International Journal of Information Technology and Management

Vol. X, Issue No. XV, May-2016, ISSN 2249-4510

THE ROLE AND SIGNIFICANCE OF CRYPTOGRAPHY FOR NETWORK SECURITY IN CURRENT SCENARIO

www.ignited.in

International Journal of Information Technology and Management
Vol. X, Issue No. XV, May-2016, ISSN 2249-4510

The Role and Significance of Cryptography for Network Security in Current Scenario

Praful Kumar[1] Dr. Ramdip Prasad[2]

[1]Research Scholar, Magadh University, Bodhgaya

[2]Associate Prof., Dept. of Mathematics, J. N. L. College, Khagaul, Patna

Abstract – Network security is concerned with the protection of network resources against alteration, destruction and unauthorized use, cryptography and encryption are most critical components of network security. In my assignment, as a network security manager, this paper "explores the performance of various cryptographic schemes and evaluates web security and the security of wireless network system".

Keywords: Cryptography, Network Security, Protection

- X -

1. INTRODUCTION

Cryptology has two components, kryptos and logos. Cryptographic methods to certify the safety and security of communication and main goal is user authentication, data authentication such as integrity and authentication, non-repudiation of origin, and confidentiality and it has two functions encryption and decryption.

Secret key cryptography is identified as symmetric key cryptography. Both sender and receiver know same secret code described the key and messages are encrypted by the sender and use key, decrypted by the receiver. It use single key for both encryption and decryption. This method works healthy "if you are communicating with only a limited number of people, but it becomes impractical to exchange secret keys with large numbers of people". Secret key cryptography use is such as data encryption standard, advance encryption standard, Cast-128/256, international data encryption algorithm, and rivest ciphers etc.

Public key cryptography is called asymmetric encryption and use couple of keys one for encryption and another for decryption, Key work in pairs of coordination public and private keys. Public key can freely distributed the private key. If senders and receivers don't have to communicate keys openly, they can give private key to communication confidentially, Public key cryptography use for key exchange and digital signatures such as RSA, digital signature algorithm, public-key cryptography standard etc.

Hash functions use a mathematical transformation to permanently encrypt information. It also called message digests and one way encryption. Hash function use to provide a digital fingerprint of file contents and it is commonly employed by many operating system to encrypt passwords and it provide measure of the integrity of a file. It is also use message digest, secure hash algorithm, RIPEMD etc.

In IT security Management, Cryptography is both an art and a science—the use of deception and mathematics, to hide data, as in steganography, to render data unintelligible through the transformation of data into an unreadable state, and to ensure that a message has not been altered in transit. Another feature of some cryptographic systems is the ability to provide assurance of who sent the message, authentication of source, and proof of delivery.

The purpose of cryptography is to protect transmitted information from being read and understood by anyone except the intended recipient. Ideally, unauthorized individuals would never be able to read an enciphered message. In practice, reading an enciphered communication can be a function of time; however, the effort and corresponding time that is required for an unauthorized individual to decipher an encrypted message may be so large that it can be impractical. By the time the message is decrypted, the information within the message may be of minimal value.

Cryptography can be used to implement confidentiality, integrity, authentication, and nonrepudiation (enStratus, 2012, Ferguson, *et al.* 2010, Microsoft, 2005, Mogull, 2005, NIST, 2001).

2. THE ROLE OF CRYPTOGRAPHY:

Many feature combine to throw network security to the top issues in the organisation and face IS professional daily. Nowadays business operation decentralization and correspondence growth of computer network is the number one driver of concern about the network security. As far as security concern, many organisation networks are accidently waiting to occur, such accident will occur is impossible to predict but security breaches will occur. When organisation network security chooses is 100% involve cryptography technology. The following five basic uses of cryptography in network security solution are:

Confidentiality - Cryptography gives confidentiality through changing or hiding a message and protects confidential data from unauthorized access and use cryptographic key techniques to critically protect data;

Access control - Only authorized users (login & password) can access to protect confidential data etc. Access would be possible for those individual that had access to the correct cryptographic keys; (Mitchell, M, 1995)

Integrity - Cryptographic tools give integrity verify that permit a recipient to authenticate that message transformed and cannot prevent a message from being transformed but effective to identify either planned and unplanned change of the message; Authentication is the ability to verify who sent a message. Cryptographic function use different methods to certify that message is not changed or altered. These hash functions, digital signatures and message authentication codes (NIST, 2010, Olzak, 2006).

3. SIGNIFICANCE OF CRYPTOGRAPHY:

The requirement of information security within an organization has undergone two major changes in the last several years. The security of information felt to be valuable to an organization was provided primarily by physical and administrative documents, before the widespread of data processing equipment. An example of the latter is personnel screening procedures used during hiring process. An example of the former is the use of rugged filling cabinets with a combination lock for storing sensitive documents.

