Network Security to a Digital Library

By

Vidya Varidhi Upadhyay

Information Scientist

Central Library

Banaras Hindu University

Varanasi, U.P. 221005.

Rituja Upadhyay

Director

Pawan Infotech

Varanasi, U.P. 221005

M. M. Upadhyay

Lecturer

Ramdev Degree College Bhadohi, U.P.

ABSTRACT

-

Libraries and information centers are changing rapidly towards digitization. Now a days a stand-alone computer is of no use. It must be on network to utilize the resources. In the process of computer communication and data transmission the issue of network security arises. In this paper we try to the explain the meaning of network security, possible attacks, threats upon it and various approaches used to achieve this security.

KEYWORDS: Network Security, Encryption, Data Transmission, Digital Library

0. INTRODUCTION

The requirements of information security within an organization have undergone major changes. With the introduction of the computer, the need for automated tools for protecting files and other information stored on computer became evident; especially in the case for a networked and distributed environment. Network security measures are needed to protect information during its transmission and to guarantee that data transmissions are authentic.

The essential technology underlying virtually all automated networks and computer networks is encryption. Two fundamental approaches are in use: conventional encryption also known as symmetric encryption and public-key encryption also known as asymmetric encryption, which leads to digital signatures.

In general there is a flow of information from a source such as a file or a region of main memory, to a destination such

as another file or a user.

1. ATTACKS ON NETWORK

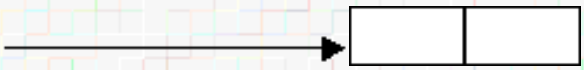
1.1 The types of attacks on security of a computer system or network may be of following types

Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file management system.

Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program or a computer. Example includes wiretapping to capture data in a network, and the illicit copying of files or programs.

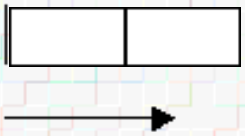
Modification: An unauthorized party not only gains access but tampers with an asset. This is an attack on integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.

Fabrication: An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file.



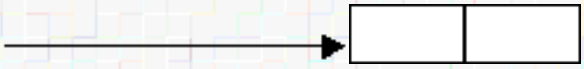
Information Source Destination Source

(a) Normal Flow



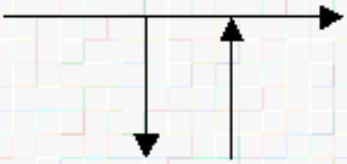
Information Source Destination Source

(b) Interruption

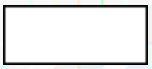


Information Source Destination Source

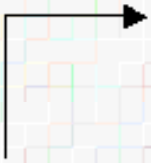
(c) Interception



Information Source Destination Source



(d) Modification



Information Source Destination Source

e) Fabrication

A useful categorization of these attacks is in terms of passive attacks and active attacks.

1.2 Passive attacks.

Passive attacks mean the eavesdropping on, or monitoring of transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of attacks are involved here:

(1) Release of message contents and

(2) Traffic analysis.

The release of message contents is easily understood. A telephone conversation, an electronic mail message or a transferred file may contain sensitive or confidential information.

The problem of traffic analysis is more serious. By masking the contents of messages or other information traffic, that opponents even if they capture message, may not extract the information from the message. The common technique for masking contents is encryption. If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages. The opponent could observe the frequency and lengths 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 the data. However it is feasible to prevent the success of these attacks.

1.2 Active attacks

The second major category of attack is active attack. These attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories

(1) Masquerade: It takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of the active attack. For example authentication sequence can be captured and replayed after a valid authentication has taken place.

(2) Modification: It simply means that some portion of a legitimate message is altered, or the message is delayed or reordered, to produce an unauthorized effect.

