International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 5, Issue 1 (January-February 2018), PP.001-008

NETWORK SECURITY & CRYPTOGRAPHY

Ruchika R. Mate[1] Shivani S. Shamkuwar[1] Nidhi A. Wasule[1]

[1]*P.G. Student, Master of Computer Application, G. H. Raisoni College of Engineering Nagpur ,India*

Abstract :- "SECURITY" in this contemporary scenarios has become a more sensible issue either it may be in "REAL WORLD" or in the "CYBER WORLD".in this world as opposed to the cyber world an attack is often preceded by information gathering.Computer system are more just hardware and software.As computers are linked together vie computer networks,the data and software become more vulnerable to disturbance. The focus of the paper is on network security. Our paper covers different kinds of threats & firewalls in the network by implementation of different security services using various security mechanisms.The security mechanisms are primarily based on cryptographic algorithms like symmetric-DES, AES, asymmetric-RSA, ECC. the logical conclusion is to use both kind of algorithms and their combinations to achieve optimal speed and security levels. It is hoped that the reader will have a wider perspective on security in general, and better understand how to reduce and manage risk personally.

Keywords: - Algorithms, Cryptography, Keysize, Network security, Security services**.**

I. INTRODUCTION

Over the past several years, mainframe and minicomputers have been replaced by the computer network. When mainframe and minicomputers were purchased, they came with many built-in security features. Although there were breaches of security, most were controllable. The computer was generally kept in a limited access room.

The number of authorized users was generally small in number. Sign-on IDs and passwords were necessary to use the computer system and the amount and type of usage was logged. Today as everyone migrates to networks of personal computers, little attention is being payed to the area of security. "Few organizations seem to recognize that part of the cost of IT is its security.

As desktop computing becomes an everyday part of business life so the need for better security measures will increase. A basic understanding of computer networks is requisite in order to understand the principles of network security.

The impressive development of computer networks has reached the point, where security becomes essential. Users want to exchange data in a secure way. The problem of network security is a complex issue. Network security means protection network.

1.1 Why do we need security?

There are many threats to the security of our computers and networks. These range from data stealing and diddling to the accidental loss of data.

(1) **Data Stealing:** Data stealing is a serious problem. Whether the data is modified or not, the interception and illicit use of data should be a major concern. Data stealing may be simply removing a diskette with important

data. It may involve copying the data from a hard disk.

(2) **Data Diddling:** One problem often over-looked in network security is the modification of data or data diddling. Data diddling is hard to detect and even harder to identify and prove who the culprit is.

(3) **Hackers:** Hackers are typically young males who are exploring a computer system or network. Many hacker activities include modification and steal of data.

(4) **Viruses:** Certainly the best known problem in computer security today is that of computer viruses. Computer viruses are a leading threat to secure computing. There are over 3000 computer viruses and strains with several new ones developed every day.

(5) **Loss of Data:** The biggest cause of data loss is accidental, i.e. "operator error." This accounts for, by some estimates, as much as 80% of the reported data loss. Only about 7% of the data lost can be attributed to computer viruses although this percentage is increasing. The remaining 10% of the data lost can be attributed to computer crime, environmental causes.

II. SERVICES FOR SECURITY

The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

(1)**Confidentiality:** Ensure that the information in a computer system and transmitted information are accessible only for reading by authorized parties. This type of access includes printing displaying and other forms of disclosure, including simply revealing the existence of an object.

(2)**Authentication***:* Ensure that the origin of a message or electronic document is correctly with an assurance that the identity is not false;

(3)**Integrity:** Ensures that only authorized parties are able to modify computer systems assets and transmitted information. Modification includes writing, changing, changing status, deleting, creating and delaying or replaying of transmitted messages.

(4)**Non-repudiation:** Requires that neither the sender nor the receiver of a message is able to deny the transmission.

(5)**Access control:** Require that access to information resources may be controlled by or for the target system.

2.1. Attacks

Attacks on the security of a computer system or network are best characterized by viewing the function of a computer system as provided information

2.1.1. Passive Attack:

An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis).

A. Eavesdropping: The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

B. Traffic analysis: The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

2.1.2. Active Attack:

An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS).

A. Masquerading: The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.

B. Replay: The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

C. Message modification: The attacker alters a legitimate message by deleting, adding to, changing, or reordering it.

D. Denial-of-service: The attacker prevents or prohibits the normal use or management of communications facilities.*DoS* (Denial-of-Service) attacks are probably the nastiest, and most difficult to address. Some things that can be done to reduce the risk of being stung by a denial of service attack include Keeping up-to-date on security-related patches for your hosts' operating systems.

