ISSN 2229-5518

Effectiveness of DES, Triple DES and AES on MPLS network

Mona Mudaliar, L K Bhaiya

Abstract— MPLS is Multi-Protocol Label Switching Network .Internet Engineering Task force (IETF) developed this technology specially to speed up the forwarding characteristics of routers. It uses the protocols of both layer 2 and layer 3.It employs label switching technique hence making the technology fast, efficient and secure. Various types of encryption algorithm are used to secure MPLS network .Some of them are advanced Encryption Standard (AES),Data Encryption Standards(DES) and Triple DES (TDES) to secure the network against brute force attack. In this paper we have encrypted a string and analysed the DES, Triple DES and AES algorithm on MPLS network against brute force attack and plotted a graph to show the effectiveness in MATLAB environment.

Index Terms— AES, DES, Keylength, Label, MPLS, TDES, Triple DES.

1 INTRODUCTION

MPLS stands for Multi-Protocol label switching, is now a days a popular technology which has grabbed the attention of network service provider because of its routing performance. Internet Engineering Task Force (IETF) proposed this technology [3].MPLS uses a label switching technique to speed up the routing performance.The packet forwarding is done via label in MPLS network. The MPLS labels are advertised between routers. The IP packets are prefixed by these labels and forwarding is done on the basis of these labels and not by destination IP address that means forwarding of packets is based on lookup of labels rather than a lookup of the IP addresses hence speeding up the routing procedure.

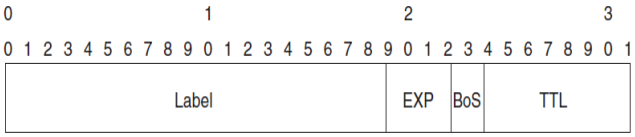

Fig.1. Syntax of MPLS Label

Label field is of 20 bits whose value can be from 0 to 2^{20}-1or 1,048,575. The bits from 20 to 22 bits are experimental (EXP) bits. These bits are used for quality of service (QoS). Bit 23 is Bottom of Stack (BoS).Its value is 1 if this is bottom label in the stack otherwise 0. Bit 24 to 31 are the 8 bits used for Time To Live (TTL).0 value of TTL indicates that the packet is discarded.

- *Mona Mudaliar is Assistant Professor at RSR Rungta college of Engineerig and Technology,Bhilai,Chattisgarh,INDIA. E-mail: mudaliar.mona@gmail.com*
- *L K Bhaiya is Associate Professor and Head of Electronics and Telecommuinications department at Rungta college of Engineerig and Technology,Bhilai,Chattisgarh,INDIA,.E-mail: lalit04_bhaiya@yahoo.com*

The labeled packets in the MPLS network are routed via label switched path (LSP) which is a sequence of label switch routers (LSRs) [2]. The ingress LSR and egress LSR are the initial and final label switch routers espectively. The intermediate LSRs are the LSRs that lie in between ingress and egress LSRs. A forward equivalence class (FEC) is a group or flow of packets that are forwarded along the same path and treated the same with regard to the forwarding treatment.

To communicate with each other routers follows certain protocols.The two important protocols are Label Distribution Protocol (LDP) and Resource Reservation Protocol.LDP is a dynamic label distribution protocol which form a label database on the IP backbone. Resource Reservation Protocol manages resources for routers for smooth flow of traffic.

Security plays a vital role for successful operation of any communication network. Every communication network should ensure that the data sent from the source reaches to its destination securely. For security purposes, there are various encryption and decryption algorithm to make the data transmission and reception a secure process.

There are different encryption techniques to secure MPLS network against various attacks, like brute force attack. Brute force attack is a strategy in which attacker attempts to use all possible combinations of key until the correct key is found. So encryption algorithms like AES, DES and Triple Des which is a part of IPSec are used to secure MPLS technology against various attacks.

In this paper we have encrypted a string by different bits of keylength and a brute force attack has been done to analyze the effectiveness of the encryption algorithms i.e AES,DES and TDES for different key length in MATLAB environment.

