International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 5(2), September - October 2015 ISSN 2278-6856

NETWORK SECURITY USING ENCRYPTION TECHNIQUES

Ajay Kumar*, Preeti Yadav#

*Asst. Prof. in IGU Meerpur Rewari(Haryana)

#Asst. Prof in Govt Girl college Gurgoan(Haryana)

Abstract

Network Security using Encryption Techniques is a concept to protect Information over wireless network. Information security is the process of protecting information by protecting its availability, privacy and integrity. Access to stored information on computer databases has increased greatly. To provide security to information there are various types of techniques as traditional cryptographic methods like Substitution techniques, Transposition techniques, hashing Functions and algorithms like DES, RSA, AES, IDEA, ECC etc. are used. This paper focuses mainly on the different kinds of encryption techniques that are existing, and comparative study all the techniques together as a literature survey. Aim an extensive experimental study of implementations of various available encryption techniques.

Keywords:- Encryption, Decryption, Network Security, Plain Text, Cipher Text, Key.

I. INTRODUCTION

In our modern age of telecommunications and the Internet, information has become a precious commodity. Sometimes it must therefore be kept safe from stealing - in this case, loss of private information to an eavesdropper. There are many features to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential feature for secure communications is that of cryptography [1], which not only protects data from stealing or modification, but can also be used for user authentication. The main aim of cryptography is to protect data transferred in the likely presence of an enemy. In other words, Cryptography is the art of enciphering and deciphering of encoded messages [2]. It can be seen as an ancient art that has taken many forms over the years. Encryption started with simple pen-and-paper methods based on letter subs substitutions.

BASIC TERMS USED IN CRYPTOGRAPHY

- **Plain Text:** The original message that the person wishes to communicate with the other is defined as Plain Text. In cryptography the actual message that has to be send to the other end is given a special name as Plain Text. For example, Alice is a person wishes to send "Hello Friend how are you" message to the person Bob. Here "Hello Friend how are you" is a plain text message.
- **Cipher Text:** The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, "Ajd672#@91ukl8*^5%" is a Cipher Text produced for "Hello Friend how are you".
- **Encryption:** A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send confidential messages through an insecure channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side.
- **Decryption:** A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.
- **Key:** A Key is a numeric or alpha numeric text or may be a special symbol. The Key is used at the time of encryption takes place on the Plain Text and at the time of decryption takes place on the Cipher Text. The selection of key in Cryptography is very important since the security of encryption algorithm depends directly on it. For example, if the Alice uses a key of 3 to encrypt the Plain Text "President" then Cipher Text produced will be "Suhvlghqw".

II. CLASSIFICATION OF CRYPTOGRAPHY

Encryption techniques can be classified in two categories- Symmetric and Asymmetric key encryption

A. Symmetric Encryption: In symmetric Cryptography the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc. There are various symmetric key algorithms such as DES, TRIPLE DES, AES, RC4, RC6, and BLOWFISH [3].

B. Asymmetric Encryption: Asymmetrical encryption methods, also referred to as Public Key encryption systems, were developed in 1976 by Whitefield Diffie and Martin Hellman [4].

The principle of public key encryption is that parties, the sender as well as the receiver, have a pair of keys. The one key does not have to be kept secret and is called t he public key. The two different keys held by the parties have different uses – one is used for encryption and the other for decryption. The encryption key is the public key, while the decryption key is the "private" key. The private key must be kept secret. The public and the private key are mathematically related so that anything encrypted with the one can be decrypted with the other. The sender takes the receiver's key, which is publicly available on a website for instance, and encrypts a message. He then sends it to the receiver who will only be able to decrypt the message with his private key. The main advantage of this method is that the sender and receiver do not have to exchange keys at any time. Public key encryption thus solves the key distribution problem of symmetric encryption, but unfortunately not without potential problems. The difficulty of the mathematical functions that public key encryption relies on can be seen as relative.

At the moment there does not exist a mathematical algorithm that can factorize a number into prime numbers quickly. But if a mathematician were to develop such an algorithm, the RSA system will be compromised and many institutions that use the algorithm will be vulnerable.

