IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 05, Issue 01 (January. 2015), ||V1|| PP 40-43

Computerized network security and cryptography

Motea Abdelaziz Mohammed Noman1,Saifeldeen Fatooh2,
Abdelrasoul Jabar Alzubaidi 3
1 PHD candidate motiea@hotmail.com , 2 Dean of Emarat college , 3 Sudan University of science and Technology- Engineering College- Electronics Department Rasoul46@live.com

Abstract: For the first few decades of their existence, computer networks were primarily used by university researchers for sending e-mail and by corporate employees for sharing printers. Under these conditions, security did not get a lot of attention. But now, as millions of ordinary citizens are using networks for banking, shopping, and filing their tax returns, network security is looming on the horizon as a potentially massive problem .The requirements of information security within an organization have undergone major changes in the last several decades .With the introduction of computer the need for automated tools for protecting files and other information stored on the computer became an evident .This is especially the case for a shared system, such as time sharing system and the need is even more acute for systems that can be accessed by any user . This paper deals with building a secured algorithm to ensure data security in the computer network.

Keywords: encryption, data, algorithm, computer network,

I. INTRODUCTION

Security is a broad topic and covers a multitude of sins. In its simplest form, it is concerned with making sure that nosy people cannot read, or worse yet, secretly modify messages intended for other recipients. It is concerned with people trying to access remote services that they are not authorized to use. Most security problems are intentionally caused by malicious people trying to gain some benefit, get attention, or to harm someone. Network security problems can be divided roughly into four closely intertwined areas: secrecy, authentication, nonrepudiation, and integrity control. Secrecy, also called confidentiality, has to do with keeping information out of the hands of unauthorized users. This is what usually comes to mind when thinking about network security. Authentication deals with determining whom you are talking to before revealing sensitive information or entering into a business deal. Nonrepudiation deals with signatures.

Secrecy means that only the sender and intended receiver should be able to understand the contents of the transmitted message. Because eavesdroppers may intercept the message, this necessarily requires that the message be somehow encrypted (disguise data) so that an intercepted message can not be decrypted (understood) by an interceptor. This aspect of secrecy is probably the most commonly perceived meaning of the term "secure communication." Note, however, that this is not only a restricted definition of secure communication, but a rather restricted definition of secrecy as well.

Authentication means that both the sender and receiver need to confirm the identity of other party involved in the communication - to confirm that the other party is indeed who or what they claim to be. Face-to-face human communication solves this problem easily by visual recognition. When communicating entities exchange
messages over a medium where they can not "see" the other party, authentication is not so simple. For instance, a received email containing a text string saying that the email came from a friend , should be assured that it is indeed came from that friend. Figure (1) below demonstrated data hacking by an intruder.

Figure (1) data hacking by intruder

II. METHODOLOGY

The system design is divided into parts; hardware and software. In the hardware, two sets of personnel computers interfaced to RF transceivers are used . The two sets are linked by an RF media for the data communication. The two sets of the personnel computer plus the RF transceiver form a model for a secured data exchange.

A software code is developed in the personnel computer to encrypt the data . The code of encryption is written in Turbo C++ language (TC++). A decryption code is implemented in the receiving part based on the encryption technique used .

III. SYSTEM LAYOUT

The aim of the hardware and software design is to illustrate the usage of the encryption and decryption processes in the computer networks..The electronic devices required to construct the encryption and decryption system is a personnel computer, RF transceiver , plus interconnection links and lab link cables. The block diagram of the hardware implementation of the entire system is shown in Figure (2) below.

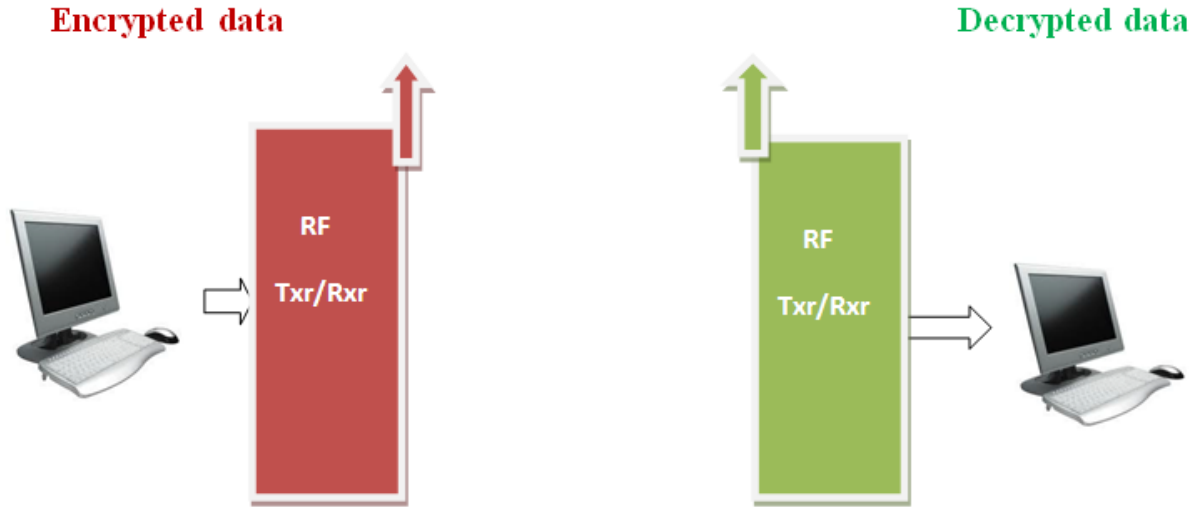

Figure (2) Block diagram of the system

The input system consists of two sets of electronic blocks. Each set consists of a personnel computer plus an RF transceiver The mechanism of the system operation is based on XORing a group of four bytes with a predefined table containing four ASCII coded bytes. The encryption operations are illustrated in equations (1) to (3) below:

Encrypte-byte1 = (byte-1) XOR (ASCII of M) **…… …… (1)**
Encrypte-byte2 = (byte-2) XOR (ASCII of A) **…… …… (2)**
Encrypte-byte3 = (byte-3) XOR (ASCII of M) **…… …… (3)**
Encrypte-byte4 = (byte-4) XOR (ASCII of N) **…… …… (4)**

The hardware components are :

- Personnel computer (PC) :

A PC furnished with a serial and parallel ports is used for interfacing with the RF transceiver.

