International Journal of Engineering, Science and Mathematics
Vol. 7 Issue 10, October 2018,
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

SECURITY VULNERABILITY ON MULTI- PROTOCOL LABEL SWITCHING IN VIRTUAL PRIVATE NETWORK

EZE, M.N., OGBU, M.N.C., ARINZE, S.N.
Department of Electrical and Electronic Engineering
Enugu State University of Science and Technology (ESUT)
Enugu State Nigeria

Abstract
Presently, Multi-Protocol Label Switching (MPLS) is the global data transmission technology used for delivery of voice and multimedia applications in Virtual Private Network (VPN). The main purpose of security is to protect the network assets. However, insecurity issues on the cloud of MPLS-VPN system remain the major challenges for the network designers. This paper discusses the security vulnerability on an MPLS-VPN with different enhancement techniques that have been implemented in the network in order to enhance it. Security vulnerabilities such as policy flaws, malicious software, protocol weaknesses and software / hardware vulnerabilities in MPLS-VPN need to be mitigated.
Keywords: Network Security, MPLS, VPN, Security Vulnerability, Enhancement Techniques.

1. Introduction

Multi- Protocol Label switching (MPLS) is an efficient and effective data transmission technology that forwards the packet across the network using short fixed-length known as label. MPLS is the latest technology developed by Internet Engineering Task Force (IETF) in 1999. This technology support many services such as Traffic Engineering (TE), creation of Virtual Private Network (VPN), and Quality of Services (QoS). VPN is an enterprise network that transmits data over the Internet by allowing users to securely enter into internal public infrastructure via unsecured network. According to Qureshu (2014) the main two functions performed by MPLS in VPN are packet forwarding and route distribution. During data transmission, there is no security of the VPN data traffic in MPLS networks. Thus there are number of insecurity issues associated with MPLS-VPN technology. The term security simple means protection against malicious attack by outsider / insider VPN users. Hackers gain illegitimate access to a MPLS-VPN network resources or the cloud. Security in a cloud based MPLS-VPN can be viewed from twodifferent perspective namely from service provider or from the user. For the user, the attack is against intrusions from outside of the VPN customer into his or her domain while for the

provider the attack is really available at the core side of MPLS network. Mende, D. et.al (2011) stated that MPLS does not provide protection against core, VPN customer security and Confidentiality, Authentication and Integrity (CAI) triad security requirement. There is need to provide an appropriate measure to mitigate those attack against cloud based MPLS-VPN.

Arora et al (2012) carried a study about the performance of different security techniques on a cloud network. The objective of the paper was to find quantitative terms such as Speed-up Ratio which help in implementation of security algorithms used to protect large traffic. The results showed that those security techniques when implemented on cloud based network like MPLS-VPN are more efficient than using them on single system. Usman, S. H. (2013) looked at the responsibilities of Internet Service Providers (ISP) to provide more security for their VPN customers. It was observed that people use internet as an avenue for illegal activities such as breaking into other people networks, stealing data and blocking legitimate users from services they subscribed. Veni, S., and Kadhar-Nwaz, G.M., (2012); demonstrated a new approach known as a new **(k, n)** Threshold Secret Sharing (TSS) scheme for security enhancement in MPLS in the VPN customers. The MPLS security issues like confidentiality, integrity, modification and fabrication of packet were stated. Okafor, et al (2013) formulated a security model called Self-Monitoring Analysis and Reporting Technology Intrusion Detection System (SMART-IDS). In the model, a site-to-site VPN scheme for LAN and wireless supports were provided. The developed model improved the backbone of MPLS-VPN for proper security implementation. The result of the model gave high throughput with an improved QoSmetrics.