Another issue with public key encryption is the fact that at the moment there does not exist a central certificate authority, only a decentralized model. This poses a problem in that if a sender wants to acquire and authenticate a receiver's public key, he has to do so at a certificate authority. A trust relationship is needed between certificate authorities, or alternately, only one certificate authority should exist.

III. PREVIOUSLY RELATED WORKS

This subsection describes and examines previous work on most common algorithm implementation for both software and hardware approaches. The metrics taken into consideration are processing speed, throughput, power consumption, and packet size and data types.

Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices has done by D. S. Abdul. Elminaam et.al.(2009) presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points can be concluded from the Experimental results. First; in the case of changing packet size with and with out transmission of data using different architectures and different WLANs protocols, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Second; in case of changing data type such as audio and video files, it is found the result as the same as in text and document. In the case of image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption. He is found that 3DES still has low performance compared to algorithm DES. Third point [5].

When the trans mission of data is considered there was insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). There is insignificant difference between open key authentications and shared key authentication in ad hoc Wireless LAN connection with excellent signals. In case of poor signal it is found that, transmission time increased minimum by 70 % over open sheered authentication in ad hoc mod. Finally –in the case of changing key size – it can be seen that higher key size leads to clear change in the battery and time consumption.

Comparison of Data Encryption Algorithms has done by Simar Preet Singh, and Raman Maini -The simulation results showed that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results compared to other algorithms, since it requires more processing power. The first set of experiments was conducted using ECB Mode. The results show the superiority of Blowfish algorithm over other algorithms in terms of processing time. It shows also that AES consumes more resources when data block size is relatively big. Another point can be noticed here that 3DES requires always more time than DES because of its triple phase encryption characteristic. Blowfish, which has a long key (448 bit), outperformed other encryption algorithms. DES and 3DES are known to have worm holes in their security mechanism; Blowfish and AES do not have any so far [5]. As expected, CBC requires more processing time than ECB because of its key-chaining nature. The result indicates also that the extra time added is not significant for many applications, knowing that CBC is much better than ECB in terms of protection.

Evaluation of Performance Characteristics of Cryptosystem Using Text Files designed by challa Narasimham and Jayaram Pradhan (2008) - They performed the performance comparison for variable sized text files as input. An analysis on computational running times results in significant difference among the methods. He believe in that the performance of DES, especially in decryption method is very high than the alternatives. Despite the key distribution, DES is more suitable to the application, which has the decryption as the highest priority. He has proposed and performed the test cases on the two PKCS methods i.e., RSA and NTRU Though the encryption, decryption and complexity are high in NTRU, the RSA provides the highest security to the business application. He presented all these parameters with computational running times for all the methods, so as to select the appropriate method [6]. Abdel-Karim and his colleague Al Tamimi presented simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm? AES showed poor performance results compared to other algorithms since it requires more processing power.

Using CBC mode has added extra processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data blocks. The results showed that Blowfish has a very good performance compared to other algorithms. Also it showed that AES has a better performance than 3DES and DES. Amazingly it shows also that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [7]. P. Prasithsangaree and his collegeue P. Krishnamurthy have analyzed the Energy Consumption of RC4 and AES Algorithms in Wireless LANs in the year 2003. They have evaluated the performance of RC4 and AES encryption algorithms. The performance metrics were encryption throughput, CPU work load, energy cost and key size variation. Experiments show that the RC4 is fast and energy efficient for encrypting large packets. However, AES was more efficient than RC4 for a smaller packet size. From the results, it appears that we can save energy by using a combination of RC4 and AES to provide encryption for any packet size. The tradeoffs with security are not completely clear [8]. Comparative Analysis of AES and RC4 Algorithms for Better Utilization has designed by Nidhi Singhal, J.P.S.Raina in the year (2011). The performance metrics were throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Experiments show that the RC4 is fast and energy efficient for encryption and decryption. Based on the analysis done as part of the research, RC4 is better than AES.we compare the encryption time of AES and RC4 algorithm over different packet size. RC4 takes less time to encrypt files w.r.t. AES. In AES, CFB and CBC takes nearly similar time but ECB takes less time then both of these [9].

IV. EVALUTION OF ENCRYPTION TECHNIQIES

To effectively evaluate encryption techniques, the different encryption techniques must be examined and evaluated according to criteria, especially from a business perspective. Some of the evaluation criteria were taken from the list of specifications that NIST compiled when they evaluated the proposals for the Advanced Encryption Standard [11]. Further criteria were taken from a paper by Bruce Schneier, entitled "Security in the Real World: How to evaluate security technology" [10].

