Cryptography: A Useful and Widely Used Tool in Today's Engineering Security

Ekwe A.O[1] , Okonba B.J[2]

[1,2] *Department of Electrical/Electronics Engineering, Mouau, Abia, Nigeria*

Abstract-Encryption is a useful and widely used tool in security engineering today. It involved the use of codes and a cipher to transform information into unintelligible data. This paper presents a systematic approach for data encryption. Ad-hoc networks that communicate between the nodes of the network using basic server client methodology were created first. These algorithms were found very effective and maintain security and also reduce the overhead. And, through the data encryption and decryption, the protection of data confidentiality, availability, authentication, authorization and integrity were achieved.

Keywords: Encryption; Availability; Confidentiality; Authorization.

I. INTRODUCTION

Cryptography is a useful and widely used tool in data security. It involved the use of codes and a cipher to transform information into unintelligible data. It secures information by protecting its confidentiality. It can also be used to protect information about the integrity and authenticity of data. Also, cryptography checksums helps in preventing undetected modification by encrypting the checksum in a way that makes the checksum unique. To protect against the chance of intruders modifying or forging information in transit, digital signatures are formed, by encrypting a combination of a checksum of the information and the author's unique private key [1]. Its application can also be seen in organization security, military communications, financial transactions, and so on [2]. Symmetric key is one of cryptographic methods algorithms widely used due to its efficiency and its capability of data protection [3]. It has a single key that is used by both communication partners. In a network, when a node wants to communicate with another node, a secret key (symmetric key) will be generated for their communication. Each sender has a unique secret key for communicating with the receiver and all information is encrypted using the corresponding secret key

In this paper, systematic approaches for encryption of data for wireless networks were reviewed.

II. BACKGROUND INFORMATION

The three basic security concepts relevant to data (information) are confidentiality, integrity and availability. The concepts relating to the people who use that data (information) are authentication, authorization, and non-repudiation. It is easy to gain unauthorized access to data in an insecure networked environment, and it is hard to catch the intruders.

During the 1980s, hackers and crimes relating to computers were beginning to emerge. The 414 gang are raided by authorities after a nine-day cracking spree where they break into top-secret systems. The Computer Fraud and Abuse Act of 1986 were created because of Ian Murphy's crime of stealing information from military computers [4]. Examples of important information that can be stolen are passwords, access control files and keys, personnel information and encryption algorithms.

For providing data security, a variety of cryptographic techniques are developed such as symmetric key, asymmetric key or the digital signature concept. According to the properties of public key-based certificate, a user T will use the public key issued by an authority and hash function to register with the authority [5]. Many key management functions have been developed such as rekeying or key revocation to reduce the overhead of key exchange [6]. The aim of encryption algorithms is to just encrypt a certain portions of the messages with less overhead consumption, but simultaneously, sufficient messages are encrypted to provide reliable safety to secure the transmitted message confidentiality.

III .DESIGN METHODOLOGY AND IMPLEMENTATION OF CRYPTOGRAPHY

To protect against the chance of intruders modifying or forging information in transit, digital signatures are formed, by encrypting a combination of a checksum of the information and the author's unique private key.

A. Encryption

The most basic building block of security is encryption, which scrambles a message before transmission, so that an interceptor cannot read the message as it flows over the network. However, the receiver knows how to decrypt (descramble) the message, making it readable again. Encryption provides privacy, which is called confidentiality. Both terms means that message can be transmitted without fear of being read by adversaries. Encryption methods falls into two categories (symmetric key encryption and public key encryption), with numerous specific encryption algorithms.

a. Symmetric key encryption

Symmetric key encryption has a single key that is used by both communication partners. Figure 1 shows a symmetric key encryption method.

- When party A sends to party B, party A encrypts with the single symmetric key and party B decrypts with the same key.
- When party B transmits to party A, in turn party B encrypts with the single symmetric key and also party A decrypts with the same key.