E. Unauthorized Access : "Unauthorized access" is a very high-level term that can refer to a number of of attacks.The goal of these attacks is access some resource that your machine should not provide the attacker. These can take the form of a virus, worm, or Trojan horse. One of the most publicized threats to security is intruder. Generally referred to as a hacker or cracker, and some other threats are executing commands illicitly, confidential breaches, destructive behavior. Through any convention that you have to the outside world. This includes Internet connections, dial-up modems, and even physical access.

III . FIGURES

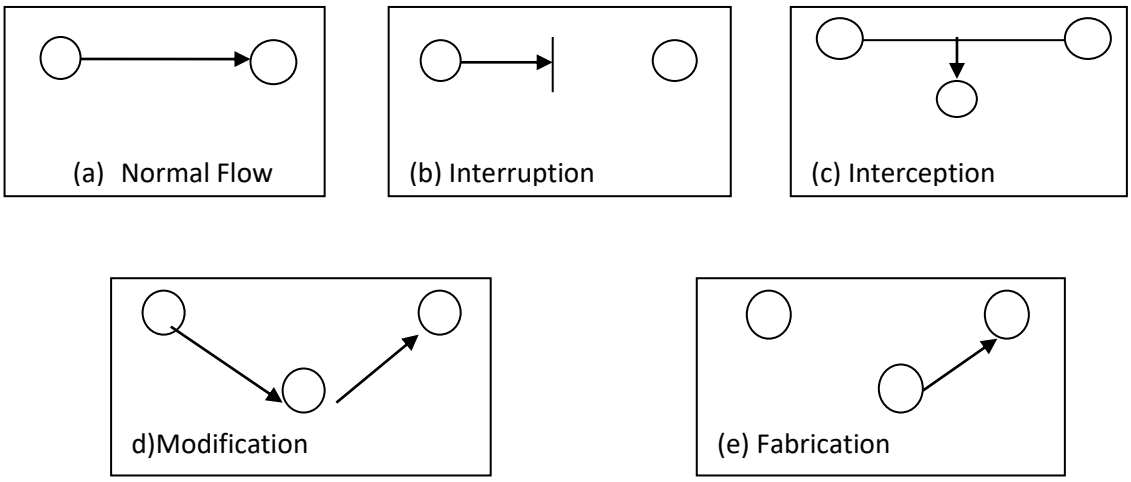


Fig: Security Threats

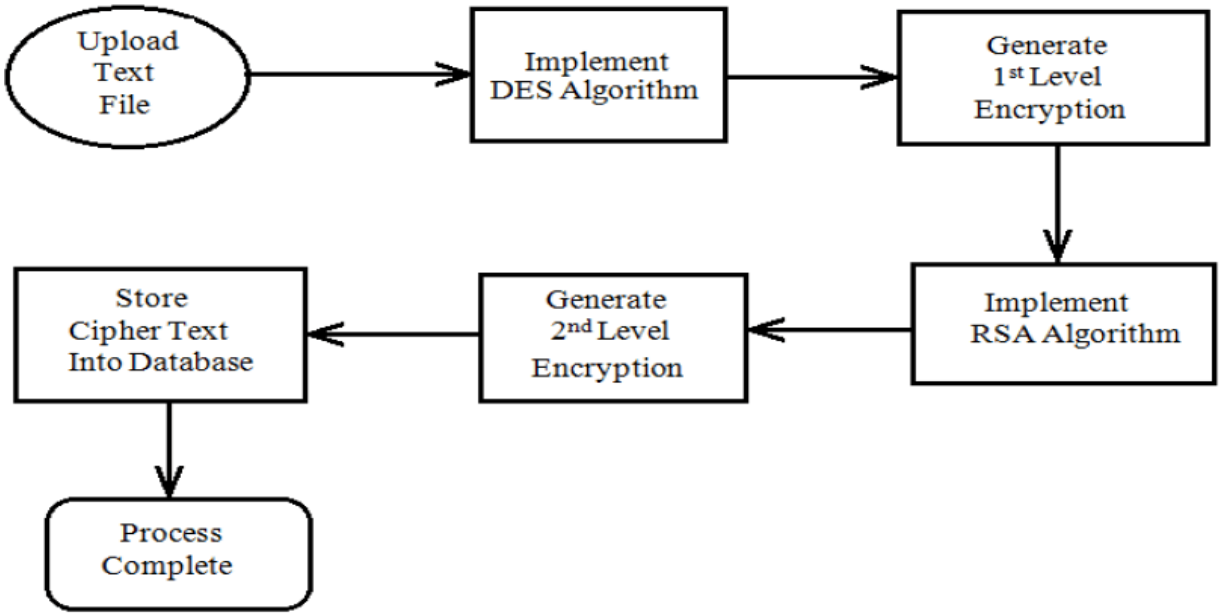


Fig: Block diagram of multilevel encrypton

IV. SECURITY MECHANISMS

A mechanism that is designed to detect, prevent, or recover from a security attack. Cryptography and Steganographic are such two techniques. Hence we focus on development, use and management of Cryptographic techniques.

