Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 11, November 2013, pg.331 – 338

RESEARCH ARTICLE

An Enhanced Security for TCP/IP Protocol Suite

Dr. M. Anand Kumar[1], Dr. S. Karthikeyan[2]

[1]Department of Information Technology, Karpagam University, India

[2]Department of Information Technology, College of Applied Sciences, Oman

anandm_ss@yahoo.co.in, skarthi@gmail.com

Abstract— Network and internet applications are growing rapidly in the recent past. These applications are used by thousands of users and controlled by different administrative entities. It is mainly used as an efficient means for communication, entertainment and education. With the rapid growth of internet, there is a need for protecting confidential data. The Internet was however originally designed for research and educational purpose, not for commercial applications. So internet was not designed with security in mind. As the internet grows the existing security framework was not adequate for modern day applications. The main reason was due to the lack of security services in the TCP/IP Protocol Suite. The lack of authentication mechanism of TCP/IP Protocol Suite is mainly due to the poor protection mechanism of packets and broadcast nature of the lower layer protocols. Moreover there is no protection for the application layer of the network model. This paper presents the proposed security architecture for the TCP/IP Protocol Suite.

Keywords— Internet; Network security; ICMP; IP; Cryptography

I. INTRODUCTION

This work aims to investigate a large number of security approaches adopted in the TCP/IP Protocol Suite and to propose a new architecture for the existing model. The first contribution of this work was to provide the security for applications of the application layer protocols Second aspect of the work was to enhance the security for the internet control message protocol which is one of the main protocols that was used by the network managers for troubleshooting the networks. The third and very important aspect of this research was to provide the security for Real Time Applications.

The Internet today is being used by billions of users for a large variety of commercial and non commercial purposes. It is controlled by different entities. [1] pointed out that Internet is mainly used as an efficient means for communication, entertainment and education. There is a need for protecting confidential data because of the rapid growth of Internet. The current version of IP Protocol namely IPv6 comes with built in security mechanism called IPSec [2]. IPSec provides security services at the IP layer by enabling a system to select required security protocols to determine the cryptographic algorithms to use for the services and put in place of any cryptographic keys required to provide the security services. But IPSec do not provide any security for applications in application layer. Internet Control Message Protocol attacks is still possible which a major setback of IPv6.

The usage of current version of Internet and TCP/IP Suite results in many flaws such as: Spoofing is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage. Repudiation is the ability of users to deny that they performed specific actions

or transactions. Eavesdropping is process of capturing packets from the network transmitted by others computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information, Denial of service is the process of making a system or application unavailable [3].

Another important aspect of TCP/IP Protocol Suite is Internet Control Message Protocol Suite security. The usage of Internet control message protocol is very important for network administrators to track the status and troubleshoot the network. But due to the security flaws many administrators are blocking the ICMP protocol function [4]. This makes very difficult to identify and troubleshoot the network problems

II. LITERATURE SURVEY

The rapid growth of the current Internet, which operates using Internet Protocol version 4(IPv4) has created a number of problems for the administration and operation of the global networks [5]. Lot of research works was being done by the research communities to improve the current version of Internet Protocol. The work [5] pointed out the issues of the current version of Internet protocol.

The work [7] pointed out that the insufficient public IP address space does not allow the growth of the Internet. At the moment, most of mobile devices are required to have an IP address to connect to the Internet which leads to high consumption of IP address. Internet Engineering Task Force has considered this issue and proposed a new version of Internet Protocol namely Internet Protocol version 6 (IPv6). Next section provides the detailed literature of the two versions of IP Protocol namely IPv4 and IPv6.

Even as IPv6's new features will likely generate newer protocol attacks, the older known IPv4-related attacks will morph into new forms. Further, the lack of trained professionals as well as the scarcity of IPv6-related tools for network security analysis and monitoring will lead to slow response times against security attacks, which could exacerbate simple security breaches in massively interconnected IPv6 environments [3].

