, at minimum. The user who will transfer the Data is called Source Host or Sender and the other who will receive the Data is called Destined Host or Receiver. There has to be path from the Sender to the Receiver through which the Data will travel from one end to another. This path is called Transmission Medium. It can be Wired or Wireless. A Protocol is a set of Rules to be followed by both sides during their Communication.

The Sender has a Transmitter through which it transmits the Data to the Receiver through the Transmission Path. The Destined Host has a Receiver through which it receives the Data from the Transmission Path. Generally, at both ends, Transmitters and Receivers are replaced by Transceivers (Transmitter + Receiver), a device which can transmit as well as receive the data. The commonly

used Transceivers are MODEMS (Modulator + Demodulator).



BASIC COMPUTER NETWORK MODEL

INTRODUCTION to NETWORK SECURITY: Network Security is the branch of Computer Science that deals with the problems of providing the secure and safe communication between the two users of the computer network. While communicating with each other through computer networks, a number of problems arises like hacking, phishing, security attacks, unauthorized access, etc. that will create havoc for its users. So, to deal with such problems, we require some security measures. The main aim of providing security is to make sure that our sensitive data like passwords and account number will remain protected from unauthorized access of external users. To make sure that our network remains secure, we have to make sure that each individual computer of the network will be protected from security threats and then the entire network will be protected from the security threats. So, basically we require two kinds of Security Measures:

1. Computer Security, to make each Computer safe and protected.
2. Network Security, to make the entire network safe and protected for the communication between its users.

SECURITY THREATS:

There are a number of security threats in Computer
Networks, which includes:

1. Security Attacks
2. Unauthorized Access
3. Intrusion
4. Malicious Software

SECURITY ATTACKS: Basically there are two types of security attacks, viz. Active Attacks and Passive Attacks.

ACTIVE ATTACK: An Active Attack is one in which the attacker has to send the data to at least one of the parties communicating or to both the parties. It might be possible that in such type of attack, you will get any misleading data from another side, you will get incorrect data, you get partially correct data, it might be that the data is from wrong address, etc. Some examples of active attacks are MAN in the MIDDLE ATTACK, Denial of Service Attack, etc.

PASSIVE ATTACK: In this type of Attack, the attacker can only use the data to be transmitted from one end to another, but can't transfer any data from his own. He just wants to access your data. This type of attacks includes Traffic Analysis, Eavesdropping, Monitoring of transmissions, etc.

UNAUTHORIZED ACCESS: Unauthorized Access means to access the data / information for which you are not authorized. It means there has been some information that is kept secret or protected from you and you want to access that information at any cost. This type of Security Threat is called Unauthorized Access. To keep our System or Network away from unauthorized access, we provide Passwords to our Systems. Generally, we provide Biological Passwords and now a day, we use Artifact Based Passwords for making our Systems and Networks secure.

INTRUSION:

The process by which any user either external or internal to an organization / network tries to access the data for which it is unauthorized is called Intrusion. The person who can do such operations is called Intruder. There are three types of Intruders:

1. Misfeasor
2. Clandestine User

3. Masquerader

MISFEASOR: An Intruder who wants to access the data by unauthorized means and who is internal to a network or organization, such type of Intruder is called Misfeasor.

***CLANDESTINE USER*:** An Intruder who tries to access the unauthorized data by showing himself as a Super User or the person who can access any data of the network by showing that he/she has all the privileges for doing that, such type of Intruders are called Clandestine Users.

MASQUERADER: A person who tries to access the unauthorized data of a network and who does not belongs to that network, such Intruder is called Masquerader.

MALICIOUS SOFTWARE: Malwares or Malicious Software is harmful programs that provide serious hazards to our Computers and Networks. These are codes written in programming languages and are stored in files in such a way that no one can find them. Various examples of Malicious Software include Trojan Horse, Trapdoors, Logic Bombs, Zombies, Worms, Virus, etc.

TROJAN HORSE: The main goal of the Malware is to get executed without being Detected and Deleted. Trojan Horse or simply Trojan is a bug that performs this task by simply inviting the user to click its execution button and after its execution, creates several problems for the person who has executed it, which includes Deletion of necessary Files, Installation of Harmful Software by its own, etc. To keep our System protected from such Malware, we require properly updated Spyware Software.

