Proceedings of Annual Paper Meet
and International Conference
The Institute of Engineers, Bangladesh
Electrical Engineering Division
9th February, 2002

NETWORK SECURITY: A GLOBAL IMPERATIVE IN THE NEW MILLENNIUM

Shareeful Islam[1] and Md. Saiful Islam

Dept. of Computer Science and Information Technology
Islamic University of Technology (IUT), Dhaka
Board Bazar, Gazipur-1704, Bangladesh

ABSTRACT

The last two decades have experienced a tremendous growth in the field of IT enable processes. Advances in material science, sophisticated chip design coupled with unprecedented developments in computer software have fueled the leaps taken in information technology storage and communication system. The growth of networks (LANs and WANs) has linked organizations, nations and people at a scale never imagined before. Information and knowledge are institutional assets and need to be protected today's IT world. Network security measures are needed to protect data during the transmission and to guarantee that data transmissions are authentic. This paper discusses the major security violations of computer systems, different mechanism to secure networks and finally put forward some suggestions regarding network and information security.

1. INTRODUCTION

Information security is composed of computer security as well as network security. Before the widespread use of data processing equipment, the security of information felt to be valuable to an organization was provided primary by physical and administrative means. With the introduction of computer the need for automated tools for protecting files and other information stored on the computer become evidence. Today computer networks have revolutionized use of computer. They pervade our daily life, from automated teller machines, to airline reservation systems, to electronic mail services, to electronic bulletin board. Network security measures is needed to protect data during their transmission, and guarantee that data transmission is authentic. Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, modify message intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. It also deals with how to tell whether that they are not authorizing to use. Security also deals with the problems of legitimate message being captured and replayed, and with people trying to deny that sent certain message. Most people, who work with, maintain or use a network, need network security and also want to know how it should be implemented.

[1] *Corresponding author E-mail: sumel75@iit-dhaka.edu*

2. MAJOR TYPES OF SECURITY VIOLATIONS

Security is usually considered as encompassing three primary attributes; confidentiality, integrity and availability, with respect to various information entries such as data, program, access control parameters, cryptographic keys and computational resources (including processing and memory). Confidentiality implies that information can not be read or otherwise acquired except by those to whom such access is authorized. Integrity implies that information can not be altered except under properly authorized circumstances. Availability implies that resources are available when desired. All three of these attributes must typically be maintained in the presence of malicious users and accidental misuse and ideally also under certain types of system failures.

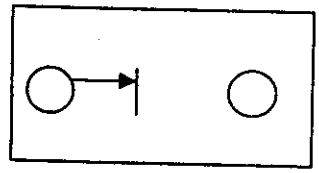
The types of security violations of the above three attributes are best characterized by viewing the function of the computer system to be providing information. In general, there is a flow of information from source to destination. There are four categories of security violations depicted in fig. 1.

•**Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This type of threat is interruption.

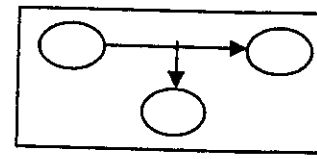
•**Interception** An unauthorized party gains access to an asset. This is a threat on security. It could be a person, a program, or a computer.

•**Modification** An unauthorized party not only gains access to but tampers with an asset. This is a threat of integrity.

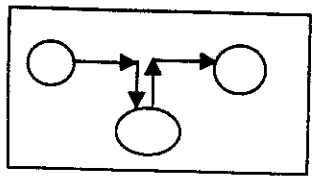
•**Fabrication** An unauthorized party inserts counterfeit objects into the system. This is also a threat to integrity



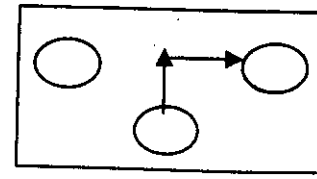
Interruption



Interception



Modification



Fabrication

Fig.1: Different kinds of security violations

We can also visualize these attacks in terms of following form [1]:

•Passive attack

Passive attack means the eavesdropping on, or monitoring of, transmission. The goal of the opponent is to obtain information that is being transmitted .Two types of attack are involved here: release-of-message contents and traffic analysis. The release-of-message content is easily understood telephone conversation or e-mail message etc is example. The emphasis in dealing with passive attacks is on prevention rather than detection.

•Active Attack

A major category of attack is active attacks. These attacks involve some modification of the data stream or the creation of a false stream and again it can be subdivided into four categories: masquerade, replay, modification of message, and denial of service.

•Password guessing attack

Security experts at Carnegie Mellon University estimate that more than a million passwords have already been stolen on the Internet [3]. Hackers have many tools, such as dictionary programs and sniffers, which assist them to steal password. A hacker will launch a dictionary attack by passing every word in a dictionary (which can contain foreign languages as well as the entire English language) to a login program in the hope that it will eventually match the correct password.