Some problems that affect IPv4 networks such as Reconnaissance, Unauthorized access, Host initialization and associated attacks, Routing attacks, DoS attack on Duplicate Address Detection Protocol, Man-in-the-middle attack, Multicast-based attacks and Spoofing attacks can also attack IPv6 networks. Moreover several other new unanticipated security issues will likely emerge as the hacking community starts actively targeting IPv6 networks

The work [8] pointed out the importance of cryptographic security for the transport layer and application layer. It was stated that "Cryptographic protocols are a vital component of Information Security as a means of securing modern networks against attackers by providing data integrity, encryption and authentication to network traffic at the transport layer. Sensitive information, such as banking details, that transverses networks will most likely do so through an encrypted tunnel provided by the cryptographic protocol; it is thus imperative that both the protocol itself is secure and the applications use of the protocol is correct and sensible".

The work [9]proposed a new hybrid cryptographic algorithm. The proposed algorithm was designed by the combination of DES and AES algorithm. If the plain-text of b bit, then first bit uses AES to encrypt and second bit uses DES to encrypt. The decryption process is invert of the encryption process. The main limitation of this hybrid algorithm is that the process is done for each and every bit similar to that of stream ciphers

Many cryptographic algorithms have been implemented by the research organizations all over the world. But all the algorithms had some limitations such as the existing algorithms implemented for specific applications, key size or block size of algorithms limited to 64,128 and 256 bits, existing algorithms support only text data not for voice and performance issues [10].

III. STATEMENT OF THE PROBLEM

From the Literature review, it was identified that the current TCP/IP Protocol Suite does not provide any security for applications of Application layer. The study also shows that the existing cryptographic algorithms such as DES, 3DES, RC2 have some security issues and performance issues. It is also found that AES and blowfish are highly secured than other encryption algorithms. The work [11] stated that "According to academic papers and reports regarding the security evaluation for such algorithms, it is difficult to ensure enough security by using the algorithms for a long time period, such as 10 or 15 years, due to advances in cryptanalysis techniques, improvement of computing power, and so on. To enhance the transition to more secure ones, National Institute of Standards and Technology (NIST) of the United States describes in various guidelines that NIST will no longer approve two-key triple DES, RSA with a 1024-bit key, and SHA-1 as the algorithms suitable for IT systems of the U.S. Federal Government after 2010". Based on this study the statement of the problem is formulated and the new algorithm is proposed.

IV. PROPOSED FRAMEWORK

This work follows the proposed algorithm framework as shown in Figure 4.1 below. The framework focuses on three keys processes or activities in order to achieve the research objectives. The three keys processes are as follows:

- 512 Bit SF Block Cipher for encryption and decryption.
- Enhanced version of ICMP protocol (EICMP protocol).
- Real Time Application Security Algorithm (RTAS algorithm).

A. SF Block Cipher

The existing TCP/IP Protocol suite is modified and a new protocol called Application Layer Security Protocol is implemented. It is added as an additional layer of the existing TCP/IP Protocol suite model. The layer is placed between the transport layer and application layer. The proposed protocol comprises of both symmetric and asymmetric cryptographic algorithms namely SF Block cipher, Blowfish, IDEA algorithm and SHA -2 Message digest. SF Block cipher is a new proposed algorithm with 512 bit block and 512 bit key. Elgamal and SHA -2 are both existing algorithms selected for use in the proposed architecture. The detailed encryption and decryption process was given in the previous paper[12].