With the introduction of the computer, the need of automated tools for protecting files and other information stored on the computer became mandatory. This is required for a system like time-sharing system and also sometime need is even more acute for systems that can be accessed over a public telephone data network or internet [Electronic codebook, 2012, en Stratus, 2012, Ferguson, *et. al.* 2010)

The second major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer. Network security is required to protect data while in transit. In fact network security term is misleading since all business, government and academic organization interconnected their data processing equipment with a collection of interconnected networks.

Cryptography is a science that applies complex mathematics and logic to design strong encryption methods. Cryptography is also an art. Cryptography allows people to keep confidence in the electronic world. People can do their business on electric channel without worrying of deceit and deception.

When people started doing business online and needed to transfer funds electronically, the applications of cryptography for integrity began to surpass its use for confidentiality. In today's world thousands of people interact electronically every day by different means like e-mails, ATM machines, e-commerce or cellular phones. The rapid increase of information transmitted electronically resulted to an increased reliance on cryptography and authentication (Cipher-block chaining, 2012, Digital signature, 2012).

The simplest example of cryptography is transformation of information to prevent other from observing its meaning. Here, we prevent information from reaching an enemy in usable form. Confidentiality is the viewed as the central issue in the field of information protection. Secure communication is the straightforward use of cryptography. The key management problem has prevented secure communication from becoming commonplace. The development of public-key cryptography creates a large-scale network of people who can communication securely with one another even if they had never communicated before.

Early cryptographers used three methods for information encryption:

1. Substitution

2. Transposition

3. Codes.

Mon alphabetic ciphers

One of the earliest methods in cipher is a Caesar cipher with only 25 possible keys, which is far from secure. A dramatic increase in the key space can be achieved by allowing an arbitrary substitution.

Polyalphabetic Ciphers

To improve simple monoalphabetic technique is to use different monoalphabetic substitution as one proceeds through the plaintext message. This approach is called polyalphabetic substitution cipher. This technique has following features.

1. A key determines denotes which rule is used or chosen for a given transformation.

2. A set of related monoalphabetic substitution rule is used.

Transposition Ciphers

All the techniques we have seen so far include substitution on a cipher text symbol for a plain text symbol. A very different kind of mapping is achieved by performing permutation on the plain text letters. This technique is called transposition cipher.

4. CONCLUSION

Security of wireless network system play key role in every organisation and also implement all network security strategies for the organisation in present and future and secure network resources against alteration, destruction, and unauthorized use. Cryptography tools and web security tools are also very helpful to secure the network system and protect IT assets, confidential data and information.

REFERENCES

Cipher-block chaining. (2012). in *wikipedia.org*. Retrieved fromhttp://en.wikipedia.org/wiki/Block_cipher_modes_of_operation#Cipher-block_chaining_.28CBC.29

Digital signature. (2012). In *wikipedia.org*. Retrieved fromhttp://en.wikipedia.org/wiki/Digital_signature

Electronic codebook. (2012). In *wikipedia.org*. Retrieved from http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation#Electronic_codebook_.28ECB.29

enStratus. (2012). *enStratus Security Architecture.* Retrieved May 21, 2012, from enStratus Networks, Inc.: http://enstratus.com/media/document/1/security_architecture.pdf

Ferguson, N., Schneier, B., & Kohno, T. (2010). *Cryptography Engineering: Design Principles and Practical Applications* (Kindle ed.). Indianapolis, IN: Wiley Publishing.
Key escrow. (n.d.). In *Webopedia.* Retrieved fromhttp://www.webopedia.com/TERM/K/key_escrow.html

http://resources.infosecinstitute.com/role-of-cryptography/

http://www.simplilearn.com/cryptography-rrt3co34vd103-video

https://www.ukessays.com/essays/computer-science/the-role-of-cryptography-in-network-security-computer-science-essay.php

Microsoft. (2005, December). *Data Confidentiality*. Retrieved May 16, 2012, from MSDN: http://msdn.microsoft.com/en-us/library/ff650720.aspx

Mogull, R. (2005, August). *Management Update: Use the Three Laws of Encryption to Properly Protect Data.* Retrieved February 4, 2006, from Gartner: http://www.gartner.com

NIST. (2001, November 26). *Advanced Encryption Standard.*Retrieved May 15, 2012, from NIST Computer Security Resource Center: http://csrc.nist.gov/publications/fips/fips197/fips-pp.197.pdf

NIST. (2010, February 16). *Block Cipher Modes*. (N. I. Technology, Producer) Retrieved May 15, 2012, from Computer Security Resource Center: http://csrc.nist.gov/groups/ST/toolkit/BCM/index.html

Olzak, T. (2006, February). *Data Storage Security.* Retrieved May 19, 2012, from Adventures in Security:http://adventuresinsecurity.com/Papers/Data_Storage_Security.pdf