Triple des against a brute force attack computer science essay

Technology, Computer

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 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 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

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 [1]. So, 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 2 discusses the Security Requirements of MPLS network.

Section 3 gives the quick overview of the various encryption algorithms used in this technique.

Section 4 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.

Section 5 gives a thorough discussion about the implementation results.

Finally, Section 6 concludes this paper by summarizes the key points and other related information.

2. 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 [2]. In pure IP network it is easy to spoof IP addresses which is a key issue in Internet Security. But, because MPLS works internally with labels, instead of IP addresses, so it 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 [3]. The intelligence is done in (PE) provider edge device where

based on the configuration, the label is chosen and prepended 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 can be 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 [2]:

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.

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.

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.

Service Reliability: MPLS has the ability to protect the communication session against denial of service attacks.

3. REQUIREMENT OF ENCRYPTION ON LABELS 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:

Encrypt the data with one of the above mentioned algorithms.

Encode the data according to MPLS.

Brute Force Attack has been done.

Time taken to find a correct key is measured against different key lengths.

Data

Label

Encrypt

Label

Data

MPLS

Decrypt

Secret Key

Brute Force Attack

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.

3. 1 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. Separate functions for encryption and decryption have been implemented in MATLAB using JAVA cryptography API.

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.

3. 2 Methodology Used

This Section will discuss the methodology and its related parameters like: system parameters, experiment factors and experiment initial settings.

3. 2. 1 System Parameters

The experiments are conducted using Intel 64-bit processor with 32 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.

3. 2. 2 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.

3. 2. 3 Experimental Initial Setting

We started the attack with 8 bit of key length and extended upto 64 bit. 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 algorithms.

4. 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 to break the encryption algorithm, actual encrypted string and the label applied, all are shown in fig. 5

Figure 5 Screenshot of various factors like time to break, actual encrypted string and the label applied

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 only two

values of the key is to be cracked. 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.

i) Effect of key length 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 six different scenarios by increasing the length of the key.

Table 1

DIFFERENT KEY LENGTHS

Scenario	Key length (Bits)
1	8
2	16
3	24
4	

32

5

40

6

48

7

56

8

64

Following are the graphs for scenarios stated in table1. These graphs show the number of seconds required to breach the corresponding algorithm against brute force attack.

Figure 5 Number of seconds required with key length of 8 bits

Figure 6 Number of seconds required with key length of 16 bits

Figure 7 Number of seconds required with key length of 24 bits

Figure 8 Number of seconds required with key length of 32 bits

Figure 9 Number of seconds required with key length of 40 bits

Figure 10 Number of seconds required with key length of 48 bits

Figure 11 Number of seconds required with key length of 56 bits

Figure 12 Number of seconds required with key length of 64 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.

i) Effectiveness of algorithms against brute force attack

The results of the iterations of brute force program have been shown in the below figure in Table 2. This graph is plotted in MATLAB environment.

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.

Figure 13 Effectiveness of AES, DES and Triple DES against brute force attack

Table 2

Number of seconds required to breach DES, Triple DES and AES

KeyLength

(bits)

DES

(Seconds

Triple DES (Sec)

AES

(Sec)

8

0. 27

0. 31

0. 55

16

39. 59

52. 11

110. 44

24

1442. 52

4575. 13

17443. 22

32

3085. 02

10534. 81

36758. 31

40

7765. 12

21435. 13

78252. 12

48

15229. 91

44671. 11

156277. 81

56

30118. 73

89212. 15

330115. 42

64

65416. 91

122294. 54

775313. 21

5. CONCLUSIONS

The presented results showed that AES has a better security than DES and Triple DES against brute force attack since AES takes more time to break by brute force program for a given key length. Time taken by AES algorithm to break the security considerably increases with the increase in key lengths. respectively.