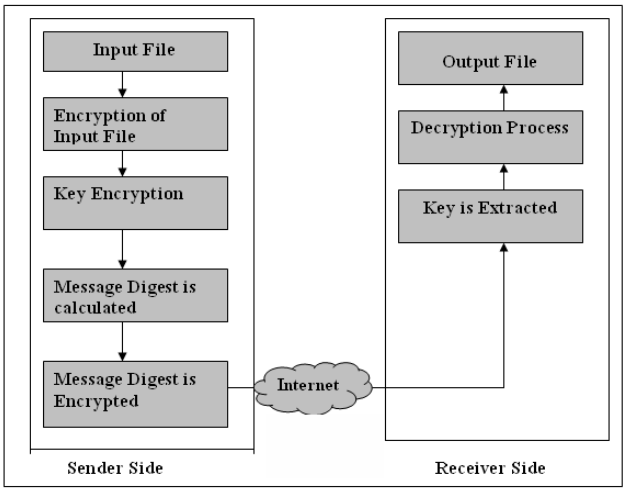


Fig. 1 Proposed Architecture

B. Enhanced Packet Format for ICMP Protocol

The proposed method includes an extra field AuthCode in the ICMP message format. The unused portion of the ICMP packet was used for this purpose. In this message format the Type field identifies the ICMP message type. For ICMPv6, values from 0 to 127 are error messages and values 128 to 255 are informational messages. Code field identifies the "subtype" of message within each ICMP message Type value. Thus, up to 256 "subtypes" can be defined for each message type. Checksum field is a 16-bit checksum field which provides error detection coverage for the entire ICMP message. Message Body contains the specific fields used to implement each message type.

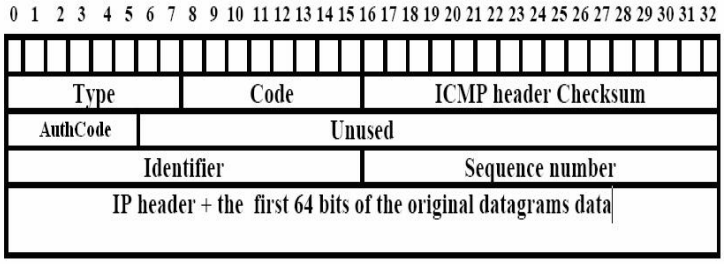


Fig 2 Enhanced ICMP Packet Format

The AuthCode field contains the secret key which is generated by the proposed algorithm. If there is any problem in the network, the ICMP message will be generated by the host or router based on the nature of the problem. Then the ICMP message will be sent to the source machine. On receiving the message the source machine knows the reason for the problem and takes necessary action to solve the problem. In between this if any person tries to retrieve the information such as source address, destination address, network address he will not be able to access any information unless he knows the authentication code.

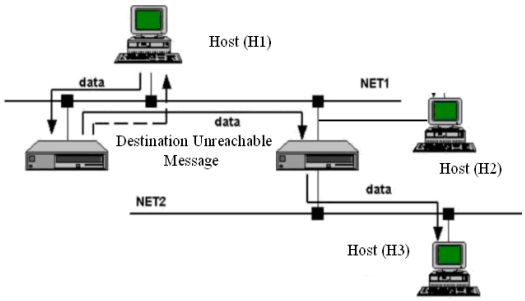
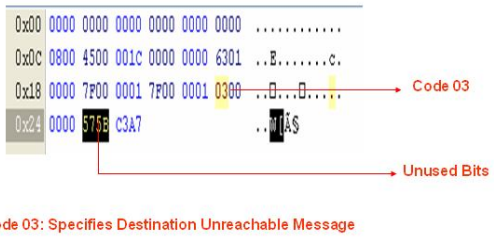


Fig 3 EICMP Operation

In the figure 3, Source host H1 is sending data packet to destination machine H3 of another network through router. If the router unable to find the destination machine, then it generates ICMP destination message and send it to host machine. The generated ICMP packet contains the Authcode generated by the Proposed ICMP Protocol. In between, if machine H2 tries to retrieve the information, it was not possible because of the Authcode that was only known by the source machine.H1. So with the proposed protocol, high level of security can be achieved. The figure 4 shows the destination unreachable message.

Screen Shot : ICMP Destination Unreachable Message



Code 03: Specifies Destination Unreachable Message

Fig 4. Simulated ICMP Packet

The ICMP packet mentioned above was tested in a small network that contains 150 systems. The source IP address is 192.168.1.9 and the destination IP address is 208.38.134.211. The same packet is tested for multiple source and destination using network analyzer tool and the following data are traced such as time, Mac source address, Mac destination address, frame, protocol, IP Source, IP Destination and size of the Packet.