(3) Replay: It involves the passive capture of a data unit and its subsequent retransmission to produce an

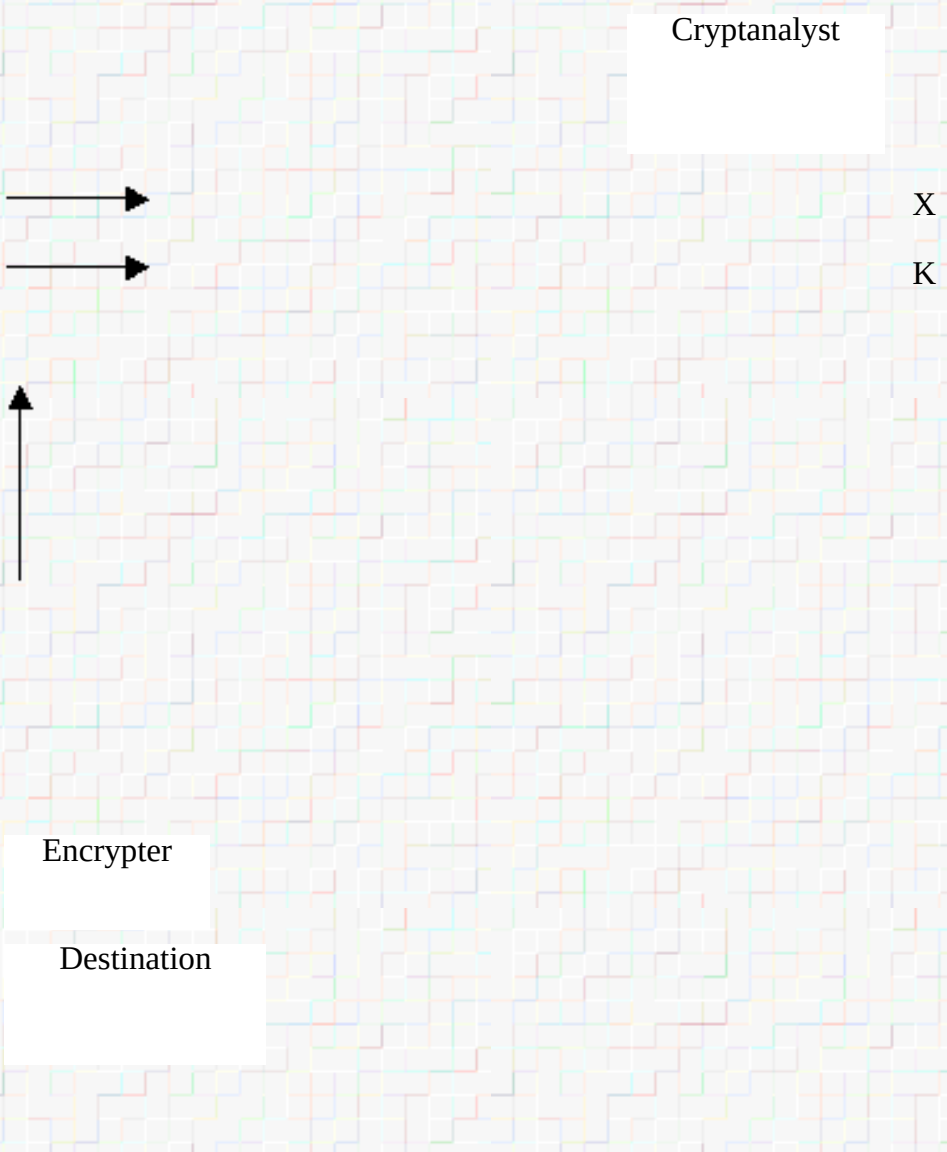
unauthorized effect.

