ISSN No. 0976-5697

Volume 1, No. 4, Nov-Dec 2010

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Performance and Analysis of AES, DES and Triple DES against Brute Force Attack to protect MPLS Network

Gurpreet Kaur*
Student, DAVIET, Jalandhar
Punjab (144001) India
preet8184@rediffmail.com

Dinesh Kumar
Assistant Professor, DAVIET, Jalandhar
Punjab (144001) India
erdineshk@gmail.com

Abstract: Over the last few years, the Internet has evolved into a ubiquitous network and inspired the development of a variety of new applications in business and consumer markets. So, Multiprotocol Label Switching (MPLS) is another challenge and a versatile solution to address the problems faced by present day networks. Main objective of MPLS is to provide security in the data exchanged. So, in this paper we have implemented Encryption Algorithms like AES, DES and Triple DES to provide sufficient levels of security for protecting the confidentiality of the data in the MPLS network. This paper also analyzes the performance of these algorithms against Brute Force Attack implemented in the MATLAB environment to protect the MPLS Network.

Keywords: AES, DES, Triple DES, MPLS, Security, Keylengths.

I. INTRODUCTION

MPLS stands for Multiprotocol Label Switching, is a technology proposed by Internet engineering Task Force (IETF). It was designed to facilitate several problems areas in the internet including routing performance and is increasingly being adopted by service providers in their core networks. MPLS solutions are to be used with Layer2 and Layer 3 Protocols. MPLS has emerged as a potential solution for addressing traffic engineering, security and survivability for IP networks. So, a label is assigned to a packet when it enters the MPLS network at ingress Label Switched Router [7]. A label is a short fixed length identifier which is of 20 bits ranging from 0 to 19 that is used to forward the packets. Within the network the labels are used to route the packets without regard to the original packets header information. So, in this paper to secure the data which is attached with the label, various Encryption algorithms like AES, DES and Triple DES has been implemented on MPLS network. Our technique does not require any hardware; it is totally based on software. Following Sections discusses the proposed scheme.

Section II discusses the Security Requirements of MPLS network.

Section III explains the methodology used to encrypt the data in MPLS Network.

Section IV discusses the enhancement of IPSec using encryption algorithms to protect MPLS network.

Section V walks through the used setup environment and the settings for the encryption algorithms on MPLS. This section also illustrates the performance evaluation methodology chosen settings to allow for a better comparison and thorough discussion about the implementation results.

Finally, Section VI concludes this paper by summarizes the key points.

II. SECURITY REQUIREMENTS OF THE MPLS NETWORK

Network Managers have many options for site to site connectivity like traditional leased lines, ATM based connectivity and frame relay. But other two types of modern VPNs i.e MPLS and IPSec are becoming increasingly attractive to network managers [13]. In pure IP network it is easy to spoof IP addresses which is a key issue in the Internet Security. But, because MPLS works internally with labels, instead of IP addresses, so it is not so easy to breach the security. The very fact to make concept clear is that it is not possible to insert packets with wrong labels into the MPLS network from outside, since the customer edge(CE) is unaware of the MPLS core and thinks that it is sending IP packets to the router [1]. The intelligence is done in (PE) provider edge device where based on the configuration, the label is chosen and attached to the packet. So, MPLS is more secure than normal IP addressing technique. But, the spoofing here can also be possible. The attacks like brute force attack can break the security, although it is not so easy, but it can do so. MPLS alone cannot provide security; it is combined with IPSec to provide sufficient levels of security. So, various encryption and hashing algorithms are used to maintain the confidentiality of the data. IPSec requires each side to authenticate with the other, so privacy is maintained in IPSec VPN through the use of encryption. A secure MPLS network provides the following facilities to its users [13]:

A. Data Confidentiality

IPSec VPNs provide data confidentiality through robust encryption algorithms. It seeks to ensure data confidentiality by defining a single path between physical sites on a service provider network. This prevents attackers from accessing transmitted data unless they place sniffers on the service provider network. Though MPLS minimizes the chance that data may be intercepted, IPSec provides better confidentiality through encryption.

B. Data Integrity

IPSec uses hashing algorithms to ensure data integrity. There are inherent methods as such to provide data integrity

within MPLS VPNs. However, the odd of data being shared by a man-in-the-middle attack is low due to the separation address space and routing information provided by MPLS VPNs.

C. Data Availability

IPSec relies on the Internet for transport. Although an attacker could not read the data, but it could DOS an IPSec VPN by entering false routes into the Internet Routing Tables. MPLS VPNs rely on LSPs i.e. Label Switched Paths for transport and since LSPs have local significance only, spoofing is difficult to accomplish. Thus, MPLS can provide better data availability in this regard.