Sidhu, A. and Mahajam, R. (2014) explained that security in the cloud service architecture is always a big issue for the vendor as well as users. Different security models and algorithms that have been applied have failed to solve most of the security threats especially in cloud domain. Most of the security techniques were used for securing ordinary file but not for the transfer of communication messages. The proposed model by the authors was a hybrid approach of various algorithms like Advanced Encryption Standard (AES) and Message Digest 5 Hash function (MD5- which is a cryptographic Hash function) and these will handle the security issues. The results obtained with the hybrid algorithms were implemented in JAVA language. This prevented the inside attack in the cloud MPLS-VPN. However the authors recommended the use of other encryption technique such as Rivest Cipher, Data Encryption Standard (DES) etc. for better security concern of the network cloud. It was also recommended that future research work on

comparison of security features under various attack in the cloud services should be carried out. Jakimoski, K. (2016) evaluated the security techniques for data protection in cloud computing. These security techniques were classified into four sections namely: confidentiality, access control, authentication and authorization. Secure Socket Layer (SSL) was used to overcome attacks like man-in-the-middle attack or Distributed Denial of Service (DDOS) attack.

2.Theoretical Background of MPLS-VPN

Multi-Protocol label Switching is a technology proposed by Internet Engineering Task Force (IETF) in order to overcome the limitation of traditional IP network. This technology is used by Internet Service Providers (ISP) especially in the core side of the network to give assure Quality of Service (QoS). Many telecommunications operators and ISP currently use services based on MPLS to create Virtual Private Networks (MPLS-VPN). This MPLS-VPN network is the technological method used to transport and route several types of network traffics using an MPLS backbone. There are three types of MPLS-VPN deployed in networks today, namely: Point-to-Point, Layer 2 and Layer 3 MPLS-VPN.

Point-to-Point MPLS-VPN used virtual leased lines like E1/T1 Ethernet and ATM to provide point-to-point connectivity between two sites. Layer 2 MPLS-VPN also known as Virtual Private LAN Service (VPLS) can offer what is called switch in the cloud service between LAN sites. Layer 3 MPLS-VPN utilizes layer Virtual Routing and Forwarding (VRF) to segment routing tables for each VPN customers.

MPLS-VPN can be implemented in two different methods: Overlay and Peer-to-Peer method. In overlay implementation method, the ISP gives the customer a dedicated circuit for the service delivery, while in peer-to-peer, ISP peers with the customer via Provider Edge (PE) routers. The PE routers have VRF instance to keep all the customers routes separate from other customer.

The elements of the MPLS-VPN are the customer network (VPN site), Customer Edge (CE) router, Provider network in the core (MPLS cloud), Provider Edge (PE) router, and Provider (P) router. These are shown in architectural diagram of a cloud based MPLS-VPN which is depicted in the figure below

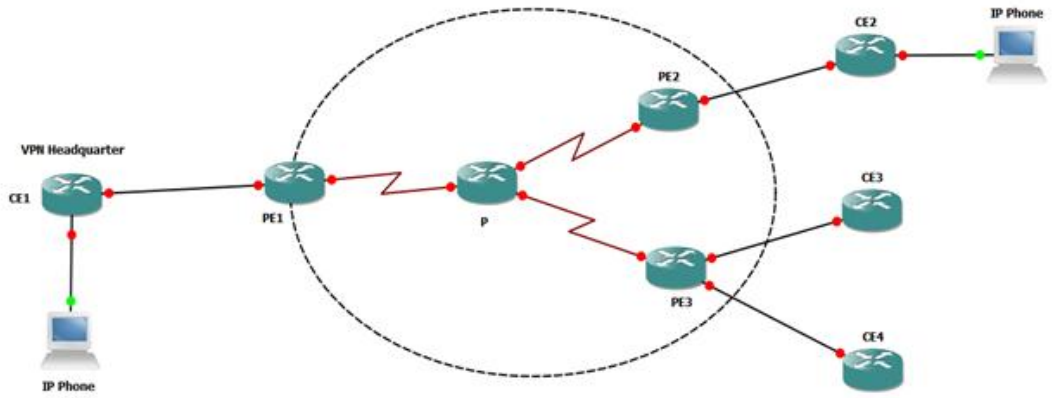

Fig 1 Architecture of MPLS-VPN

The core network of the MPLS consists of PE and P routers and PE routers are used to provide VPN services to the customers. Customer routers (CEs) are connected to the PEs. In MPLS-VPN technology packets can be transferred and processed in three different planes namely control, data and management planes. Each of these planes handle different functions in an enabled MPLS network. Exchanging, processing and establishing of routing information are done in a control plane, while data plane handle the implementation of those VPN data. Management plane is where the entire equipment configuration is managed. All these planes in an MPLS-VPN experience different security threats which need to be addressed.