TABLE I
CAPTURED DATA

N	Time	MAC Source	MAC Destination	Frame	Protocol	IP Source	IP Destination	Size
1	14:13:58.500	00:1D:92:BB:74:2F	00:90:7F:3C:AC:40	IP	ICMP->Echo request	192.168.1.9	208.38.134.211	74
2	14:13:58.781	00:90:7F:3C:AC:40	00:1D:92:BB:74:2F	IP	ICMP->Echo reply	208.38.134.211	192.168.1.9	74
3	14:13:59.500	00:1D:92:BB:74:2F	00:90:7F:3C:AC:40	IP	ICMP->Echo request	192.168.1.9	208.38.134.211	74
4	14:13:59.796	00:90:7F:3C:AC:40	00:1D:92:BB:74:2F	IP	ICMP->Echo reply	208.38.134.211	192.168.1.9	74
5	14:14:00.515	00:1D:92:BB:74:2F	00:90:7F:3C:AC:40	IP	ICMP->Echo request	192.168.1.9	208.38.134.211	74
6	14:14:00.812	00:90:7F:3C:AC:40	00:1D:92:BB:74:2F	IP	ICMP->Echo reply	208.38.134.211	192.168.1.9	74
7	14:14:01.531	00:1D:92:BB:74:2F	00:90:7F:3C:AC:40	IP	ICMP->Echo request	192.168.1.9	208.38.134.211	74
8	14:14:01.828	00:90:7F:3C:AC:40	00:1D:92:BB:74:2F	IP	ICMP->Echo reply	208.38.134.211	192.168.1.9	74

The following graph shows the status of incoming and outgoing packets of ICMP message. It shows that after the modification of ICMP Packet, there is no major time delay in sending and receiving ICMP messages. It also shows that it does not affect other protocol operations such as IGMP, TCP and UDP that operates at the time of sending and receiving ICMP packet.

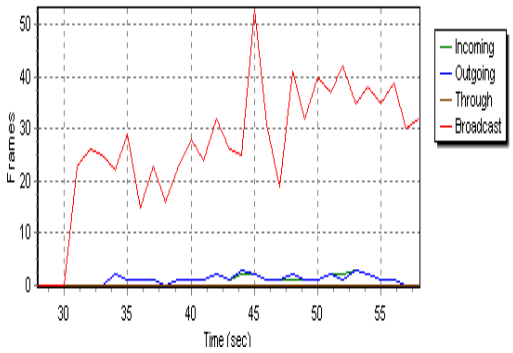


Fig 5 Time Delay

It also indicates that there is no major change in the traffic when executing the proposed ICMP packet. It shows that 80 frames of ICMP protocol is transmitted at the time of testing. The 29 frames of TCP and 89 frames of IGMP are transmitted during the testing.

Fig 6 Traffic Analysis

C. Real Time Application Security

The proposed system implements another approach to apply the security for real time applications such as voice data. The following algorithm is sampled with different voice file formats. MATLAB is used to sample the data.

1. Read the existing voice data file or record the data using Windows sound recorder and store the file in Wav format.
2. The audio file is sampled in MATLAB using the wavread( ) function which gives samples ranging from 1 to -1.
3. The samples is converted into array of integer data from 0 to 255 by adding one to each value and then multiply by 128.
4. Transfer the data to text file and store it in hard disk.
5. The data file is given as input to SF Block to encrypt the data and convert back to Wav format using the function wavwrite ( ).
6. The Decryption algorithm is used to get back the original data.

Spectrogram is generated for wav file before and after the encryption process. . Two dimensional plots of voice waves can be used to easily identify magnitude; however combined frequency distributions and magnitudes are more easily viewed in a spectrogram. First the voice data file is loaded with the help of MATLAB command wavread () Then the sampling frequency is captured and stored in a variable. The captured data was further sampled with small range of random number. Finally the sampled voice is viewed in spectrogram with the following equation 1.

S= Specgram (readed_data, 512, f) (1)

Where

S = spectrogram

readed_data = data from wavread () function
512 = the number of samples that are used for the discrete Fourier Transform
f = sampling frequency.

The analysis shows that there is a major change in the frequency of the audio signal after the encryption using the proposed model. It indicates that the proposed algorithm is highly secure and difficult to break the key. It is also identified that the algorithm best suited for real time applications such as video conferencing data and Voice over IP applications.