III. METHODOLOGY USED TO ENCRYPT THE DATA IN MPLS NETWORK

In this paper encryption on labels in MPLS network is proposed using AES, DES and Triple DES encryption algorithms. For implementing and evaluating above encryption algorithms we have done the following steps:

[a] Encrypt the data with one of the above mentioned algorithms.
[b] Encode the data according to MPLS.
[c] Brute Force Attack has been done.
[d] Time taken to find a correct key is measured against different key lengths.

These steps are shown in fig.1 below:

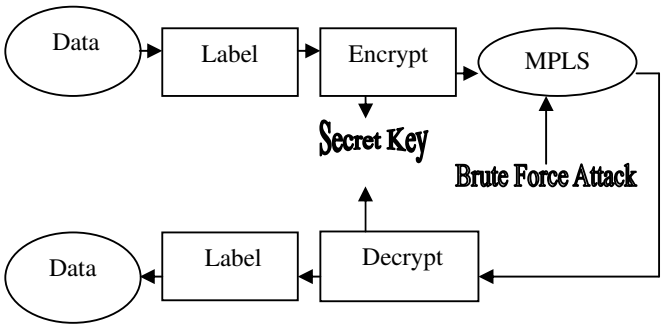

Figure 1. Data Encryption

This paper analyzes the effectiveness of AES, DES and Triple DES encryption algorithms against brute force attack on MPLS network. The comparison has been conducted by running brute force attack program against these algorithms.

A. Implementation Setup

This section describes the implementation environment and the used system components. The implementation of DES, Triple DES and AES uses classes available in JAVA package javax.crypto [11]. Separate functions for encryption and decryption have been implemented in MATLAB using JAVA cryptography API which is shown below in fig. 2

Figure 2. JAVA Cryptography Package

Brute Force program is implemented in MATLAB environment. This implementation is thoroughly tested and is optimized to give the maximum performance for the algorithm.

B. System Parameters

The experiments are conducted using Intel 64-bit processor with 2 GB of RAM. The program is written in MATLAB. The experiments will be performed couple times to assure that the results are consistent and are valid to compare the different algorithms .The brute force attack has been done using single PC. It can be enhanced by the use of parallel computers with high computational powers to decrease the time required to find the key for the above algorithms.

C. Experiment Factors

In order to evaluate the performance of the compared algorithms against brute force program on MPLS networks, the experimental factors must be determined. The chosen factors here to determine the effectiveness of encryption algorithms are the key length and the time taken to breach an algorithm by brute force program.

D. Experimental Initial Setting

We started the attack with 8 bit of key length and extended upto 40 bits. It can further increased upto supported key length of AES algorithm i.e 256 bits. But for this high computational power is required in terms of parallel computers to breach the security.

IV. EHANCEMENT OF IPSEC USING ENCRYPTION ALGORITHMS TO PROTECT MPLS NETWORK

In the current networks IPSec uses AES, DES and TDES algorithms to enhance the security of IP network. Even though the Encryption and Hashing algorithms are already implemented, but still they are not resistant to various attacks on the Internet like DOS, DDoS, Man in the Middle and Spoofing attacks. So, to recover from all this, a new technology called MPLS along with the combination of IPSec is implemented to enhance the security of network [5]. Specifically, IPSec should be used if one or several of the following requirements exist:

A. Encryption of all traffic over the MPLS core- If an attacker is able to sniff traffic on the core, with IPSec he will be able to see only the site from which the traffic came, and the site to which it goes.
B. Authentication of the endpoints- The CE routers can authenticate each other, so that an attacker cannot introduce router in the VPN, even if the SP's MPLS core is not fully secured.
C. Integrity of the traffic- Packets cannot be changed on their way through the core without the change being noticed.
D. Replay Detection- If IPSec (AH) Authentication Header is used; an attacker cannot save a packet and replay it later. This can be crucial in application environments where simple messages such as "close connection" exist, which could be saved by an attacker and later be used for a DOS attack against this service.

V. RESULTS AND DISCUSSIONS

This Section will show the results obtained from running the brute force program on AES, DES and Triple DES. The results of implementation have been shown below in the

form of graphs. The time of launch of brute force attack is shown at the start of the program as in Fig 3.

