A Valuable Exercise of Multi Encryption Standards with Data Streams in TCP Transmission

Achal Agarwal[1], Gulista khan[2]
[1]*M.Tech Scholar, Deptt. Of Computer Science, TeerthankarMahaveer University, Moradabad, India.*
[2]*Assistant Professor, Deptt. Of Computer Science, TeerthankarMahaveer University, Moradabad, India.*
[1]achalagarwal3@hotmail.com, [2]gulista.khan@gmail.com

***Abstract*-In this era of Information, where all the communication and records are digitized, the need for secured media is eminent for transactions and confidential files. Information security is vital for many systems like core banking, defence systems, Satellite control systems, etc. wherein breach of secure data can lead to major consequences. Hence there is a demand for a strong encryption scheme which is very inflexible to snap[1].**
For this purpose only a lot of encryption algorithms were formed in past, but the main confront was the security of the encryption Algorithm which we use[2]. The recent advancement in the field of network and information security came when most of the government organisation along with defence faced issues regarding data interruption[2].

In this paper we will propose a layout to use multiple encryption standards thus providing maximum security to data while transmission. The two main features that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. This paper provides a new idea of using already established Algorithms to get maximum level of security in TCP transmission.

Keywords: Cryptography, Encryption, Random Hash Function, Security, Secure TCP Transmission.

I.INTRODUCTION

To ensure the security, the process of converting the plain text to cipher text is called encryption[3]. Although this conversion idea is old, the way of encryption should not be susceptible to attacks. Caesar's cipher method, poly alphabetic substitution method, bit-level encryptions like substitution box, permutation box, encoding, and rotation are some of the unadventurous encryption methods which were used around first world war. These methods are easy to put into practice and can be splintered easily with the high end technologies. The objective of this research is to develop multi encryption scheme that can be used to encrypt top-secret files including text, images and multimedia files while transferring it over TCP connection.

II. RELATED WORK

Most of the existing schemes are susceptible to attacks andit is breached at some point of time by cryptanalyst analysing them. Various cryptanalysis techniques are available to decrypt most of the encryption standards at one point of time4,5,6. Eachand every algorithm either it may be block cipher or streamcipher or any other cipher types can be easily attacked byperforming various cryptanalysis techniques like linearcryptanalysis, n-gram analysis, meet in the middle attack,brute force attack, Man in the middle attack etc... Misfortune tosay that intruders can breach any systems even it has a multifaceted algorithmic design. Most of the famous algorithms of all ages were breached easily by eavesdroppers at one stage and weare evidencing it in our day-to-day daily life. This happensbecause of its platform dependency and the emerging trend ofopen software solutions available all over the world. Despitesome systems are developed to support cross platform, theydo not use multi level encryption.

This is because the algorithmicdevelopers always believe in their own encryptionformulas and firmly attached to the tradition of modifying orusing or creating a single algorithm which is not secure aftera period of time. It is quite obvious to digest the fact it is easyto cryptanalysis any algorithm within months as soon as theyare adapted to practical use. Even though very few systemssupport multiple encryptions, they do not use randomizedencryption hence can be cracked as soon as they came toknow the algorithms used to build multi level encryption.Most of the existing systems support text encryption preferablythan other media types. Since the intruders and eavesdroppershad shown their excelling skills towards breakingthe encryption algorithms almost in all important and sensibleareas like Banking, Military, Defence, Networks, a needfor "practically strong and infeasible to get attacked" algorithmbecomes vital. This paper suggests one such techniquewhich never ever gives a clue of the encryption patternadopted, no of encryption algorithms used, their order of execution[7].

III. CURRENT SYSTEM

The current system which is different and efficientfrom the existing systems as follows,

1. System is developed in such a way that it is platformdependent.

2. It was developed through multiple encryption algorithmswhereas the existing systems are always focussed asencryption at single level.

3. it uses a Random function generator which generatesa n-digit random number based upon the n-number ofEncryption algorithms used. Thus generated n-digitnumber determines the order of selecting Encryptionalgorithms. Since the number determining the order iscompletely random it is infeasible to crack the order ofexecution.

4. Another significant feature of this random generator is,it is totally depends upon the key phrase that we provide and hence for various phrases it produce differentorder, which results the intruder in a more worse scene.

5. Moreover the number of encryption algorithm that we use, their order of execution will always remain a secret and hence it don't even leave a single chance for the eavesdroppers to make a guess on our system and hence the security offered is up to the best of ever provided.

6. This proposed system is developed in order to support not only text files but also images and media files. But still many of the existing systems are developed in order to suit basic text formats.

IV. DRAW BACKS OF CURRENT SYSTEM

1. The major drawback of this above said system was developed in such a way that it was platform dependent, while in the current era of technology, it is highly unpredictable that both the sender and receiver will be using same platform.

2. It was developed through multiple encryption algorithms being applied on same data stream thus maximising the time latency involved.

3. This system uses a Random function generator which generates a n-digit random number based upon the n-number of Encryption algorithms used. But it was not clarified how the authorised user will be able to decrypt the receiving stream means how many decryption algorithms he or she need to apply and in which order.

4. It is totally dependent upon the key phrase that was provided to it and hence producing different order for various phrases, which results the receiver in a worse scene.

5. Moreover the number of encryption algorithm that it uses, their order of execution will always remain a guess only and hence it don't even leave a single chance for the receiver to make a guess on such system and hence decrypting the stream at receiver end will be worst.

V. PROPOSED SYSTEM

The proposed research work here is based on the principle of uncertainty. Till now the major challenge is the security of keys, because either whole data is being encrypted using same keys or a same sequence of encryption standards is followed. We want to introduce a new idea in which we are not going to follow the same pattern for each of the packet.