The criteria are as follows:

- **Robustness** – With the advances in technology it is of vital importance that any encryption system is robust enough to withstand the advances in technology. The more an encryption technique relies on mathematics, the less the robustness.
- **Availability** – Some of the encryption techniques discussed have been around for years, but not all are fully functional yet. Those that have been around for some time may have the advantage of being "tried-and-tested", while some organizations are not familiar with others.
- **Integration [11]** – The integration level of an encryption system will depend on how easily it can be integrated at the application level. The encryption technique must be able to be implemented on software and hardware.
- **Distribution** – With present day technology evolving around the Internet and networks, it is important that encryption techniques work on an entire network, not only on a point-to-point basis. When one broadcast a message through a network all the intended recipients should get the same encrypted, secure message.
- **Time efficiency [11]** – Users expect encryption to be immediate, otherwise the process is cumbersome. The time efficiency of an encryption technique measures how long it takes to encrypt and decrypt information.
- **Flexibility [11]** – The flexibility issues of an encryption technique refer to the use of keys and whether the key lengths are set, or whether different key lengths can be used.
- **Reliance on users [10]** – In many systems, security is based on user-remembered secrets. When a user has to choose a key or a password, he/she usually chooses something that he/she will be able to remember. The issue is whether the encryption techniques will fail if a user has chosen a "bad" password or key.
- **Tested [10]** – Before an encryption technique can be made publicly available for purchasing it has to be tested thoroughly. The amount of testing done in a laboratory or in a public symposium may influence the security of an encryption technique.
- **Governmental support [10]** – In our society, businesses may be inclined to make use of an encryption technique if the government regards it as being secure. Some encryption algorithms have been approved by the government.
- **Security [11]** – The main, and most obvious, criterion for an encryption technique is the security of the algorithm. Has the algorithm been compromised? Is there any reason why the security of the algorithm is doubted? Most organizations invest in encryption techniques to ensure the confidentiality of their information, and this is the deciding factor.

V. CONCLUSION

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access, and consistent and continuous monitoring and measurement of its effectiveness (or lack) combined together. We have studied various cryptographic techniques to increase the security of network.

REFERENCES

[1]. C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key- distribution Protocols," Phys. Rev. Avol. 73, 2006.

[2]. Whitman, M.E., Mattord, H.J., Principles of Information Security, Thomson Course Technology, 2003
[3]. Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.
[4]. Tudor, J.K., Information Security Architecture: An integrated approach to security in the organization, Auerbach Publications, 2000
[5]. Simar Preet Singh, and Raman Maini "COMPARISON OF DATA ENCRYPTION ALGORITHMS" International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127
[6]. Challa Narasimham, Jayaram Pradhan, "EVALUATION OF PERFORMANCE CHARACTERISTICS OF CRYPTOSYSTEM USING TEXT FILES" Journal of Theoretical and Applied Information Technology,pp55-59 2008.
[7]. Abdel-Karim Al Tamimi "Performance Analysis of Data Encryption Algorithms"
[8]. Prasithsangaree.P and Krishnamurthy.P(2003), "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM 2003, pp. 1445-1449.
[9]. Nidhi Singhal1, J.P.S.Raina2, Comparative Analysis of AES and RC4 Algorithms for Better Utilization", International Journal of Computer Trends and Technology- July to Aug Issue 2011 pp177- 181.
[10]. Schneier, B., Security in the Real World: How to Evaluate Security Technology, Computer Security Journal, Volume 15, Number 4, 1999
[11]. National Institute of Standards and Technology, http://csrc.nist.

AUTHOR

AJAY KUMAR: Ajay Kumar did his MCA from LIMAT Faridabad, Haryana (India) and M.Tech (Computer Science) from GITAM Jhajjar, Haryana (India). He has teaching experience about 4 years in India. He has UGC NET qualified. At present he has been working as Assistant Professor (Guest Faculty) in Department of Computer Science & Application, Indira Gandhi University, Meerpur, Rewari (India). His research interest in Networks Security and database management System. He has about 5 international journal publications.