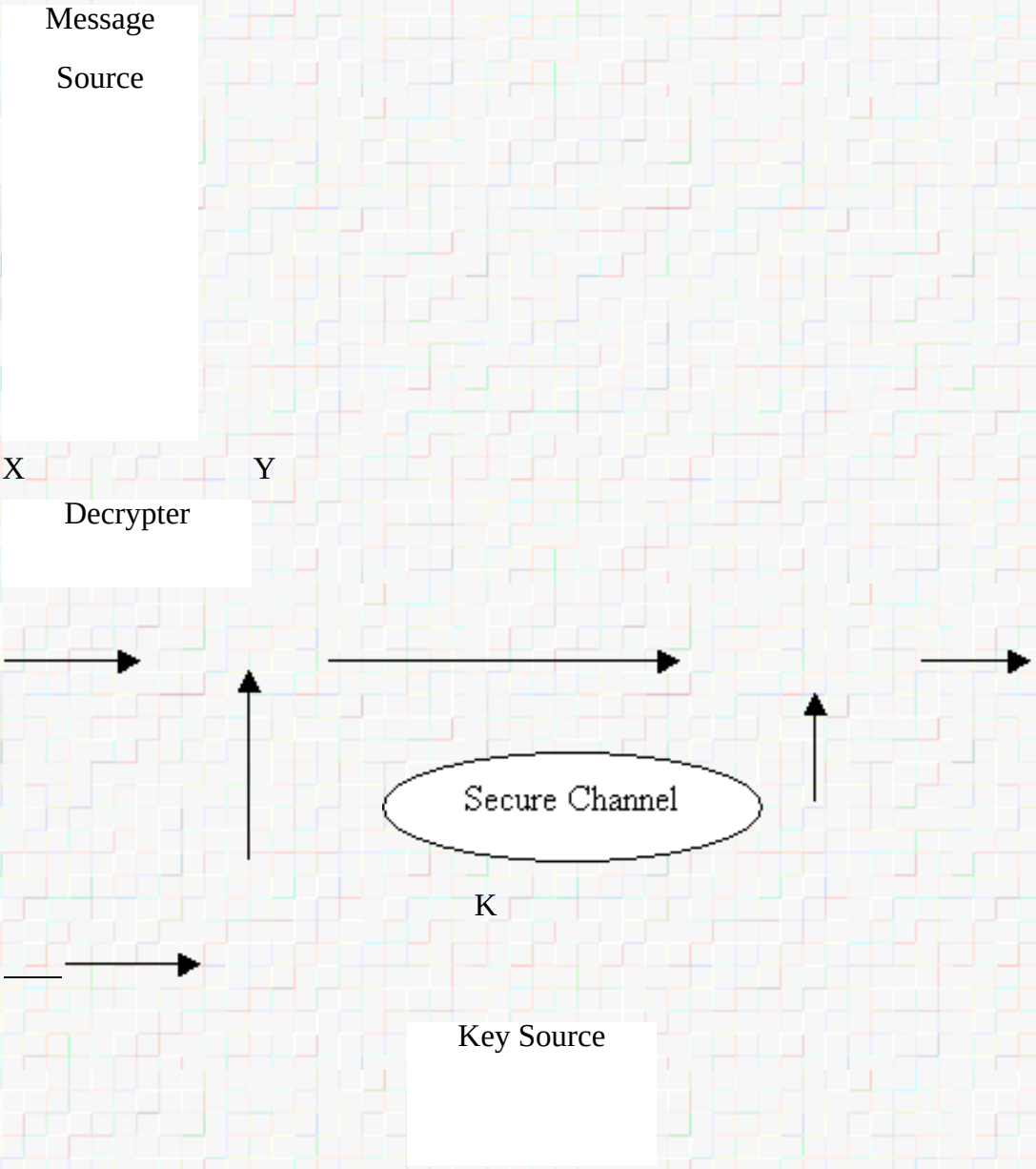
(4) Denial of service: It prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target; for example an entity may suppress all messages directed in a particular direction. Another form of service denial is the disruption of an entire network, either by disabling the network or by overloading it wit messages so as to degrade performance.

2. ENCRYPTION

2.1 Conventional Encryption

The following figure illustrates the conventional encryption process. The original message, referred to as plaintext, is converted into apparently random, nonsense, referred to as cipher text.





Model of conventional cryptosystem

The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext that controls the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. Changing the key changes the output of the algorithm.

Once the cipher text is produced, it is transmitted. Upon reception, the cipher text can be transformed back to the original plaintext by using the same key that was used for encryption.

The security of encryption depends on several factors. The encryption algorithm must be powerful enough so that it is impractical to decrypt a message on the basis of cipher text alone. Further the security also depends on the secrecy of the key, not on the secrecy of the algorithm. So it is assumed that it is impractical to decrypt a message on the basis of

the cipher text plus knowledge of the encryption/decryption algorithm.

