Review on Network Security and Cryptography

Kajal* 
Scholar, Department of Computer Science & Engineering 
ABESIT, Ghaziabad, Uttar Pradesh, India 
kajal0375@gmail.com

Rizwan Khan 
Associate Professor, Department of Computer Science & Engineering 
ABESIT, Ghaziabad, Uttar Pradesh, India 
rizwan.khan@abesit.in

Abstract—In these days communication technology is very advanced. Digital communication has become very important to secure transmission of information between the sender and the receiver. Security for exchange is a very important feature because it protects information from interloper. In this paper we present a hierarchy of network security technologies such as privacy, authentication, non-rejection and honesty control. There are two popular security mechanisms, namely cryptography and steganography. Both are well known and widely used techniques. Cryptography is used to send data in an encrypted form using the encryption key. Encrypted data is transmitted through unsafe public media. Decryption algorithms are also used to decrypt messages when using decryption keys. Steganography is used to hide data in other cover media.

Keywords—Network Security, Cryptography, Decryption, Encryption, Steganography.

I. INTRODUCTION

The transmission of information via the Internet may include sensitive personal data that may be attacked by intruders. In addition, there are many applications on the Internet and many websites require the user to fill out the form in which sensitive personal data can be used. The user may need personal and secure communication for a number of reasons, which protect his information from intruders who are still waiting for an attack on sensitive data. Therefore, confidentiality and data integrity are necessary to protect information from unauthorized access and use. Network security issues can be divided into four parts: confidentiality, authentication, rejection, and integrity checking. Confidentiality or confidentiality concerns the protection of information against unauthorized users. This means that unauthorized users should not be able to read and understand the information. Verification means the identification process of a person based on the user name and password. In security systems, authentication is the process by which people access items based on their identity. Authentication ensures that the person he claims but does not say anything about the person's right.

II. SECURITY REQUIREMENTS

A. Confidentiality

The information must only be readable for the desired recipient. That is, save information from saving. There are two main techniques for obtaining security: cryptography and steganography. Cryptography is the science of secret or hidden writing of information. There are two main components: coding and decoding. There are two types of cryptography algorithms: public key cryptography and symmetric key cryptography. Steganography is a technology of secret communication where the intruder may not suspect that communication is going on. Secret information in steganography is hidden in another file without any problems. A carrier file or cover file can be an image, audio, video or text file.

B. Authentication

It means verification. Verification means the identification process of a person based on the user name and password. In security systems, authentication is the process by which people access items based on their identity. Authentication ensures that the person he claims but does not say anything about the person's right.

C. Non-repudiation

Non-repudiation is a guarantee that someone can not deny something. Generally, profanity refers to the ability to ensure that this message or message from the sender is not communicated.
D. Data integrity

In terms of networking, data integrity refers to the overall completeness, accuracy and stability of the data. Data integrity should be imposed when sending data through the network. This error can be achieved using the probe and correction protocol.

![Diagram of Network Security]

III. CRYPTOGRAPHY

Cryptography is a technology that ensures security by preventing messages from being encrypted and readable. Cryptography is a technology to transmit data on the Internet by applying an encryption algorithm that intruders are difficult to attack specific confidential information or personal information. The two basic words used in encryption are encryption and decryption. The encryption process is the process of converting plain text to encrypted text, and the decryption process is the reverse process of encryption. Plain text is text that contains the original message or unencrypted data and the cipher text is text that can be shared after encrypting the message. A key is necessary for encrypting and decrypting messages.

![Diagram of Encryption and Decryption]

1. Plain Text

Unscrambled information to be sent. This may be confidential information such as simple text documents, credit card numbers, passwords, bank account numbers, or personnel information, or secret expressions communicated between organizations.
2. **Cipher Text**

 Represents ordinary text that is incomprehensibly represented by the application of a mathematical algorithm. The code text is coded plain text that is sent to the recipient.

3. **Key**

 A mathematical value, formula, or process that describes how to encode or decode a flat text message. The key is the only way to decrypt the encrypted information.