•Sniffers and CPM

Hackers also install a program to steal user names and passwords as they are transmitted over the net. Such a program is called a sniffer [3]. It works by changing the operation of the Ethernet adapter in the computer so that, instead of ignoring messages intended for other machines, it accepts everything and stores it in a file. Other hacker programs then analyze this file and extract the names and passwords from all the other junk. This mode is called 'promiscuous'. It is impossible to detect a promiscuous interface from outside the computer, so network administrators can not look for them. Thus, each system must check from within. Fortunately, there exists a small program freely available, which can detect a promiscuous interface, called 'CPM' (Check Promiscuous Mode). When 'CPM' run it prints out a list of all interfaces found, and whether or not they are in promiscuous mode. This should be done regularly, perhaps by including it in a regular user login.

3. DIFFERENT TYPES OF SECURITY TECHNIQUE

Network security presents a host of new problems not found n a single-system implementation. Security technique can be implemented for protecting the information from various kinds of attack. The various techniques are:

1. Privacy with conventional encryption
2. Message authentication.
3. Public key encryption and digital signature.
4. Security by using password.

3.1 PRIVACY WITH CONVENTIONAL ENCRYPTION

In a network system there is a flow of information from a source, such as file, to a destination, such as another file or a user. As we have already discussed that during this process, the data contained in the file may be interrupted, intercepted, modified or

fabricated. So, network security measures are needed to protect data during transmission. The powerful and most common technique to countering the threats is encryption. Encryption is a process that conceals meaning by changing intelligible message into unintelligible messages and that can be achieved by means of either a code or cipher.

The original message referred to as plaintext is converted into apparently random nonsense, referred to as ciphertext. The encryption process consists of an algorithm and a key. The key is a value independent of the plain text that controls the algorithm. The algorithm will produce a different output depending on the specific key being used at a time. Changing the key changes the output of the algorithm. Once the ciphertext is produce it is transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

Encryption algorithm must be powerful enough so that it is impractical to destroy a message on the basis of the ciphertext alone. Security of the conventional encryption depends on the secrecy of the key, not on the secrecy of the algorithm. That is it is assumed that it is impractical to destroy a message on the basis of the ciphertext plus knowledge of the encryption/decryption algorithm. So it is not necessary to keep the algorithm secret just keep the key secret.

Main problem in conventional is to keep the key secret [1]. In fig.2 plaintext $X=[X_1, X_2,\text{--},X_M]$ Where M elements of X letters are some finite alphabet .For encryption a key of the form $K=[K_1, K_2, \text{---}, k_J]$ is generated. The key is generated at the message source, then it must also be provided to the destination by means some secure channel.

With the message X and key K as input encryption algorithm produce ciphertext $Y=[Y_1, Y_2, \text{-------}, Y_N]$ So by using encryption algorithm E:

$$Y= E_k (X)$$

At the destination the transformation is $X= D_k (Y)$ where D is the decryption algorithm .In the below figure shows the model of conventional encryption. Where a message X is encrypted by key to produce ciphertext Y then decrypted by key through secure channel. The most common used conventional encryption algorithms are block ciphers. Two most important conventional algorithms, both of which are block ciphers, are DES and Triple DES.

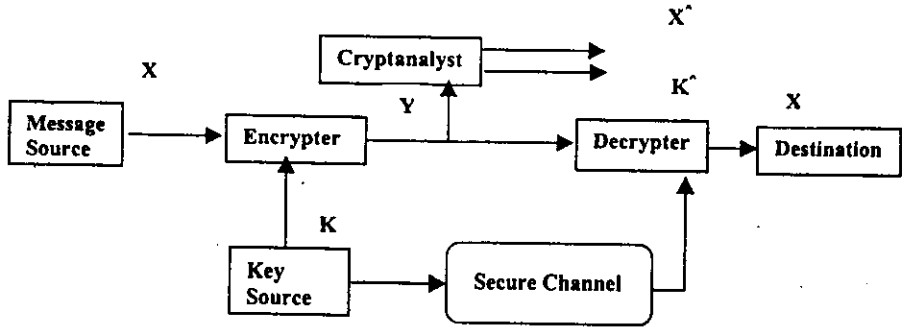


Fig. 2: Model of conventional encryption

3.2 MESSAGE AUTHENTICATION

Encryption protects against passive attack (eavesdropping). A different requirement is to protect against active attack. Protection against such attack is known as message authentication .A message, file, document, or other collection of data is said to be authentic when it is genuine and actually coming from its alleged source. Message authentication is a procedure that allows communicating parties to verify that received messages are authentic and the contents of the message have not been altered.
It is possible to perform authentication simply by the use of conventional encryption. It assume that only the sender and receiver share a key (which is as it should be), then only the genuine sender would be able to successfully encrypt a message for the other participant. Several approach of message authentication does not rely on encryption but rely on a related family function. An authentication tag is generated and appended to each message for transmission. The message itself is not encrypted and can be read at the destination independent of the authentication function at the destination.