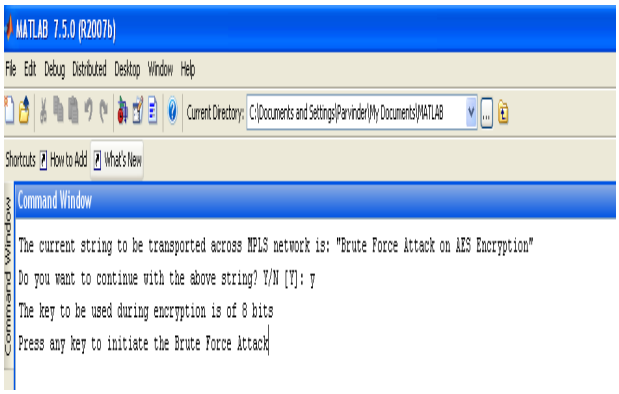

Figure 3. Screenshot of running brute force program

The program exits on success of the attack on the encryption algorithm which is shown below in fig 4

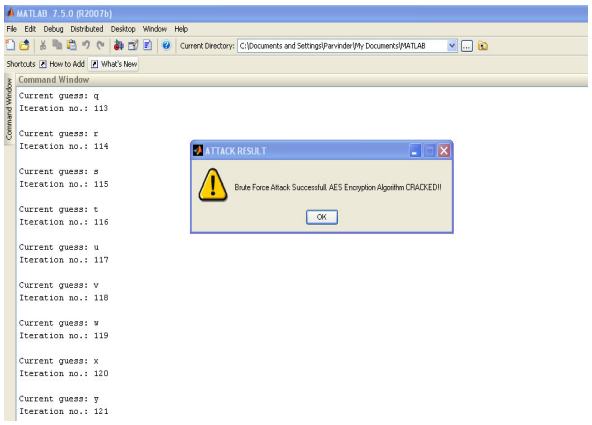

Figure 4. Screenshot of cracked Algorithm

The time required for breaking the encryption algorithm, actual encrypted string and the label applied all is shown in fig 5. The screenshot is of 24 bit key length.

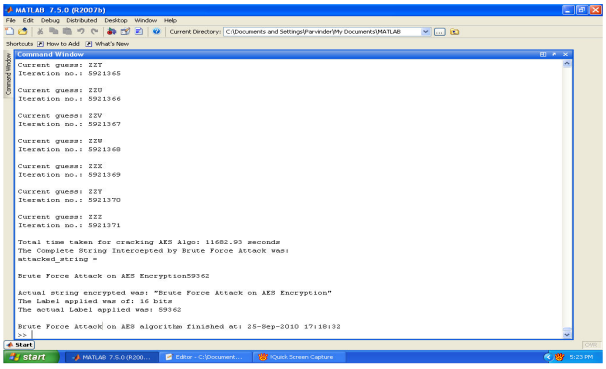

Figure 5. Screenshot various factors like time to break the security, actual encrypted string and the label applied on it.

It is highlighted here that the implementation has been performed assuming that the user has arrived at all the correct values of the key and for 8- bit, only one value of the key is to be cracked. Similarly, for 16- bit two values of the key are to be cracked and so on upto 40 bits. This has been done to save the time required. The key length can be optimized to reduce the time taken for encryption and decryption process so that it does not slow down the system.

A. Effect of keylength variation

We compare the change in security performance by using different key lengths for encryption algorithms. Graphs are plotted between the time required to find the correct key and different key lengths. We have taken five different scenarios by increasing the length of the key. These scenarios are shown in Table I.

Table I. Different Keylengths

Scenarios	*Keylengths (Bits)*
1.	8
2.	16
3.	24
4.	32
5.	40

Following are the graphs for scenarios stated in table I. These graphs show the number of seconds required to breach the corresponding algorithm against brute force attack.

