International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

NETWORK SECURITY AND CRYPTOGRAPHY

MOHANRAJ.S

RESEARCH SCHOLAR

SRI RAMAKRISHNA COLLEGE OF ARTS AND SCIENCE

COIMBATORE-6.

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.

Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more and more people become wired, an increasing number of people need to understand the basics of security in a networked world. 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, hash algorithm and etc. Generally, the logical conclusion is to use various kinds 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: Network security Fire walls Authentication Traffic analysis

I.INTRODUCTION

A basic understanding of computer networks is requisite in order to understand the principles of network security. In this section, we'll cover some of the foundations of computer networking, then move on to an overview of some popular networks. 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 a protection of the network assets.

II.POPULAR NETWORKS

UUCP:**UCCP***(*Unix-to-Unix Copy) was originally developed to connect UNIX (surprise!) hosts together.

Internet: The Internet is the world's largest network *of* ***networks.***

Services for security:

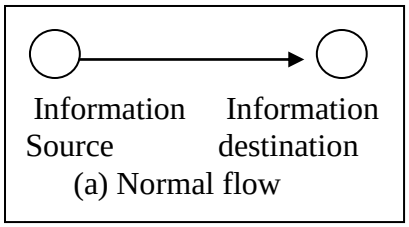
The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

- **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.

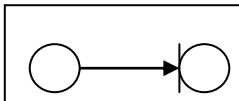
- **Authentication:** Ensure that the origin of a message or electronic document is correctly with an assurance that the identity is not false.
- **Integrity:** Ensures that only authorized parties are able to modify computer systems assets and transmitted information. Modification includes writing, changing, changing status, deleting, creating and delaying or replaying of transmitted messages.
- **Non-repudiation:** Requires that neither the sender nor the receiver of a message is able to deny the transmission.
- **Access control:** Require that access to information resources may be controlled by or for the target system.
- **Availability:** Require that computer systems assets be available to authorized parties when needed.

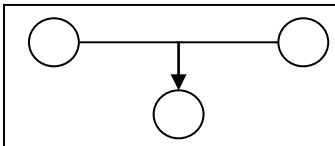
III.ATTACKS

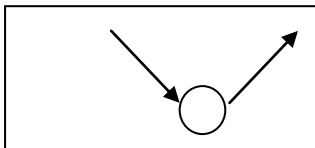
Attacks on the security of a computer stem or network are best characterized by viewing the function of a computer system as provided information. This normal flow is depicted in figure:



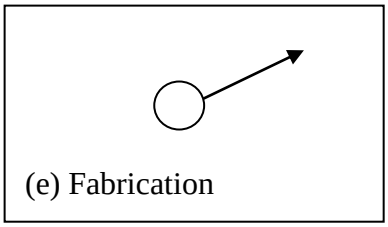
(a) Normal flow


(b) Interruption


(c) Interception


(d) Modification

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354



(e) Fabrication

Security threats

Categorization of these attacks is **passive attacks** and **active attacks.**

Passive attacks:

In this the goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are release of **message contents** and **traffic analysis.**

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.

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.

Active attacks:

These attacks involve some modification of the data stream or the creation of false stream and can be sub divided into 4 categories: **Masquerade, Replay, Modification of messages, and denial of service.**

Masquerading:

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

Replay:

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

Message modification:

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

Security threats:

Attacks came from: How, though does an attacker gain access to your equipment.

Through any connection that you have to the outside world. This includes Internet connections, dial-up modems, and even physical access.

Preventing security disasters:

- Hope you have backups
- Stay current with relevant operating systems patches
- Don't put data where it doesn't need to be
- Avoid system with single point of failure
- Watch for relevant security advisories

IV.FIREWALLS

Firewalls can be an effective means of protecting a local system or network of systems from network based security threats while at the same time, a firewall is simply a group of components that collectively form a barrier between two networks.

- Application Gateways
- Packet Filtering
- Hybrid systems

Best for me*:* Lots of options are available, and it makes sense to spend some time with an expert, either in-house, or an experienced consultant who can take the time to understand your organization's security policy, and can design and build a firewall architecture that best implements that policy.

Points of Failure: Any time there is only one component paying attention to what's going on between the internal and external networks, an attacker has only one thing to break (or fool!) in order to gain complete access to your internal networks.

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.

V.CRYPTOGRAPHY

The word **cryptography** 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.

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.

International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

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

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

Types of Cryptography:

There are three types of cryptographic algorithms:

- Secret Key Cryptography.
- Public Key Cryptography.
- Hash Algorithms.

Secret Key Cryptography:

Secret key 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.

Encryption

Plain text ---------->cipher text

Key

Cipher text---------->plain text

Decryption

Secret key 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 receivers decrypt 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, and ECB etc.

Advantages of Secret Key Cryptography:

- Very fast relative to public key cryptography.
- Considered secure, provided the key is relatively strong.
- The cipher text is compact (i.e., encryption does not add excess **Baggage** to the cipher text).
- Widely used and very popular.

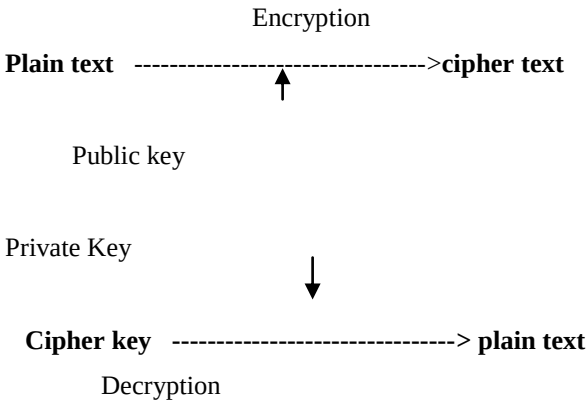
Disadvantages of Secret Key Cryptography:

- The administration of the keys can become extremely complicated.
- A large number of keys are needed to communicate securely with a large group of People.
- The key is subject to interception by hackers.

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:

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

Disadvantages of Public key Cryptography:

- Much slower compared to secret key cryptography.
- The cipher text is much larger than the plaintext, relative to secret key Cryptography.

Hash Algorithms:

Hash algorithms 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.

The following things can be done using hash algorithms.

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.

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

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.

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 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.

Hybrid Systems:

Just one crypto-system will not solve every problem. Most systems in use today employ a hybrid system.

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.

REFERENCES:

[1.] William Stallings: *Cryptography and Network security: principles and practice: 2nd edition.*

[2.] Douglas R.Stinson.*Cryptography: theory and practice*: 2nd edition

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

[4.] Smith, Laurence Dwight. *Cryptography, the Science of Secret Writing.*