TRAPDOOR: During the development of a system, the programmer or administrator of that system creates a back door entry by which they can access the system in case of any problem in which they are unable to access the system properly. Trapdoor is such a Malware that accesses the system from that back door entry and creates several problems for the user of that system.

NETWORK WORMS: A Computer Worm is a Malware that creates several problems for the user by creating the replicas (Similar Copies of itself) in order to spread to other computers. It uses the Network of Computers to spread over a number of Computers across the Network. It does not require any kind of Software Program for its execution. It generally corrupts the entire network by reducing the bandwidth offered to the network.

VIRUS: A Computer Virus is a Malware that creates Replicas of it and provide harm to Computers. It spreads from one computer to another and provides serious troubles for the users. Ultimately, the entire network gets suffered. It requires a Software Program or Code that initiates its Operation. It can provide harm to your computer by deleting necessary files, registry files, executing any operation a number of times, etc.

SECURITY PARAMETERS:

1. Integrity
2. Secrecy
3. Authorization
4. Authentication

INTEGRITY: The Integrity of the Data means the Truthiness of the Data under concern. It also concerns with the Correctness of Data.

SECRECY: It means that the Data is kept Secret from the other Users of the same network or other networks.

AUTHORIZATION: This term means that the Data that we transfer, receive or access will belong to us.

AUTHENTICATION: The meaning of this term is that the Data be transferred will be authenticated. The Name and Address of the Sender should be properly mentioned in the Data Packet during transmission. The identities of both the parties under communication must be valid.

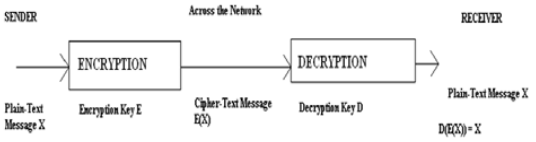
SECURITY TECHNIQUES: To make our Computer and Network secure, there exist a number of techniques, which includes:

1. Password Protection (Simple, Artifact Based & Biological)
2. Firewalls
3. Cryptography (Encryption/Decryption & Steganography)

PASSWORD PROTECTION: Password Protection is the simplest technique to implement security in a computer system or across a Computer Network. In simple Password Protection technique, a unique code has been provided to access the Computer System. This code can be composed of Alphabets, Numbers, Special Symbols, etc. and is known only to person who has provided it to his system. So, by this, one can make his system secure. But, now a day, Hacking has been implemented on vary large scale. Hacking is the process of accessing one's computer by unauthorized means. So, simple passwords are easy to crack. So, we had found another means of implementing Password Protection with the help of a device called Artifact. An Artifact is nothing but a Card (Somewhat like CREDIT CARD in size) on which a Bar Code has been Coded. When this Bar Code is pressed or is bring near the Bar Code Reader, it asks for the password, when we provide this Password, then if our Password is correct, then only we will get access to the System. But this technique also has some drawbacks, so we have found a new method for implementing Password Protection, which is called Biological Password Protection. In this technique, we use the Biological Sensors (Eye Retina Image, Hand Impression, Audio Password, Finger Print Impression, etc.) for implementing security of the System. This is by far, the best method for implementing Password Protection in any Network or Organization.

FIREWALLS: A Firewall is a tool used to keep the network safe and secure. It can be either Hardware Based or Software Based. It monitors all the traffic that is coming in the Network, as well as all the traffic that is going out of the Network. This means that each and every Byte of Data that is coming in to the Network or going out of the Network will have to pass through this Firewall. If it allows, then only the data will be allowed to come in and go out of the Network, otherwise the Data will be discarded. A basic firewall can operate up to the Network Layer of the OSI Model, which is called Network Layer Firewall or Packet Filter Firewall. A much better firewall is one that can operate up to the Transport Layer of the OSI Model, which is called Stateful Filter. The latest version of Firewall is one that can monitor the traffic up to the Application Layer of OSI Model, which is called Application Layer Firewall.