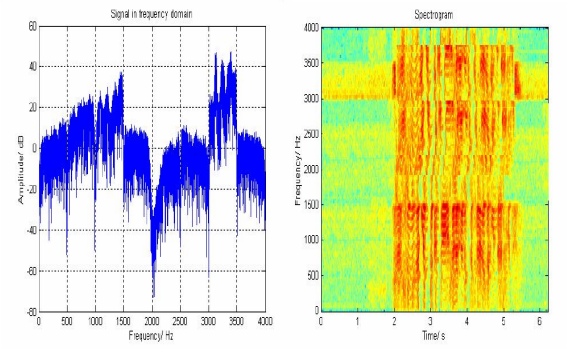


Fig 6 Spectrogram for Voice Data

V. PERFORMANCE ANALYSIS

Several performance metrics are used to evaluate the performance of the encryption algorithms such as Encryption time, Decryption time, CPU process time, and CPU clock cycles and Battery [13]. Encryption time is the total time taken to produce a cipher text from plain text. The calculated encryption time is then used to calculate the throughput of the encrypted algorithm. It gives the rate of encryption. The throughput of the encryption scheme is calculated as the total encrypted plaintext in bytes divided by the encryption time. Decryption time is the total time taken to produce the plain text from plain text. The calculated decryption time is then used to calculate the throughput of the decrypted algorithm. It gives the rate of decryption. The throughput of the decryption scheme is calculated as the total decrypted plaintext in bytes divided by the decryption time. The CPU process time is the time that is required to a CPU is dedicated only to the particular process of calculations. It reflects the load of the CPU. The CPU clock cycles are a metric, reflecting the energy consumption of the CPU while performing on encryption operations. Each cycle of CPU will consume a minute amount of energy [13].

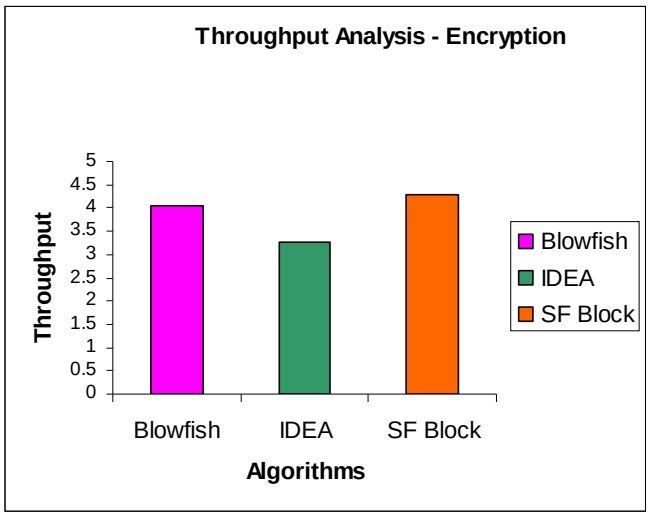


Fig 7 Throughput Analysis of Encryption

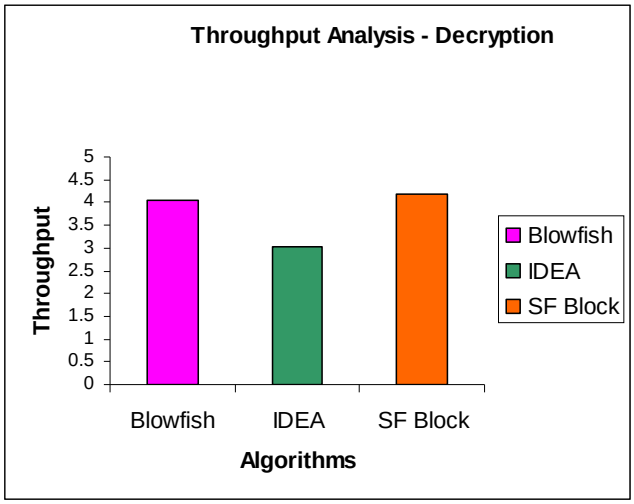


Fig 8 Throughput Analysis of Decryption

The throughput of the encryption scheme defines the speed of encryption. When there is an increase in the throughput of the encryption algorithm, there is a decrease in the power consumption algorithm. Figure 7 denotes the throughput of encryption and figure 8 shows the throughput of decryption. From the analysis it shows that the proposed SF Block cipher has better throughput than that of blowfish and IDEA algorithms. The detailed specfications of performance evaluation of SF Block Cipher is given in [12].