A. **Cryptographic Algorithm**

 An expression used to encrypt plain text to generate code text. Converting readable text to encrypted text using cryptographic algorithms is called coding, and converting encrypted text to readable text with the same cryptographic algorithm is called decryption. Figure 1 shows the cryptographic tactics. Widely cryptographic algorithms can be divided into two categories:

- **Stream algorithms**: Clear byte operation at once. Bytes can be letters, numbers or special characters. This process is inefficient and slow.

- **Block algorithms**: Works on the readable text in blocks of bytes, called blocks (hence block name algorithm or block numbers). The general block size for modern algorithms is 64 bytes, small enough to work with but large enough to prevent code breakers. Unfortunately, breaking the 64-byte algorithm with brute force is unfortunately a relatively simple task with the current microprocessor speed.

1. **Types of Cryptography**

   a. **Secret Key Cryptography(Private key Cryptography)**: This algorithm is also known as secret key cryptography, where the sender and receiver encode and decode messages using the same key. An algorithm known as symmetric key algorithm is used for symmetric key encryption. Symmetric algorithms are classified into two types: stream encryption and block encryption. The flow encryption algorithm is optimized to accept readable text streams used to create encryption keys and to encode text streams. The block number algorithm works on data blocks where readable text is divided into blocks and each block is used independently.

   Some algorithms are:
   - Data Encryption Standard(DES)
   - Advanced Encryption Standard(AES)
   - Triple Data Encryption Standard
   - International Data Encryption Algorithm
   - Blowfish Encryption Algorithm
   - Twofish Encryption Algorithm

   b. **Public-Key Cryptography**: In the public's cryptography, each user generates two keys: a public key that is used to encrypt messages sent to the user, and the user needs a private key to decrypt a message.

   Some algorithms are:
   - Diffie-Hellman
   - Rivest–Shamir–Adleman(RSA)
   - Digital Signature Algorithm(DSA)
c. **Hash Functions**: The hash function uses mathematical changes in an irreversible encryption information. The main application of the hash function in cryptography is the integrity of messages. Hash Value Message delivers the digital framework and ensures that the message is not replaced by attack, virus or other. The hash algorithm is efficient due to the very low probability that two different plain text messages will produce the same hash value.

2. **Advantages And Disadvantages**
   
   **Advantages:**
   
   - It hides information and keep safe.
   - Nobody knows what this says until there is no key for the code.
   - You can write what you want. Even if the code (subject of code) wants to keep your secret code.
   
   **Disadvantages:**
   
   - In this code takes a long time.
   - It takes a long time to understand the code.
   - If you want to send a code to another person in the past, it will cost a lot to meet.

B. **Steganography**

Steganography is a technology for embedding hidden messages or data so that the existence of messages cannot be discovered. It is the advanced technology of cryptography. The main purpose of steganography is to hide the message or secret information so that no one can detect it. If they receive doubt data, the target is lost. The various types of data can be audio, video, text and images etc.

1. **The Carrier image**: The image of the courier is also called the cover object that will carry the message / data that used to be hidden.

2. **The Message**: There may be anything like a message data, file or image etc.

3. **The Key**: A key is used to decode and understand the hidden message.

![Fig 4. Basic Model Of Steganography](image)

**Advantages And Disadvantages**

**Advantages:**

A. Difficult to detect and only detect the receiver.
B. It can speed up with many software.
C. Provides better security for data sharing across LAN, MAN and WAN.

**Disadvantages:**

- If this technique has fallen into the wrong hands like hackers, terrorists and criminals, then it can be very dangerous for everyone.
- A large number of data, huge file sizes, so anyone can doubt for all.

IV. **CONCLUSIONS**

In this paper, we introduce the scope / hierarchy of network security technology. Due to the growing demands for privacy and security, various data concealment technologies are required, and many integration and extraction techniques are being developed. We discussed all cryptographic techniques and steganography techniques. Both are well-known and widely used technologies. The secret is a very convenient and safe technique for communication. When both techniques are combined, the use of cryptography and steganography makes communication more secure.
REFERENCES


