IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727 PP 75-78
www.iosrjournals.org

Network Security and Cryptography: A Study

Dharani S
Assistant Professor, Sri Balaji Arts and Science College

Abstract:
The beginning of WWW and the booming of ecommerce applications and social networks all over the world produces a enormous amount of data. The data transmitted through web faces the issue of its security. In this digital era, the issues of network security are considered as the most important issue of the society. Cyber attacks increase with the number of internet users. The need of techniques to secure the information in networks and to protect the computer were discussed in this paper. This paper gives the overview of cryptography in network security.
Keywords: Security, encryption, decryption, Symmetric encryption, Asymmetric encryption

I. INTRODUCTION

The necessity of internet technology increased in all the places like organizations, individual, educational institutions result in the data theft and intruders attack and destroy the network by Trojan horse and other viruses and worms. The intruder tries to attack the computers connected to the network, if the intruder succeeded once in the attack then all the computers connected to that network will be in petrified state. This causes a big threat to national security, when the intruder/invader has a hidden motive[1][2]. Cryptography is a technique used to secure information and communications through the use of codes, so that the person who involved in the data transmission can only understand it. Cryptography is a combination of two words crypt(hidden) and graphy (writing).

Cryptography is an art of converting a plain text to secret code (cipher text) and vice versa as shown in Figure 1.Cryptography ensures the security services like authentication, access control, Data integrity and confidentiality, and nonrepudiation. This paper studies about different security and cryptographic methodologies.

Figure 1:Encryption and Decryption

II. NETWORK SECURITY MODEL

The network security model is shown in figure 2. The sender sends a message through some communication channel (Internet). The message must be secured during transmission from the intruder/ attacker. The security techniques have two components. First, the information sent must be secured in a way that the attacker/ intruder cannot read it. It can be achieved by adding some codes to the message and that can be used to verify the sender identity. Second Component is the sender and receiver shares a secret information (key) which is unknown to the intruder. The security model must ensure both confidentiality and integrity.

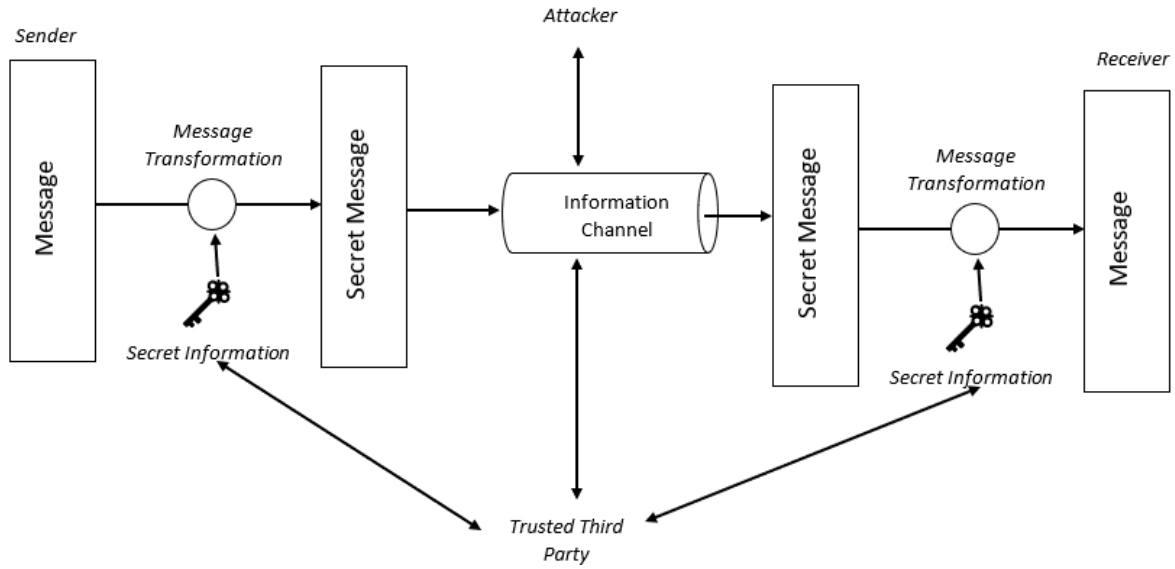

Figure 2: Model of Network Security

The model uses a trusted third party for secure transmission. The third party may take theresponsibility of distributing the secret key between the sender and receiver. The model has four basic functions to provide the security service. First task is to design for performing the encryption and decryption. The algorithm must be strong enough that the attacker cannot crack the code. Second task is to generate a secret key that is to be used in the algorithm designed. Third task is to build methods to share the secret key. Fourth task is to mention the protocol that uses the algorithm designed and the secret key used by both sender and receiver.

III. CRYPTOGRAPHY

Cryptographyis a way of transmitting message in such a way that only sender and receiver can intercept and understand the message.Some of the important terms used in cryptography are plain text (the message to be transmitted), encryption (the algorithm to transform the message into unreadable form), secret key (input to the encryption algorithm), cipher text (the converted text using the secret key and the algorithm), decryption (algorithm used by the receiver to convert the cipher text received to plain text).
Cryptography is of three main types: Symmetric, Asymmetric and Hash Functions.

3.1 SYMMETRIC ENCRYPTION

Symmetric encryption is a conventional encryption, and it is also known as single-key encryption. This type uses only one key to encrypt and decrypt. The secret key is called private key. The sender choose a secret key to encrypt the plain text into cipher text, and shares the same key to decrypt the message into plain text. This is a simple encryption technique but the distribution of a single key gives a chance of abuse.