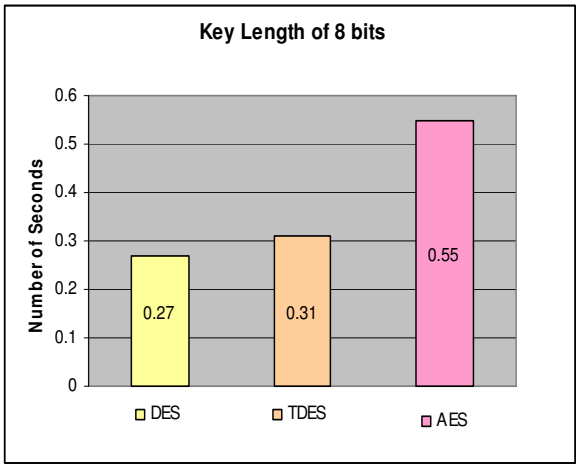

Figure 6. No. of seconds required with key length of 8 bits

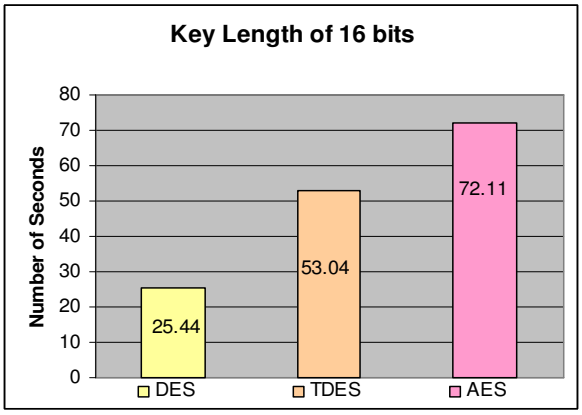

Figure 7. No. of seconds required with key length of 16 bits

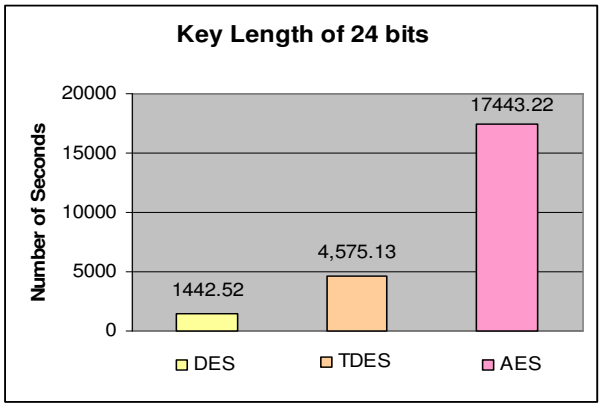

Figure 8. No. of seconds required with key length of 24 bits

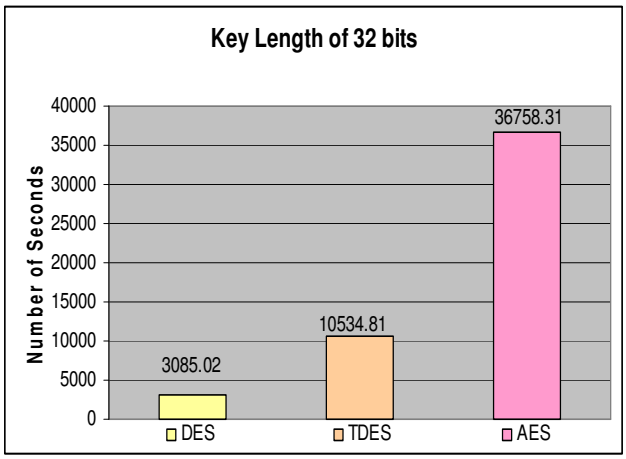

Figure 9. No. of seconds required with key length of 32 bits

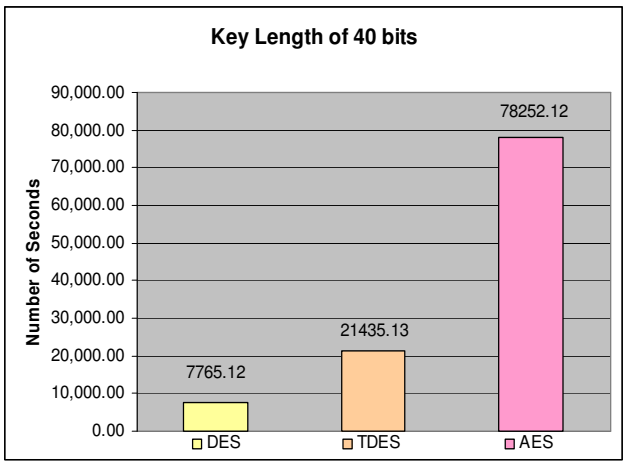

Figure 10. No. of seconds required with key length of 40 bits

The above graphs show the time taken to find the key by the brute force program on DES, Triple DES and AES for different key lengths. From these graphs it is analyzed that time taken by brute force attack increases exponentially with the increase in key length. It is clear from the graphs that in case of AES algorithm, brute force attack takes more time to find a key. Therefore, it has a better security than DES and Triple DES.

B. Effectiveness of algorithms against brute force attack

The results of the iterations of brute force program have been shown in Table II.

Table II. Number of seconds required to breach DES, Triple DES and AES

KeyLength (Bits)	*DES (Seconds)*	*Triple DES (Seconds)*	*AES (Seconds)*
8	0.27	0.31	0.55
16	25.44	53.04	72.11
24	144.52	4575.13	17443.22
32	3085.02	10534.81	36758.31
40	7765.12	21435.13	78252.12

Also, the effectiveness of AES, DES and Triple DES is shown in fig. 11 in the form of a graph which is plotted in the MATLAB environment.