- RF transceiver:

The RF transceiver performs the task of data transmission and reception.

- Lab links :

Lab links are sort of cables that connects the computer port to external electronic devices .They are used for conveying the stream of data from the PC to the RF transceiver.

IV. SOFTWARE PROGRAM AND ALGORITHM

To achieve the objective of the real time encryption procedure , we need to go through three steps as follows:

1. Step one is developing a Turbo C++ program in the computer .
2. Step two includes implementing the encryption strategy.
3. Step three includes activation of the RF transceiver..

Similar steps should be conducted for the decryption procedure.

The algorithm performs a real time encryption. The algorithm contains two subroutines . The subroutines are called one after the other. The first subroutine processes the data encryption strategy. The second subroutine outputs a byte from the data register of the LPT plus transmission of the encrypted byte by the RF transceiver..The execution of the two subroutines means performing a complex encryption procedure based on a set of four bytes table. The processing is repeated till the end of the data stream coming from the PC. The star '*' in the plain text table denotes the bytes termination. The algorithm is :

Start
Initialization :
… Program LPT port as output..
… Clear the data register of the LPT port.
... Generate ASCII coded four bytes table.(M , A , M , N)
… ASCII coded bytes table Pointer = 1.
... Generate a hundred bytes plain text table ended with '*'.
… Plain text table pointer = 1 .
… Reserve a byte location for the (encrypted byte).
… Disable the RF transceiver.

Encryption strategy:
…Access the first byte in the plan text table.
Byte encryption :
.. If a byte is star '*' go to end of program.
.. Call byte encryption subroutine.
.. Call encrypted byte output subroutine.
.. If (ASCII code table pointer > 4) , then put ASCII code table pointer to location 1.
.. Go to byte encryption .
End

Byte encryption subroutine :
.. Encrypted byte = (Plain text byte) XOR (ASCII code byte)
.. Increment pain text table pointer.
.. Increment ASCII code table pointer.
Return.

Encrypted byte output subroutine:
.. Output the encrypted byte to the data register of the LPT port (address 378 Hexadecimal).
.. Enable the RF transceiver for byte transmission.
RF transceiver:
.. If byte transmission is not acknowledged , then go to RF transceiver.
.. Disable the RF transceiver.
Return.

V. RESULTS

The system performs a complex non standard data encryption strategy. The generated four ASCII code bytes table is considered the essential part in the adapted encryption strategy..Table (1) below shows the results when operating the system .

Table (1) The results when operating the system

Plain text byte in (HEX)	(Byte) XOR (first byte in ASCII table 'M')	(Byte) XOR (second byte in ASCII table 'A')	(Byte) XOR (third byte in ASCII table 'M')	(Byte) XOR (fourth byte in ASCII table 'N')	Encrypted byte in (HEX)
41	0C				0C
4F		10			10
4C			01		01
5A				14	14

The processing indicated in table (1) will be repeated 25 times. The 25 times repetition comes from dividing (100) by (4) .

VI. CONCLUSION

The system design that enabled the data encryption and transmission adapted a non standard encryption strategy. The number of bytes in the generated ASCII code table equals four bytes while the assumed number of bytes in the plain text equals hundred..The assumed byte numbers in the two tables can be changed as well as the gate used in the algorithm .This means that the strategy is flexible and any change will not affect its principle .This type of encryption carries a high degree of data transmission security.

REFERENCES

[1] C. Gentry, Fully homomorphic encryption using ideal lattices, Symposium on the Theory of Computing (STOC), 2009, pp. 169-178.
[2] P. Paillier, Public-key cryptosystems based on composite degree residuosity classes, in Advances in Cryptology EUROCRYPT'99, LNCS 1592, pp. 223–238,
[3] Springer, New York, NY, USA, 1999.
[4] Josh Benaloh, Dense Probabilistic Encryption, SAC 94, pages 120–128, 1994.
[5] I. Damg˚ard and M. Jurik. A Length-Flexible Threshold Cryptosystem with Applications.ACISP '03, pp. 350–356.
[6] A. Kawachi, K. Tanaka, K. Xagawa. Multi-bit cryptosystems based on lattice problems. PKC '07, pp. 315–329.
[7] C.A. Melchor, G. Castagnos, and P. Gaborit. Lattice-based homomorphic encryption of vector spaces. ISIT '08, pp. 1858–1862.
[8] Craig Gentry Shai Halevi, Implementing Gentry's Fully-Homomorphic Encryption Scheme Preliminary Report, August 5, 2010. https://researcher.ibm.com/ researcher/files/us-shaih/fhe-implementation.pdf
[9] Frederiksen, T.K., A Practical Implementation of Regev's LWE-based Cryptosystem,2010.
[10] William Stallings, Cryptography and Network Security Principles and Practice, 5th Edition , Prentice Hall , 2011.