While the message X and the encryption key K as input, the encryption algorithm forms the cipher text Y, which can be written:

$$\mathbf{Y=E_k(X)}$$

The intended receiver, in possession of the key, is able to invert the transformation:

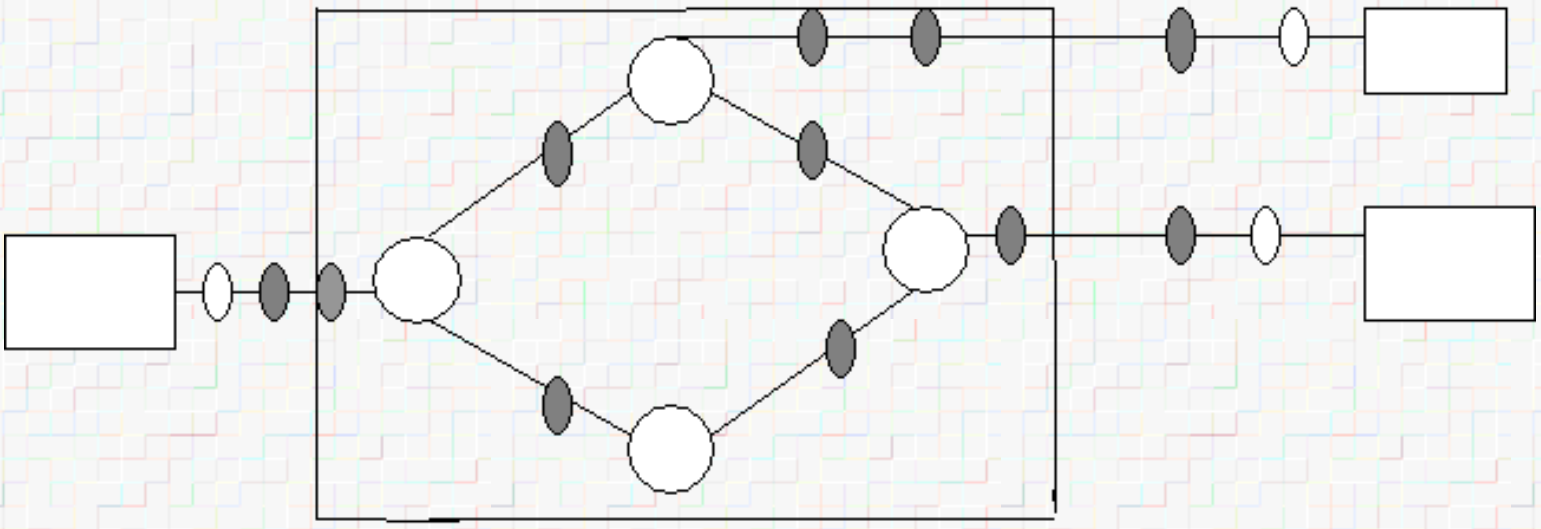
$$\mathbf{X=D_k(X)}$$

An opponent, observing Y but not having access to K or X, must attempt to recover X and K or both X and K. It is assumed that opponent does have knowledge of the encryption (E) and the (D) algorithms

The most commonly used algorithms are block ciphers. A block cipher processes the plain text input in fixed–size blocks, and produces a block of cipher text of equal size. The two most important conventional algorithms both of which block cipher, are DES (Data encryption Standard) and Triple DES. In DES with a key length of 56 bits, there are 2^{56} possible keys. Assuming that the key space has to be searched, a single machine performing one DES encryption per microsecond would take more than a thousand years to break the cipher.

2.2 Location of the encryption devices

In most encryption method we need to decide what to encrypt and where the encryption gears should be placed. As the following figure indicates there are two fundamental alternatives link encryption and end-to-end encryption.



End-to end encryption devices

Link encryption devices

Link encryption device

With the link encryption, each vulnerable communication link is equipped on both ends with an encryption device. All the traffic over all communication links is secured. This requires many encryption devices in a large network. The disadvantage of this approach is that the message must be decrypted each times it enters a packet switch; this is necessary because the switch must read the address (virtual circuit number) in the packet header to route the packet. Thus, the message is vulnerable at each switch. In case of public switching network, the user has no control over the security of the nodes.