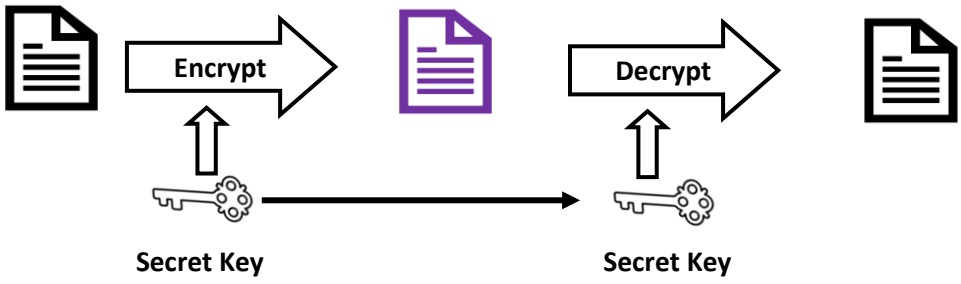

Figure 3: Symmetric Encryption and Decryption

Some of the symmetric encryption techniques are substitution techniques, transposition techniques, AES and DES.

3.2 ASYMMETRIC ENCRYPTION

In asymmetric key cryptography, there are two keys. One key is public, and another key is private. Each user has two keys (public and private). The public key is shared among the users. When sending message, the sender

A uses their private key to encrypt. At the receiver end, the receiver B uses the public key of sender A and decrypts the message (Figure 4). Another way is sender A uses the public key of receiver B to encrypt and receiver B uses the private key to decrypt the message (Figure 5).

Figure 4: Encryption using public key

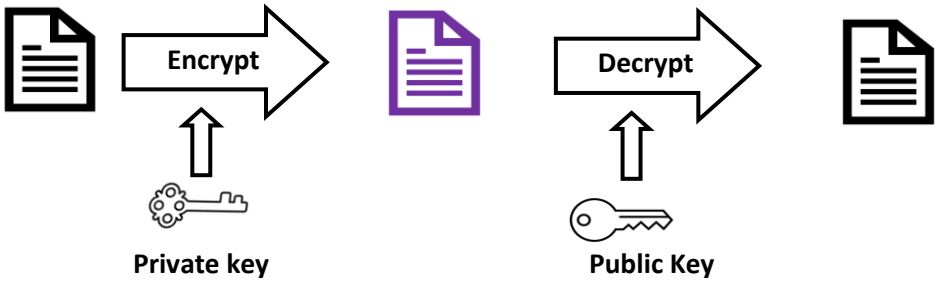

Figure 5: Encryption using Private Key

Some examples of public key cryptography are RSA, Diffie-Hellman key exchange, ElGamal cryptosystem, and Elliptic curve cryptography.

3.3 HASH FUNCTIONS

Hash functions does not have any secret keys to encryption and decryption. This uses a hash value of fixed size to encrypt the plain text. Hashing uses algorithms. It accepts variable length block of data M and produces a hash value of fixed size h= H(M), where H is hash function. Figure 6 represents the block diagram of cryptographic hash function.

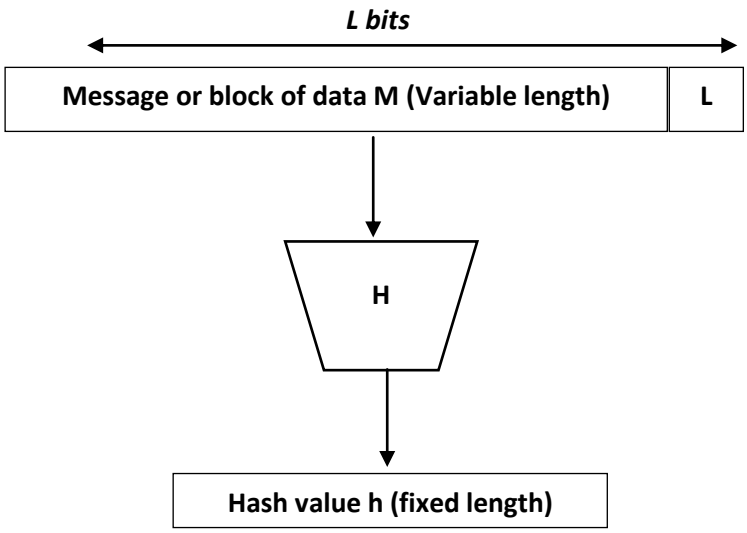

Figure 6: block Diagram of Cryptographic hash function

Some of the hash functions used are SHA-1, SHA-3, SHA-224,SHA-512, SHA-384 etc.,

IV. CONCLUSION

As the internet grows, the network and system security has become more vulnerable. The data's security is the most important thing. Cryptographic methods are used for improving security. This paper discussed the types cryptographic methods available and the importance of cryptography. Cryptography protects from some common attacks like virus infection, threats, intrusion). Other than cryptography, we have authentication, antivirus, firewalls and access control technologies to avoid network attacks. Cryptography

REFERENCES:

[1]. Zhijie Liu XiaoyaoXie, Member , IEEE ,School of Mathematics and Computer Science and Zhen Wang, Key Laboratory of Information Computing Science of Guizhou Province , Guizhou Normal University Guiyang , China, The Research of Network Security Technologies.

[2]. The Research of Firewall Technology in Computer Network Security, 2009 Second Asia-Pacific Conference on Computational Intelligence and Industrial Applications by Xin Vue, Wei Chen, Yantao Wang, College of Computer and Information Engineering Heilongjiang Institute of Science and Technology Harbin, China.

[3]. Martin, K.M, Everyday Cryptography Fundamental Principles and Applications, Oxford University Press,2012.

[4]. Paar, C.andPelzl, J, Understanding Cryptography, Springer,2010.

[5]. William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education 2013,6th Edition.