Thus, there is a place for both authentication and encryption in meeting security requirement. One authentication technique involves the use secret key to generate a small block of data, known as a message authentication code that is appended to the message. This technique assumes that two communication parties, say A and B, shares a common secret key K_{AB} .. When A send a message to B, it calculate the message authentication code as a function of the message and the key: MAC_M=F (K_{AB}, M). The message plus the code are transmitted to the intended destination. The recipient performs the same calculation on the received on the received message, using the same secret key, to generate a new message authentication code. The received code is compared to the calculate code, If assume that only the receiver and sender know the identity of the secret key, and if the received code matches the calculate code. Then the receiver is assured that the message has not been altered. If an attacker alters the message but does not alter the code, then the receiver's calculation of the code will differ form the received code. Because the attacker is assumed not to know the secret key, the attacker cannot alter the code to correspond to the alterations in the message. The receiver is assured that the message is form the alleged sender.

3.3 PUBLIC KEY ENCRYPTION AND DIGITAL SIGNATURE

Public key encryption is the truly revolutionary advance in encryption in literally thousands of years. Public key cryptography is asymmetric, involving the use of two separate keys, incontrast to the conventional symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution and authentication.
The essential steps for public key encryption are as follows:

1. Each end system in a network generates a pair of keys to be used for encryption and decryption of message that it will receive.
2. Each system publishes its encryption key by placing it in a public register or file. This is the public key. The companion key is kept private.
3. If A wishes to send a message to B, it encrypts the message using B's pubic key.

4. 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. In contrary if A prepare a message to B and encrypts it using A's private key before transmission 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 served as a digital signature. In addition it is possible to alter the message without access to A's private key, so the message is authenticated both in terms of source and in terms of data integrity.

3.4 SECURITY BY USING PASSWORD

A secret word or phrase that one uses to gain admittance or access to information is called password. Password is used to authenticate a valid user in the network. The system will allow a user to log on only if that user's ID is known to the system and if the user knows the password associated by the system with that ID. For password to be usable the operating system must maintain a password file, listing legal passwords and the privileges associated with each password. Password file can be protected from hackers by encryption where all passwords in the password table are stored in encrypted form [5]. So when user enter a password it will encrypted and compare it to the password file so it would not necessary to decrypt the password file in any time.

4.CONCLUSIONS

The trustworthiness and security of communication channels and networks are essential to success of any network system in an organization; otherwise electronic information system can create a new vulnerabilities. In this scenario for the smooth operation of network issues related to network security as well as information security following measures can be taken:

1. Designing a work plan to investigate what policies are necessary to ensure individual privacy, while recognizing the legitimate organizational needs of information.

2. Adopting a proper design method IT based network by incorporating appropriate security devices (hardware and software) and a management system to monitor and incorporate corrective measures in the quickest possible time.

3. Organization should ensure data security and interoperability through the activities such as setting encryption standards and intrusion agreement on interoperability.

4. A public key custodian should be established for ensuring public key encryption network security.

5. Organizations have to organize themselves to plug the vulnerabilities to take full advantage of the power of networks and knowledge systems.

REFERENCES

[1] Stalling W., *Data and Computer Communication*, Fifth Edition, Prentice - Hall Of India Private Limited, New Delhi -110001, 1998

[2] Tanenbaum A.S., *Computers Networks*, Third Edition, Prentice - Hall Of India Private Limited, New Delhi -110001, 1998

[3] Shavi H. and Hugo K., *Public-Key Cryptography and Password Protocols.* Department of Electrical Engineering, technion-Israel and IBM T.J. Waston Research Center, Technion city, Haifa, Israel. ACM Transaction on Information and System Security, Vol. 2, No.3, August 1999.

[4] Diffie W., Vav Oorschot P.C. and Wiener, M. J., 1992. *Authentication and authenticated key exchanges*. DES. Codes Cryptography *2*, 2 (June 1992).

[5] Stalling W., *Operating Systems*, Macmillan Publishing Company, New York.

[6] Yu, C. F. and Fligor O.G. 1990. *A specification and Verification Method for Preventing Denial Service*, IEEE transaction Software Engineering 16 (6): 581-592

[7] Stubblebine, S. G. and Gligor V. D., 1999, *On Message Integrity in Cryptographic Protocols*, pp85-104, In Proceedings of IEEE Computer Science Symp. Res. Security Privacy, Oakland CA.

[8] Kanfman, C. Perlman, R and Speciner, *Network Security*, Printice-Hall, Engle Wood Cliff, NJ, 1994.

[9] M A Cheswisck and W. R. Bellooin S. M. 1994, *Firewalls and Internet Security: Repelling the Wily Hacker*, Addison-Wesley.

[10] *Network Intrusion Detection*, IEEE Network (1999 May/June): pp-26-41