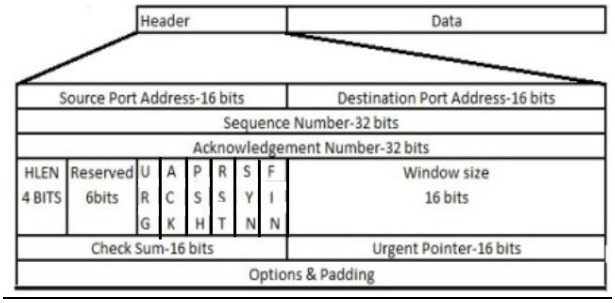

Fig-1: TCP header in IPV4

In TCP transmission in **IPV4** our whole data is being divided in data stream or packets. Each data stream will carry a TCP header, which carries its sequence num too (TCP header is shown in figure). We will feed our system with N number ($0<N<32$, converted into binary number, as N will be between of 2^0 and 2^5) of encryption schemes along with their sequence number (binary digits). While our data will be divided in data stream, at the same time we will generate a pseudo random num in between of 1 and N. A separate file will be maintained which will carry N encryption standards along with their keys called key phrase.

Sequence Num (6 Digit Binary)	Algorithm	Key-1	Key-2
010101	RSA		
101010	DES		
110011	3DES		
111010	IDEA		

Fig-2: Key phrase

As soon as data is divided in data streams, a pseudo random number will be generated for each of the data stream, and the corresponding encryption scheme will encrypt that particular data stream.

Now the overhead will be at decryption side, how it will be known that which data stream is encrypted using with encryption scheme, for this we will use 6 bits, which is reserved in TCP header for the future use. The pseudo random number which is generated for each of the data stream, which carries information about which encryption standard will be applied to that data stream, will be stored in those 6 bits, which is reserved for future use.

The reverse decryption scheme can be followed for retrieving of data. First of all check for these 6 bits, which will give information about the encryption scheme for that

particular data stream, corresponding algorithm is applied for the decryption purpose.

We are here providing a brief review of such Multi Encryption System.

1. Platform independency: This System will be developed in such a way that it can provide platform independency.

2. Use of multiple encryption algorithms: It will be developed through use of multiple encryption algorithms but one for one data stream only to provide maximum level of security whereas the existing current systems were more focussed on applying multi encryption at single level to provide maximum level of security.

3. Random Number Generator: This system uses a Random Number Generator which generates a n-digit random number based upon the n-number of Encryption algorithms used, thus generating n-digit number determining the selection of Encryption algorithm being used for particular data stream. Since the number determined is completely random making it infeasible to crack the data stream.

4. Dependency on the key phrase: Another significant feature of this random generator is, it is totally dependent upon the key phrase that was provided to it and hence producing different number for various data streams, which results the cryptanalyst in a worse scene.

5. Order of execution: Moreover the number of encryption algorithm that it uses, their order of execution will always remain a secret and hence it don't even leave a single chance for the cryptanalysts to make a guess on such system and hence the security offered was up to the best of ever provided.

6. Supported Media: The above system was developed in order to support not only text files but also images and media files mean all digitized data.

VI. ADVANTAGES OF PROPOSED SYSTEM

We are here providing few advantages for Multi Encryption System.

1. Platform independency: because of the header will be same in all platforms while using TCP Transmission..

2. Use of multiple encryption algorithms: It will be developed through use of multiple encryption algorithms but one for one data stream only to provide maximum level of security.

3. Random Number Generator: This system uses a Random Number Generator for selection of encryption algorithm from key phrase involved making it infeasible to crack all the data stream as all will be encrypted using different encryption algorithms.

4. Dependency on the key phrase: Totally dependent upon the key phrase that was provided to it and hence producing different number for various data streams, which results the cryptanalyst in a worse scene.

5. Order of execution: Moreover the number of encryption algorithm that it uses, their order of execution will always remain a secret and hence it don't even leave a single chance for the cryptanalysts to make a guess on such system and hence the security offered was up to the best of ever provided.

VII. FUTURE ENHANCEMENTS

The system can be easily modified to accept any encryptionalgorithm which is framed in future. Just by adding or removinganother algorithm in key phrase, any number of algorithmscan be included or reduced. Though the system is designedis currently for IPV4, which can be further extended to IPV6 or as another system for IPV6 can be introduced.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security:Principles and Practices*, 2nd ed., Prentice Hall,1999.
[2] William Stallings, Network Security Essentials : Application and Standards, Fourth ed.,Pearson, 2012.
[3] Kaufman Charlie, Perlman Radia, SpecinerMike:Network Security, PRIVATE Communication in a PUBLIC World,second edition by PHI,2013.
[4] Walter Tuchman , "*A brief history of the data encryptionstandard*",Internetbesieged:countering cyberspacescofflaws. ACM Press/Addison-WesleyPublishing Co. New York, NY, USA, pp. 275–280,1997.
[5] Rivest, R.; A. Shamir; L. Adleman ,"*A Method forObtaining Digital Signatures and Public-KeyCryptosystems*", Communications of the ACM 21(2): 120–126,1978.
[6] 6Sinkov, Abraham; Paul L. Irwin," *ElementaryCryptanalysis: A Mathematical Approach*", MathematicalAssociation of America. pp. 13–15,1966.
[7] SairamNatarajan et al, A Novel Approach for Data Security Enhancement Using Multi Level Encryption Scheme, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (1) , 2011, 469-473.