2 PROCEDURE

This section describes the implementation set up environment

and the system components. Classes available in JAVA package javax.crypto is used to implement AES,DES and Triple DES. Separate functions for encryption and decryption have been implemented in MATLAB using JAVA cryptography API.

Brute force attack is implemented in MATLAB environment and is thoroughly optimized to give the maximum performance for the algorithm.

3 Methodology

We started the attack with 8 bit of keylength extended up to 48 bit on a string .Label is generated and the encrypted data is transported across MPLS network. After the successful completion of brute force attack the key and the label applied are cracked after some number of iterations. It can be further extended up to 256 bits which is supported key block for AES so we can use parallel computers with high computational powers to decrease the time required to find the key for above algorithms.

4 Results and Discussions

This section deals with the results obtained after running the brute force program on AES, DES and Triple DES .The results of the implementation has been shown in the form of graphs.

On running the brute force program in MATLAB environment,key entered by the user is cracked by the program after some number of iterations and the program exits after successful cracking and is shown in fig 1

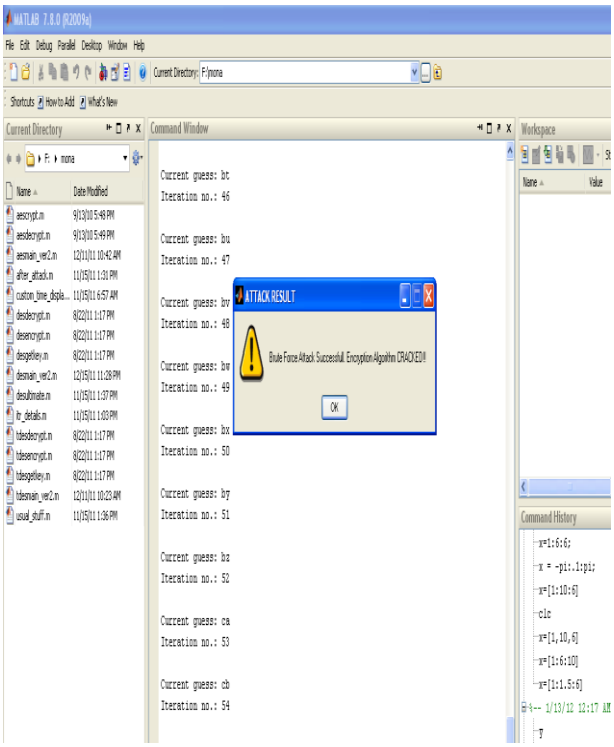

Fig. 2.Screenshot of cracked algorithm

4.1 Effect of keylength variation

The table shows the different time required (in seconds) for different keylength(in bits) for algorithm DES,TDES and AES. The comparison of security performance between the algorithms DES, Triple DES and AES is done on the basis of time taken to breach the key and has been shown in the Fig 5 to Fig 10.

TABLE 1

Key length (bits)	DES (seconds)	TDES (seconds)	AES (seconds)
8	.05	.0628	.08
16	.393	.435	.441
24	6.338	6.665	8.209
32	180.805	191.163	226.446
40	3546.88	3696.31	4402.51
48	25874.5	27286.1	34245.695