With end-to-end encryption, process is carried out at the two end systems. The source encrypts the data, which is then transmitted unaltered across the network to the destination host. The destination shares a key with the source and so is able to decrypt the data. This approach seems to secure the transmission on the network but there is still a weak spot. Suppose a host connects to a X.25 packet-switching network, sets up a virtual circuit to another host, and is prepared to transfer data to that another host using end-to-end encryption. Data over such a network is in the form of packets, consisting of a header. It is clear that header part should be decrypted but this will not work because the other host can perform the decryption. The packet switching node will receive an encrypted packet and is unable to read the header. Therefore, it will not be able to route the packet. It follows that the host may only encrypt the user data portion of the packet and must leave the header, so that it can be read by the network.

Thus, with end-to-end encryption, the user data are secure; however the transmission pattern is not. To achieve greater security both link and end-to-end encryption are needed.

3. TRAFFIC PADDING

I mentioned that, in some cases, users are concerned about security from traffic analysis. With the use of link encryption, packet headers are encrypted, reducing the opportunity for traffic analysis. However, it is still possible for an attacker to access the amount the traffic on the network and to observe the amount of traffic entering and leaving each end system. An effective counter measure to this attack is traffic padding.

Traffic padding is a function that produces cipher text output continuously, even in the absence of plain text. A continuous random data stream is generated. When plain text is available, it is encrypted and transmitted. When input text is not present, the random data are encrypted and transmitted. This makes it impossible for an attacker to distinguish between true data flow and noise, and it is therefore impossible for the intruder to deduce the amount of traffic.

With conventional encryption, a fundamental requirement for two parties to communicate securely is that they share a secret key. But how to distribute secret keys securely is the most difficult problem for conventional encryption. This problem is wiped away with public-key encryption by the simple fact that the private key is never distributed. Now, we will see how public key encryption works.

Public key encryption, first proposed by Diffie and Hellman in 1976, is the first truly advance in encryption. Public key encryption is based on mathematical functions rather than on permutation and substitution. Further, public key cryptography is asymmetric, involving the use of two separate keys, in contract to the conventional symmetric encryption, which uses only one key.

A public key cryptographic algorithm relies on one key for encryption and a different but related key for decryption. These algorithms have following important characteristic:

Ø It is computationally not feasible to determine the decryption key, given only knowledge of the cryptographic algorithm and the encryption key.

The essential steps are as following.

Ø Each end system in a network generates a pair of keys to be used for encryption and decryption of the messages that it will receive.

Ø Each system publishes its encryption key by placing it in a public register file. This is the public key. The companion key is kept private.

Ø If A wishes to send a message to B, it decrypts it using B’s public key.

Ø When B receives the message, it decrypts it using B’s private key. No other recipient can decrypt the message because only B knows B’s private key.

With this approach, all participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed. As long as a system controls its private key, its incoming communication is secure. At any time a system can change its private key and publish the companion public key to replace old public key. For example if A prepares a message to B and encrypts it using A’s private key before

transmitting it, B can decrypt the message using A's public key. Because the message was encrypted using A's private key, only A could have prepared the message. Therefore, the entire encrypted message serves as digital signature. In addition, it is impossible to alter the message without access to A's private key, so the message is authenticated both in terms of source and in terms data integrity.

Thus the above-mentioned issues should be given due consideration when a library is going to be digitized.

4. CONCLUSION

In the above discussion, we discussed various aspects of network security and methods to use them. It is very necessary to keep an eye on the security for the obvious reasons. Many new researches are also going on. We hope that in coming days, the Computer Network Security will certainly increase.

REFERENCES

Horowitz (E), SAHANI (S) and RAJASEKARAN(S). Fundamentals of computer algorithms.2000.Galgotia Publications, New-Delhi.

STALLINGS(W). Data and computer commpunication.2001. PHI, New Delhi.

MITTAL(R L). Library Administration: theory and practice, 2001.Metropolitan Book Co. New-Delhi.

http://www.tansu.com.

BRIEF BIOGRAPHY OF AUTHORS

Vidhya Varidhi Upadhyay is the Information Scientist at Central Library, Banaras Hindu University. He holds M.Sc., M.C.A and B.L I Sc..

Rituja Upadhyay is the Director, Pawan Infotech, Varanasi. She has M.A. (Economics) and teaches RDBMS, Networking and C++

M. M. Upadhyay is a Lecturer at Ramdev Degree College, Bhadohi Uttar Pradesh and holds B.Sc. (Home Science) and (Mathematics).and M.C.A..