3. Basic Properties of Security in MPLS-VPN

When considering security in an MPLS network, emphasis must be made by ensuring the whole network is secure. This will make none of the nodes to be vulnerable to attack. There are various basic properties of security in MPLS-VPN that need to be considered. They are confidentiality, integrity, authentication, and availability. They are the actual goal of any MPLS enabled network security.

- Confidentiality makes the data traffic on the network to remain private. Examples of attack methods are eavesdropping, hacking, IP spoofing and Denial of Service.
- Integrity property ensures that the message has not be modified in transit. Examples of the attack are viruses, worms, DoS and Trojans
- Authentication as a property ensures that the users of the MPLS network are who they say they are.
- Availability property gives the users easy access to the network and make all the nodes available at any point in time.

For any MPLS-VPN enterprise businesses to achieve its potential mission and vision, these properties of security must be addresses and all network must be protected for threats and vulnerabilities. Security objectives (properties) can be realize with the four A's notations **(AAAA)** meaning **A**uthentication, **A**uthorization, **A**uditing and **A**ction.

4. MPLS-VPN Security Analysis

MPLS-VPN security requirement are as follows: VPN address and traffic separation, protective model against IP-spoofing, hiding of the MPLS core structure and robustness against attacks. The key security requirement for the users is that their traffic is kept separate from other users and from the core side. In MPLS-VPN architecture, the address space is separated between users because only the PE routers know the IP-address of the user and their routes. Any VPN must use the same address space as any other VPN or as the MPLS core. Traffic routing between any two VPN or between any VPN and the core must be independent. It is important for the internal IP address of the core MPLS to remain hidden to the outside world. This will enable it to avoid attacks like Man-in-the-Middle or DoS.

5. Security Vulnerability in MPLS-VPN

Vulnerability comes from Latin word "Vulnus" which means wound and it is the state of being open or exposed to a threat. Vulnerability in MPLS-VPN means weaknesses in the MPLS technology, configurations, security policy, or in those inherent VPN devices such as routers, switches, servers and firewalls. Security vulnerability is referred to a cyber-security flaw in a network which makes the system open for attack. There are different types of security vulnerabilities such as policy flaws, malicious software, protocol weaknesses, and hardware and software vulnerabilities.

Policy flaws are the security policy weaknesses that create unforeseen threats when VPN users do not follow the policy thereby imposing risk to the system. Lack of continuity and lack of written policy are the examples of policy flaws in MPLS networks. Protocol weaknesses are those TCP/IP weaknesses that inherently made HTTP, FTP and ICMP unsecured in an MPLS-VPN. Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) are the examples of TCP/IP protocol that when they are weak, threats will take advantage of them to attacks the network. Various types of network equipment such as routers, firewall, switches constitute the hardware vulnerability. The hardware vulnerabilities that could be observed in an MPLS-VPN network are as follows: password protection, lack of authentication, routing protocol and firewall holes. Network devices, computer hardware and mobile devices have software as a common thing among

them. This software is the main source of security problems. In an MPLS-VPN, software such as router software, web browsers, web servers, Linux/ windows operating system can be exploited by an attacker due to bad software executed over the network. Software vulnerabilities can be seen as either design, implementation or configurations flaws. Examples of typical software vulnerabilities are buffer overflow, code or design defect, and web problem in SQL injection

Security vulnerability threats of MPLS-VPN occur in three different plane levels viz control, data and management levels. In the control plane , VPN routing information that passes through P and PE routers have various attacks such as alteration of the routing information and Denial of service, while in data plane level , the attack normally occurs as IP source address spoofing, protocol session hijacking, Trojans and replay of legitimate MPLS packet etc. This attack usually occurs between the VPN Customer Edge (CE) and Provider Edge routers. The security threats of the management plane are the attack to network devices via the administrative interface.