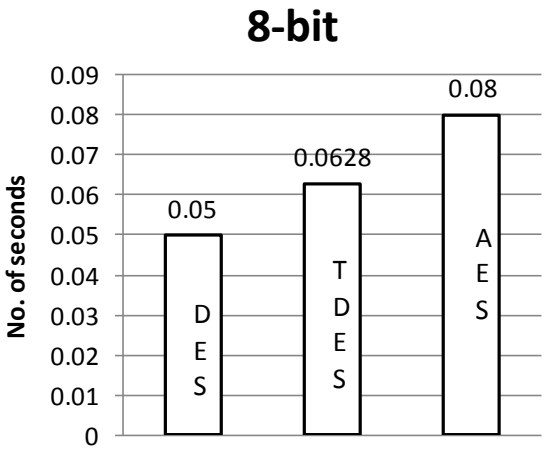

Fig.3. Number of seconds required with keylength of 8-bits

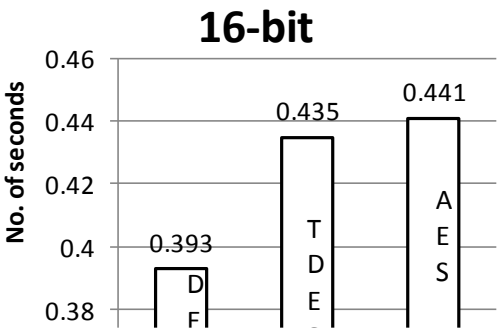

Fig.4. Number of seconds required with keylength of 16-bits

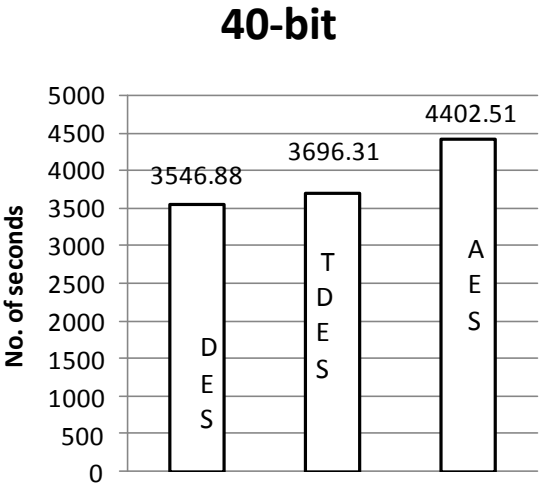

Fig.7. Number of seconds required with keylength of 40-bits

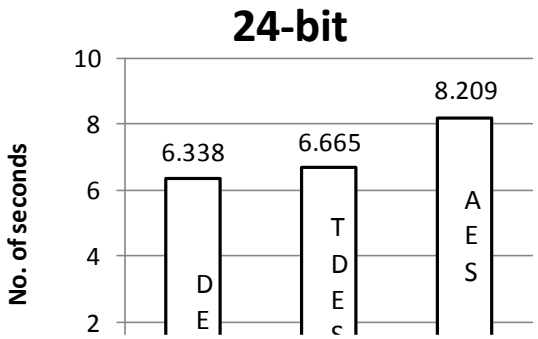

Fig.5. Number of seconds required with keylength of 24-bits

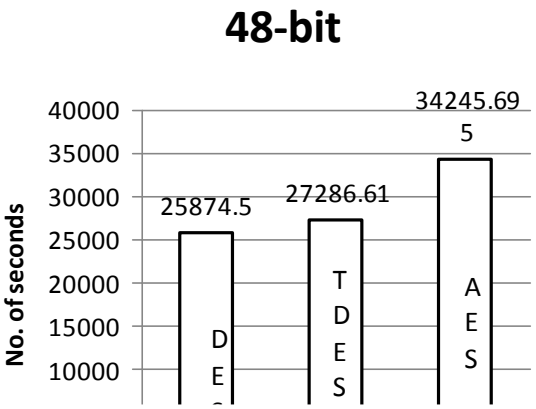

Fig.8. Number of seconds required with keylength of 48-bits

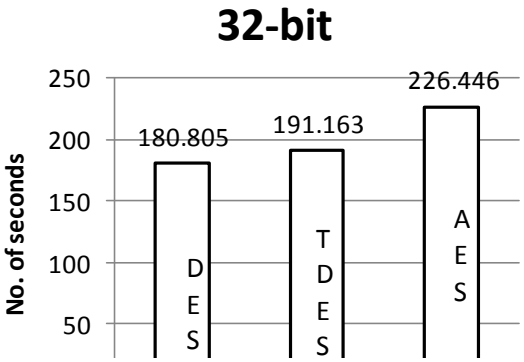

Fig.6. Number of seconds required with keylength of 32-bits

4.2 EFFECTIVENESS OF ALGORITHM AGAINST BRUTE FORCE ATTACK

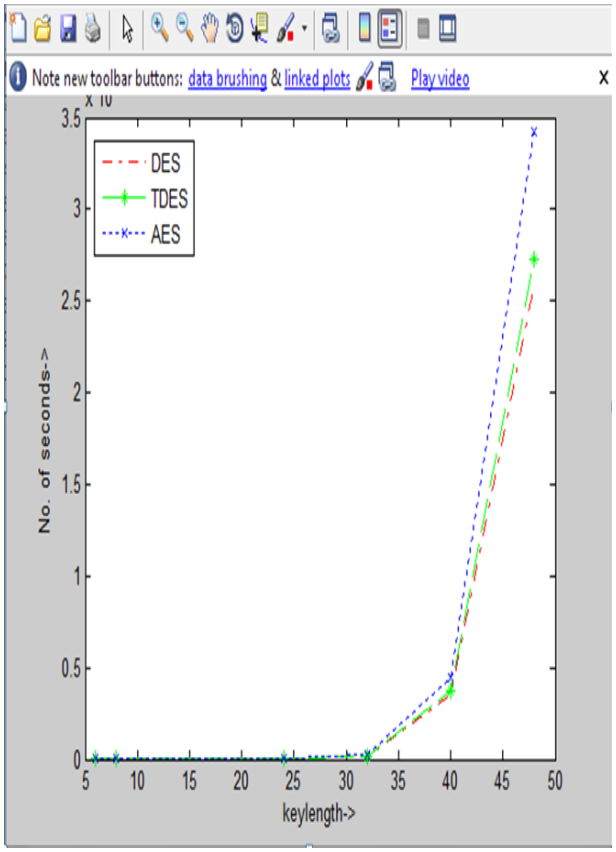

Fig. 9. Effectiveness of DES,TDES and AES

The effectiveness of DES,Triple DES and AES has been shown. The graph has been plotted in MATLAB environment.

5 Conclusions

The AES has a better security against brute force attack than DES and Triple DES as observed in the results discussed above. Hence we can say AES proves to be a better security algorithm than DES and Triple DES. AES takes much more time to break by the brute force attack for a given key length. This time rises in exponential manner with increase in key length.

6 References

[1] Gurpreet Kaur , Dinesh Kumar, "MPLS Technology on IP Backbone Network", International Journal of Computer Applications(0975-8887),Volume 5 –No.1,August 2010.