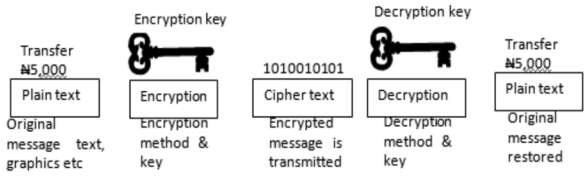

Figure 1: Symmetric key encryption

b. Public key encryption.

In public key encryption, when one party sends to another, there are two keys; the receiver public key and the receiver private key. Both of the keys are those of the receiver, not of the sender.

IV. RESULT AND DISCUSSION

A. Authorization

Authorization allows the network to permit or deny a person access to a particular database or services. It gives privileged access of specific data object like table, image etc. depending on the access role of the specific user

B. Authentication

Authentication is a means of access control that ensures that users are who they claim to be. Whether through password protection or intelligent tokens, the authentication process is intended to avoid the possibility that unauthorized users might access internal computing or network resources.

C. Confidentiality

When information is read or copied by only the authorized person, this is known as confidentiality.

D. Integrity

When information is modified in expected ways, the result is known as integrity. Ins case of data tampering , resulting from data corruption or any intrusion the same should be known to the owner of data or intended recipient.

E. Availability

When information is ever ready and accessible, this is known as availability.

V. CONCLUSION

From the result of the implementation of systematic approach for data encryption, it is evident to say that the most prevalent method for securing our data is through cryptography. Securing data through cryptography mechanism results to authorization, availability, integrity, confidentiality, and authentication.

REFERENCES

[1] Kaufman, C., Perlman, R., and Speciner, M., Network Security: Private Communication in a public world, Prentice-Hall, Eaglewood Cliffs, NJ, 1995

[2] A. Boukerche, "Handbook of Algorithms for Wireless and Mobile Networks and Computing", CRC Chapman Hall, 2005

[3] A. Boukerche, "Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks", Wiley & Sons, 2008.

[4] McDaniel, P. (2006, December 6). *Physical and digital convergence: Where the Internet is the enemy*. Eighth International Conference on Information and Communications Security. Retrieved April 24, 2009, at http://discovery.csc.ncsu.edu/ICICS06/Keynote McDaniel.html

[5] Yonglin Ren, Azzedine Boukerche and Lynda Mokdad, "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Network" *proceedings of IEEE WCNC*, pp. 7-11, 2011

[6] A. J. Prakash, and V. R. Uthariaraj, "Multicrypt: A Provably Secur Encryption Scheme for Multicast Communication", Proceedings of 1st *Int'l Conference on Networks and Communications*, pp. 246–253, 2009.

AUTHORS

Engr. Ogbonna A. Ekwe is a highly motivated Electronic Engineer with a bias in Communications. He obtained his Bachelor of Engineering (B.Eng.) degree in Electronics Engineering at the University of Nigeria, Nsukka in 2005, and a Master's Degree in Electronic Communications and Computer Engineering from University of Nottingham, United Kingdom in 2011. He possesses many years of experience in different work environments with excellent team leadership qualities. Engr. Ekwe, O. A is presently lecturing in the department of Electrical/Electronic Engineering, Michael Okpara University of Agriculture, Umudike, Abia State, Nigeria. His research interest are in the areas of Interference management for cellular communication, Communication techniques for next generation cellular systems, Channel fading mitigation for fixed and mobile wireless communication systems, etc**.**

Brown okonba .J Received his B.Eng. degree in Electrical and Electronics Engineering from University of Portharcourt, Rivers State Nigeria in 2002, and currently doing a Master of Engineering degree in Electronics and Communication Engineering, Michael Okpara University of Agriculture, (MOUAU) Umudike, Abia State Nigeria. He is a member of Nigerian Society Engineers. His research interests are in the fields of, Electronic and Communication Systems design, Security system design, Expert systems and Artificial Intelligence, Network design etc.