Security For Voice And Video Traffic By Md5 Algorithm In Vpn

Sonam Wadhwa[1], Bindia[2], Taranjeet Kaur[3], Kunwar Pal[4]
[1,2,3,4] (Department of CSE, Lovely Professional Phagwara, India

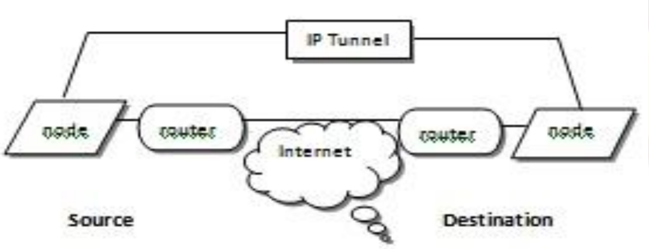
ABSTRACT

MD5 is a secure replacement to protect data over the internet .The Message Digest5 algorithm is used for data integrity with IPSec to protect the voice and video traffic in VPN. MD5 generates a unique value of 128-bit cryptographic message digest which are derived from input stream. This value is highly reliable and flexible that can be used to verify the data integrity of files content. If a single bit value in the file is modified, the MD5 checksum for the file changes.

Keywords- data integrity, checksum, MD5, firewall, VPN, Tunneling.

I. INTRODUCTION

MD5 is the extended version of MD4. The MD5 digest is used for data integrity in software systems. MD5 is used for storing secure information and transmitting data from source to destination, i.e. password and user name. Every user wants to gain access for some resources with entering the password. This algorithm is non reversible. It is hard to break because it is one way function. It can't restore to original message. Process time increases with message size increases to generate digest value. Using MD5 with IPSec as tunnel, we can provide the security over internet. MD5 is more secure as compared to other algorithms. This scenario consists of two nodes which are at source and destination and 2 routers are placed between them. IPSec tunnel used to protect the data by using MD5. It provides data integrity that the make sure data which are coming from source didn't modify.



For end to end communication, we use IPSec modes. The two modes of IPSec are Transport Mode and Tunnel Mode. Transport mode is used to protect the protocol and Tunnel mode is used to protect the whole IP datagram. IPSec used to protects the voice and video traffic by tunnel. Here router works as firewall. The protocol used for voice is G.722 and for video is H.263. HMAC-MD5 used for data integrity mechanism.

II. BASIC ALGORITHIM

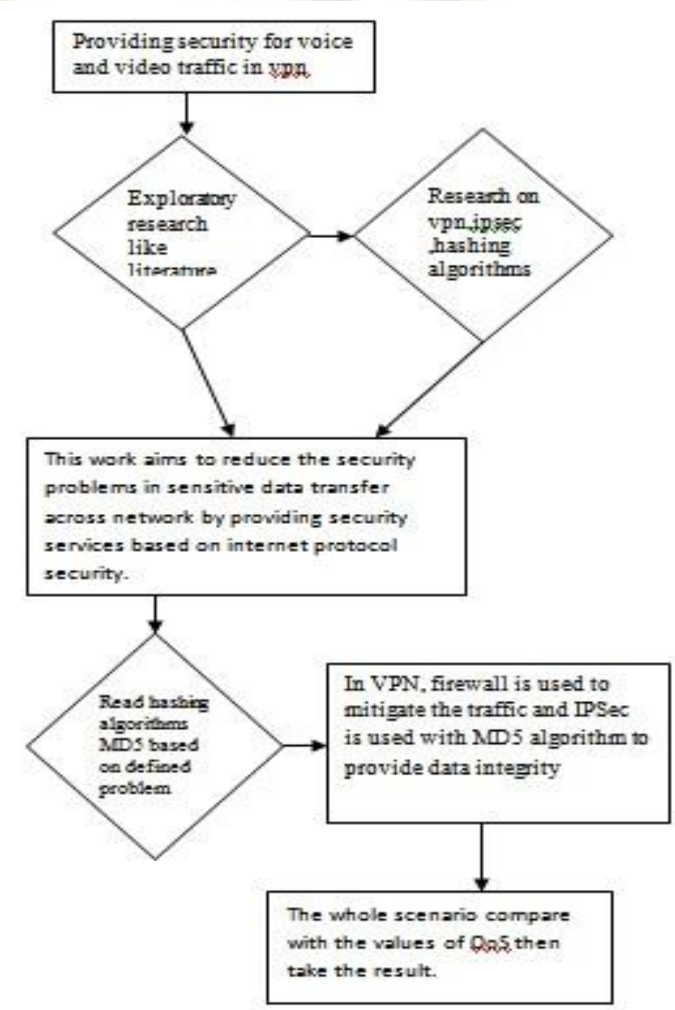
5 basic steps are involved in MD5 algorithm:

1. Append padding bits
2. Append Length
3. Initialize MD Buffer
4. Process Message in 16-Word Blocks
5. Output

III. METHODOLOGY

Step by step methodology is used for providing security in VPN for voice and video traffic. There is a flowchart which describes the scenario of research process. Flowchart consists various kind of boxes, arrows which describes the flow of information.

RESEARCH DESIGN:


Providing security for voice and video traffic in vpn
Exploratory research like literature
Research on vpn,ipsec ,hashing algorithms
This work aims to reduce the security problems in sensitive data transfer across network by providing security services based on internet protocol security.
Read hashing algorithms MD5 based on defined problem
In VPN, firewall is used to mitigate the traffic and IPSec is used with MD5 algorithm to provide data integrity
The whole scenario compare with the values of QoS then take the result.

IV. CONCLUSION

It mitigates the affect of packet delay variation and packet end to end delay. It reduces encapsulation time by using firewall. It provides data integrity over the internet by using algorithm that is Message Digest. If once the message is made then it can't be change. It is difficult to come back at the original message. It provides security for voice and video traffic over internet through established firewall between two ends and use MD5 with IPSec to provide data integrity. It provides better solution to the remove the congestion in the network through firewall.

V. ACKNOWLEDGMENT

I am very thankful to my Dissertation mentor and my friends who guided me time to time in developing my research related work. They left no stone unturned to help me. Because of their kind support and a very good knowledge of the subject, it becomes possible to complete my research. And finally God and my parents, due to them I am able to stand at this stage in all respects. Thanks to all of you.

REFERENCES

JOURNALS:

[1] W. Diffie and M. E. Hellman, (1976) "*New Directions in Cryptography* ", IEEE Transactions on Information Theory, Vol. 22, No. 6.

[2] Malik, Rupali Syal (2010), "*Performance Analysis of IP Security VPN",* International journal of Computer Application Volume 8-No.4,October 2012.

[3] Aruna Malik., Harsh K Verma (2012)*,"Performance Analysis of Virtual Private Network for Securing Voice and Video Traffic"*, International journal of Computer Application Volume 46-No.16,May 2012

[4] Dr. Arvind Kaur, Shivangi Goyal "*A Survey on the Applications of Bee Colony Optimization Techniques*", Guru Gobind Singh Indraprastha University, Dwarka , 2011.

[5] S. Khanvilkar and A. Khokhar (2004) *"Virtual Private Networks: An Overview with Performance Evaluation",* Communications Magazine 2004, pp 146 – 154.

[6] Dusan Teodoravic Mauro "*Bee colony optimization- A cooperative learning approach to complex transportation problems*", *ACM Transactions on Computational Logic 2011, proceedings of 16th Mini-Euro Conf. on Advanced OR and AI methods in transportation, pp51-60*

BOOKS

[7] William Stallings (2007); *"Network Security Essentials*: Applications and Standards"; Prentice Hall, Publications

WEBSITES

[8] http://www.irnis.net/gloss/md5-digest.shtml

[9] http://www.spitzner.net/md5.html

[10] http://www.cs.brown.edu/cgc/net.secbook/se01/handouts/Ch06-Firewalls.pdf