4.1 Cryptography

The word "cryptography" [1,2,3,4] is derived from Greek and when literally translated, means "secret writing." The study of enciphering and encoding (on the sending end), and decoding (on the receiving end) is called cryptography. Although the distinction is fuzzy, ciphers are different from codes. When you mix up or substitute existing letters, you are using a cipher [5].

Encryption refers to the transformation of data in "plain text" form into a form called "cipher text," .The recovery of plain text requires the key, and this process is known as decryption. This key is meant to be secret information and the privacy of the text depends on the cryptographic strength of the key. Ciphers are broken into two main categories, substitution ciphers and transposition ciphers. Substitution ciphers replace letters in the plaintext with other letters or symbols, keeping the order in which the symbols fall the same. Transposition ciphers keep all of the original letters intact, but mix up their order.

A.Substitution cipher:

Plaintext letter A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Cipher text letter Q W E R T Y U I O P A S D F G H J K L Z X C V B N M

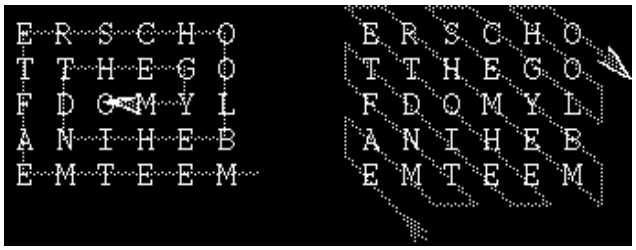
You can construct a secret message from the above table. Relative substitutions can be done. So, the message "Meet me after school behind the gym," would read

"DTTZ DT QYZTK LEIGGS WTIOFR ZIT UND."

Five letters are customary in the spy biz, so your message comes out like this:

DTTZD TQYZT KLEIG GSWTI OFRZI TUNDM

B.Transposition cipher: Text chosen in one form can be enciphered choosing a different route. To decipher, you fill the in box following the zigzag route and read the message using the spiral route. The cipher text becomes:



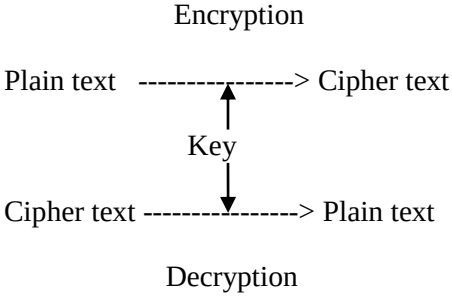
EAMTN FTDIE EHOTE RHMEM BYESC GLOHO

4.2 Types of Cryptography:
There are three types of cryptographic algorithms[1,6,7,5]:

1. Secret Key Cryptography.
2. Public Key Cryptography.
3. Hash Algorithms.

1. Secret Key Cryptography:

Secret key[7,1,2] cryptography involves the use of single key. Given a message (Plain text) and the key, encryption produces cipher text, which is about the same length as the plain text was. Decryption is the reverse of encryption, and uses the same key as encryption.



Secret key[6-9] cryptography is sometimes referred to as symmetric cryptography or conventional cryptography. If sender and receiver agree on a shared secret key, then by using secret key cryptography we can send messages to one another on a medium that can be tapped, without worrying about eavesdroppers. All we need to do is have the sender encrypt the messages and the receiver decrypts them using the key. An eavesdropper will only

see unintelligible data. Some of the secret key cryptography algorithms are - DES, 3-DES, blowfish, IDEA, AES, RC2, RC4, RC5, ECB etc.

Advantages of Secret Key Cryptography:

1) Very fast relative to public key cryptography.
2) considered secure, provided the key is relatively strong.
3) Widely used and very popular.