VI. CONCLUSION

In this thesis work, the objectives of designing new security architecture for the TCP/IP Protocol suite were achieved. A new 512 bit cryptographic encryption, decryption and key management algorithm to enhance the security of the TCP/IP protocol suite was implemented. Most of the available encryption and decryption techniques are not suitable to be used to secure confidential data over an open network since they were originally designed before a decade with limited usability. This research develops a new security framework that can be suited for text as well as voice data with minimum overload in terms of processing. The proposed architecture has been implemented and tested. The proposed system uses 512-bit block and 512-bit key length for encryption and decryption process which was the main advantage over the existing algorithms. Due to the key size and block, it was impossible to execute the cryptanalysis. Internet Control Message Protocol was enhanced with authentication to provide better security over the existing protocol. The proposed protocol can be used by the network administrator to troubleshoot the network without any fear of security breaches.

REFERENCES

[1] Saleh, A. M. , and J. M. Simmons, 2011. Technology and architecture to enable the explosive growth of the internet, IEEE Communications Magazine, 49(1): 126-132.

[2] Oppliger, R. , 1998. Security at the Internet layer, IEEE Computer, 31(9): 43-47.

[3] Caicedo, C. E. , J. B. Joshi, and D. Tuladhar, 2009. IPv6 Security Challenges, IEEE Computers, 42(2): 36-42.

[4] Atul Kant Kaushik, and R C Joshi, 2010. Network Forensic System for ICMP Attacks, International Journal of Computer Applications, 2(3):14–21.

[5] David, C. lee., Daniel L. lough, Scott F. Midkiff, Nathaniel J. Davis IV, and Phillip E. Benchoff, 1998. The Next Generation of the Internet: Aspects of the Internet Protocol Version 6, IEEE Network, 12(1): 28-33.

[6] Goth, G. 2012. The End of IPv4 is Nearly Here 2014, IEEE Internet Computing, 16(2): 7-11.

[7] Saleh, A. M. , and J. M. Simmons, 2011. Technology and architecture to enable the explosive growth of the internet, IEEE Communications Magazine, 49(1): 126-132.

[8] Homin K. Lee, Tal Malkin, and Erich Nahum, 2007. Cryptographic strength of servers: current and recent practices, Proceedings of the ACM SIGCOMM conference on Internet measurement: 83-92.

[9] Mingyan Wang, and Yanwen Que, 2009. The Design and Implementation of Passwords Management System Based on Blowfish Cryptographic Algorithm, Computer Science-Technology and Applications, 2(1): 24-28.

[10] Ijaz Ali Shoukat, Kamalrulnizam Abu Bakar and Mohsin Iftikhar, 2011. A Survey about the Latest Trends and Research Issues of Cryptographic Elements, International Journal of Computer Science Issues, 8(3): 140-149.

[11] Masashi Une, and Masayuki Kanda, 2007. Year 2010 Issues on Cryptographic Algorithms, Monetary and Economic Studies, 129-164.

[12] Anand Kumar.M and Dr. S. Karthikeyan 2011)," A New 512 Bit Cipher - SF Block Cipher" International. Journal of Computer Network and Information Security", 4[11]: 55-61.

[13] Diaa Salama Abdul, Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud, 2008. Performance Evaluation of Symmetric Encryption Algorithms, International Journal of Computer Science and Network Security, 8(12): 78-85.

AUTHORS

Dr. M. Anand Kumar has completed M.Sc and M.Phil in computer science from Bharathiar University and Periyar University. He has Completed Ph.D in Karpagam University having eight years experience in teaching.. His area of research includes network security and information security. He has presented twenty papers in national conferences and four papers in international conferences. He has published nine papers in international journals

Dr. S. Karthikeyan presently working as Assistant Professor, College of Applied Sciences, Oman and previously he was a Senior Lecturer at Caledonian College of Engineering, Oman. He has total of 14 years of teaching and research experience. He has chaired many conference sessions and served as Technical Committee member of various boards at various colleges, universities and conferences. He has 32 research papers and guiding 11 PhD research scholars from various universities in India