CRYPTOGRAPHY: The most common method of implementing secure transmission of data between two parties is by using Cryptography. Cryptography is a method by which the Data to be sent is converted into the form which could not be understood by the Hackers and only the intended receiver can understand it by again converting it into the original form. The method of converting the original data to modified data and again from modified data to original data is known only to the two parties under communication. It is a two-step process. In first step, the original data is converted to modified form, which will be sent across the network to the destined host. This process is called Encryption. In second step, the modified data received by the receiver is converted back to the original data. This process is Called Decryption. The original message is called Plain-Text and the modified message is called Cipher-Text. The Plain-Text will be converted into Cipher-Text and vice versa by using a Key.



CRYPTOGRAPHY (ENCRYPTION & DECRYPTION)

CRYPTANALYSIS: The process by which the Hackers try to decrypt the Encrypted Data without having the Correct Decryption Key is called Cryptanalysis.

STEGANOGRAPHY: The process by which the message will be transmitted across the network in such a way that it is protected without getting encrypted (Hidden by other means) is called Steganography. Example of such a technique includes Hiding Text Messages behind Images, Writing with Invisible Inks (Which will be readable only under certain color lights), etc. It is a process of providing Security by using Obscurity. The Steganography is a combination of two Greek Words STEGANOS which means Covered or Protected and GRAPHIE means Writing. So, the combined word Steganography means Concealed Writing.

ENCRYPTION TECHNIQUES: There are two types of
Encryption Techniques, as:

1. Symmetric / Shared Key Cryptography, in which single key is used for Encryption, as well as for Decryption of Data.
2. Public / Private Key Cryptography, in which either of the Key is used for Encryption and other for Decryption, depending upon the need.

Apart from these techniques, there are some techniques which first creates a Message Digest of the Original Message and then appends it to the Original Message and then Encrypts the overall Message by any of the above two techniques and at the receiving end, Decrypts it and again creates the Message Digest and compares the two. If both Digests are same, the Message is accepted else rejected. We can't create original message from its Digest. These techniques include SHA 1, MD 5, RIPEMD, Digital Functions, HASH Functions, MAC Functions, HMAC, etc. The common Encryption Algorithms are Monoalphabetic Cipher, Caesar Cipher, Hill Cipher, Vignere Cipher, Polyalphabetic Cipher, Playfair, S-DES Algorithm, DES Algorithm, AES Algorithm, IDEA Encryption Algorithm, etc. All these algorithms use common Key for Encryption as well as Decryption.

The algorithms that use different Keys for Encryption and Decryption include RSA Algorithm, Diffie Hellman Algorithm, Elliptic Curve Cryptography, etc.

CONCLUSION:

Network Security is a very broad topic and could not be covered in a single paper. In this paper, I just tried to provide you some information regarding Security Issues and how they create havoc in Computer Networks and how we can get solutions for such security issues. In this modern world, most of our tasks have been based on Computers. Now, with E Commerce, our Money transactions have become On Line.

So, during our Money Transactions, if someone will get access to our System or its information through unfair means, then it will provide a lot of damage to us. So, it is necessary for each and every one of us to make sure that we must keep our Computer Systems safe and secure and also try to make our Network Communication (even though through Internet) secure by using any of the Security Technique mentioned above. Always remember during communication, if it became necessary for you to write your password, make sure that it will be used for the intended purpose. Also make sure that the page or form on which you are working should not be a Phishing Page. So, always try to communicate in your network through secure means.

REFERENCES:

1.Khobragade S. S., Sardare P., Kumbhare B., Dongre P., & Jha D., (2011), "Cryptography & Network Security", , Conference Proceedings of International Conference on Advanced Computing, Communication & Networks, JUNE – 2011, UACEE, Page No. 697 - 700

2.Forouzan Behrouz E., "Data Communication & Computer Networks", 2nd Edition, Tata McGraw Hill Publications.

3.Stallings William, "Cryptography & Network Security", Prentice Hall Publications.

4. Kahate Atul, "Cryptography & Network Security", Tata McGraw Hill Publications.