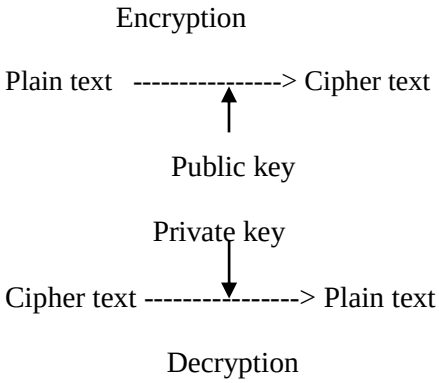
Disadvantages of Secret Key Cryptography*:*

The administration of the keys can become extremely complicated.

1) A large number of keys are needed to communicate securely with a large group of People.
2) The key is subject to interception by hackers.

2. **Public Key Cryptography**:

Public key cryptography sometimes also referred to as asymmetric cryptography**.** The public key need not be kept secret, and, in fact, may be widely available, only its authenticity is required to guarantee that A is indeed the only party who knows the co-responding private key. A primary advantage of such systems is that providing authentic public keys is generally easier than distributing secret keys securely, as required in symmetric key systems. The main objective of public-key encryption is to provide privacy or confidentiality. Public-key encryption schemes are typically substantially slower than symmetric-key encryption algorithms such as DES. The private key and the public key are mathematically linked.



Public key cryptography can do anything secret key cryptography can do like- transmitting the data over an insecure channel, secure storage on insecure media, authentication purposes and digital signatures. Some Public key cryptography algorithms are RSA, Elliptic Curve Cryptography (ECC), ElGamal, DH, DSA/DSS etc.

Advantages of Public key Cryptography*:*

1) Considered very secure, and easy to configure these systems.
2) No form of secret sharing is required, thus reducing key administration to a Minimum.
3) Supports non-repudiation.
4) The number of keys managed by each user is much less compared to secret keyCryptography.

Disadvantages of Public key Cryptography:

1) Much slower compared to secret key cryptography.

2) The ciphertext is much larger than the plaintext, relative to secret key Cryptography.

3. Hash Algorithms*:*

Hash algorithms [9] are also known as message digests or one-way transformations. A cryptographic hash function is a mathematical transformation that takes a message of arbitrary length and computes from it a fixed length number.

1. Password Hashing*:* When a user types a password, the system must store the password encrypted because someone else can use it. To avoid this problem hashing is used. When a password is supplied, it computes the password hash and compares it with the stored value if they match; the password is taken to be correct.

2. Message Integrity: Cryptographic hash functions can be used to protect the integrity of a message transmitted over insecure media.

3. **Message fingerprint***:* We can know whether some data stored has been modified from one day to the next, if we save that Data structure with a hash function. We can compare the hash function data structure with the message on the message data. If the message digest has not changed, you can be sure that none of the data is changed**.**

4. Digital Signatures: can be efficiently implemented using hash functions.

V. CONCLUSION

Everyone has a different idea of what "security"' is, and what levels of risk are acceptable. It's important to build systems and networks in such a way that the user is not constantly reminded of the security system around him. As and when new security methods are developed, breaking of these methods has increased. So measures have to be taken to fill the loopholes, of which cryptography has and is playing a major role. Cryptography is evergreen and developments in this area are a better option.

VI. ACKNOWLEDGEMENTS

6.1. Key Size*:* This has major role for amount of security. If the algorithm is inherently strong, then it can be assumed that the larger the key size [10] for the ciphers, the harder it is for a hacker to perform an attack on the cipher text. But, larger keys lead to lower levels of performance. Thus there are, trade-offs, which are traditionally made between the level of security and other factors, like performance**.**

6.2. Hybrid Systems*:* Just one crypto-system will not solve every problem. Most systems in use today employ a hybrid system.

REFERENCES

Books:

[1] William Stalling Cryptography and Network security: principles and practice; 2nd edition.

[2] J.P. Holbrook, J.K. Reynolds. ``Site Security Handbook."

[3] A.Menezes, P.van Oorschot and S.Vanstone: Handbook of Applied Cryptography.

[4] Speciner, M. Perlman, R: Network security, Englewood Cliffs, NJ

Links:

[5] Cryptography:http://vssut.ac.in/lecture_notes/ ;page no:6,7

[6] Security services:http://vssut.ac.in/lecture_notes/;page no:8-11

[7] Key:http://www4.ncsu.edu/~kksivara/sfwr4c03/lectures/lecture9

[8] Digital signature:https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture12;page no:6

[9] Hashing algorithm:http://www.cs.man.ac.uk/~banach/COMP61411.Info/CourseSlides/Wk4.1.Hash.

[10] Key size:https://infoscience.epfl.ch/record/164526/files/NPDF-22.

.