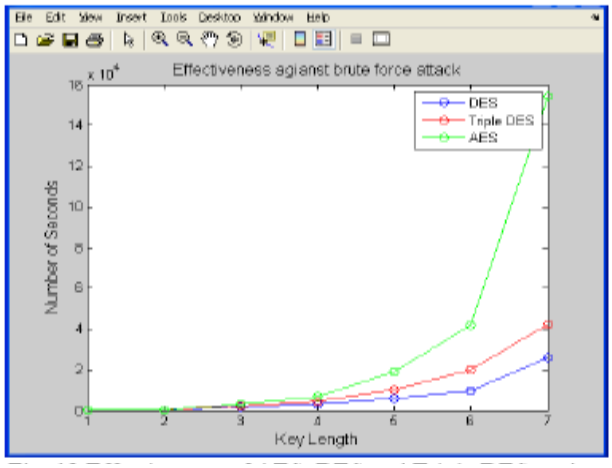

Figure 11. Effectiveness of AES, DES and Triple DES against brute force attack.

The above data and graph represents the effectiveness of AES, DES and Triple DES algorithms against brute force attack. It is evident from the data presented that AES proves to be of better security against the brute force attack than DES and Triple DES for securing MPLS network.

VI. CONCLUSION

Summary of the key points:

A. AES proves to be better secure than DES and Triple DES as it takes considerably much more time to break by the brute force program for a given key length.

B. Time taken to break AES algorithm by a brute force program increases exponentially with the increase in the key lengths.

C. Time taken to breach AES algorithm is more than that of Triple DES and time taken by Triple DES is more than that of DES algorithm. Hence it has been prove that:
Security of AES > Security of Triple DES > Security of DES.

VII. REFERENCES

[1] Cisco Systems,"White paper: Security of the MPLS Architecture". August 14, 2001.

[2] M, Wiener, "Brute force attacks on cryptographic keys". October, 2001.

[3] "Advanced Encryption Standard", Federal Information Processing Standards (FIPS) 197, Nov. 2001. [Online Available At]

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[4] A. Barlow, V. Vassiliou and L. Owen, "A cryptographic protocol to protect MPLS labels". Information Assurance Workshop, IEEE Systems, Man and Cybernetics Society. pp. 237- 242, 18-20 June 2003.

[5] R. Rong, F. Deng and M. Ke, "A detailed implement and analysis of MPLS VPN based on IPSec". Machine Learning and Cybernetics, Proceedings of 2004 International Conference on, vol.5, no., pp. 2779- 2783. 26-29 Aug. 2004.

[6] H. Liwen and P. Botham, "Pure MPLS Technology". Availability, Reliability and Security, ARES 08, Third International Conference on, pp.253-259, 4-7 March 2008.

[7] G. Aggarwal, D. Huang and D. Methi, "Network Protection Design for MPLS Networks". International Workshop on Design of Reliable Communication Networks. pp. 481-486. 16-19 October, 2005.

[8] Reducing the exhaustive key search of the Data Encryption Standard (DES) Computer Standards & Interfaces, Volume 29, Issue 5, july 2007, Pages 528-530 Raphael C.-W. Phan.

[9] J. Pico, J. Fajardo and A. Ferro, "MPLS-VRF integration: forwarding capabilities of BGP/MPLS IP VPN in GNU/Linux". International Conference on, Optical Network Design and Modelling, pp. 1-6, 12-14 March, 2008.

[10] V. Ramakrishnan, C. Wargo and S. John, "GMPLS Network Security: Gap Analysis". ICNS Conference, IEEE Systems. pp. 1-7. 5-7 May 2008.

[11] M. Sachin and K. Dinesh, "Implementation and Analysis of AES, DES and Triple DES on GSM Network". IJCSNS International Journal of Computer Science and Network Security. vol. 10, no.1. January 2010.

[12] M. N. Islam, M.M.H. Mia, M.F.I. Chowdhury and M.A. Matin, " Effect of Security Increment to Symmetric Data Encryption through AES Methodology", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/ Distributed Computing, pp. 291-294, 2008.

[13] A. Garry, " Comparing BGP/MPLS and IPSec VPNs". SANS Institute InfoSec Reading Room, 2002.

[14] Gary C. Kessler, "An Overview of Cryptography", November, 2010. [Available Online At:]

http://www.garykessler.net/library/crypto.html