[2] Luc de ghein, "MPLS Fundamentals", CISCO press, 2007.

[3] David A. Barlow, Vasos Vassiliou, Henry L. Owen," A Cryptographic Protocol To Protect MPLS Labels", Proceedings of the IEEE, 2003.

[4] Ayan Banerjee, John Drake, "Generalized Multiprotocol Label Switching: An Overview of Routing and Management Enhancements", IEEE, 2001.

[5] Dr. Surat Tanterdtid, Akekachat Pao, "IP/MPLS –Based Data Communication Network for Power Utility", IEEE Bologna PowerTech Conference, June 23-26, 2003.

[6] O.Gure, B.K. Boyaci, N.O. Unverdi, "Analysis of the service quality on MPLS networks", 5th European Conference on Circuits and Systems For Communications, Belgrade Serbia, November 23-25, 2010.

[7] Vikram Ramakrishnan, Chris Wargo and Sherin John, "GMPLS Network Security: Gap Analysis", Computer Networks and Software, Inc.

[8] Luyuan Fang, Nabil Bita, "Interprovider IP-MPLS Services: Requirements, Implementations, and Challenges", IEEE communications magazine, June 2005.

[9] Md. Nazrul Aslam, Md. Monir Hossain Mia, Muhammad F . I . Chowdhury, M.A Matin, "Effect Of Security Increment To Symmetric Data Encryption Through AES Methodology.

[10] Tingzhou Yang, Dimitrios Makrakis, "Hierarchical Mobile MPLS: Supporting Delay Sensitive Applications over Wireless Internet", IEEE, 2001.