6. Security Enhancement Techniques

Network security is one of the important issues that organizations need guarantee for. Many techniques have been proposed for the enhancement of security vulnerability of MPLS-VPN. Techniques are Intrusion Detection System, Secure Socket Layer Encryption, Cryptographic Hashing Algorithm -- (Message Digest 5 (MD5) and Security Hash Algorithm), Advanced Encryption Standard, Rivest-Shamir-Adlehman (RSA), Diffie-Hellman and IP Security.

Encryption technique is the fundamental technique used for the protection of data in any network. This technique is normally used for the purpose of confidentiality. Encryption technique can be categorized into symmetric (private) and Asymmetric (public) key. Only one key is used to encrypt and decrypt data traffic in symmetric encryption technique while two keys are used in asymmetric type. There are four types of this technique commonly used in MPLS network, namely Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), Rivest- Shamir-Adlehman (RSA). DES is an algorithm that is used for parity check to verify the integrity of the data traffic in a network. RSA is a public key scheme used for encrypting message, exchanging keys and creating digital signatures. This technique is based on exponentiation that uses modular arithmetic to secure data during transmission. This technique is commonly used to directly encrypt user data transmission which takes to time to decrypt. Transport Layer Security formerly known as Secure Socket Layer technique is used to protect a layer 3 and

4 application such as HTTP by adding encryption and authentication to a layer 2 and 3 protocol.

IPSecurity (IPSec) technique is usually run with encryption like Encapsulating Security Protocol (ESP) and Authentication Header (AH) on the customer edge router or over the MPLS cloud. Diffie-Hellman technique is the key that exchange key between two users by generating a shared private key across an unsecure domain. This technique was named after Whitfield Diffie and Martin Hellman. Intrusion Detection System is another technique that logically combines with one or more firewalls to protect networks. The four main types of IDS are as follows:

- Network intrusion detection system
- Host-based intrusion detection system
- Perimeter intrusion detection system
- Virtual machine based intrusion detection system

IDS technique is used to strengthen the system security thereby increasing the resistance to core and outside MPLS cloud attacks.

7. Conclusion

This paper proposed a study of security vulnerability on Multi-Protocol Label Switching in Virtual Private Network. Basic security properties and requirement were explained. Different techniques that had been used to enhance security on MPLS network were stated. As a future work the paper is proposing the use of Software Defined Algorithm as a new security approach for a Cloud Based MPLS-VPN.

References

Afolabi, A. O., and Atanda, O. G. (2016). "Comparative Analysis of some Selected Cryptographic Algorithms". *Computing Information Systems, Development Informatics and Allied Research Journal.Vol. 7,* No. 2, pp. 41 -52.

Arora, P., Singh, A. and Tiyagi, H. (2012).Evaluation and Comparison of Security Issues on Cloud Computing Environment.*World of Computer Science and Information Technology Journal (WCSIT),* Vol. 2 No. 5, pp. 179 - 183.

Jakimoski, K. (2016). "Security Techniques for Data Protection in Cloud Computing". *International Journal of Grid and Distributed Computing.Vol. 9*, No. 1, pp. 49 -56.

Mende, D., Rey. E. and Schmidt, H. (2011).Practical Attacks against MPLS or Carrier Ethernet Networks.*Enno Rey Netzwerke (ERNW) providing Security.*Version 9.

Okafor, K.C., Okezie, C.C., Udeze, C.C. and Okwuelu, N. (2013). "SMART-IDS: An Enhanced Network Security Model in IP- MPLS based VPN". *African Journal of Computing and ICT Reference format, Vol. 6,* No. 3, pp. 135-146.

Qureshi, K.N, Abdullah, A.H, Hassan, A.N, Sheet, D.K and Anwar, R.W, 2014. Mechanism of Multi-ProtocolLabel Switching for forwarding packets and performance in Virtual Private Network.*Middle-East Journal of Scientific Research*.Vol. 20, No. 12, pp 2117-2127.

Sidhu, A., and Mahajam, R. (2014)."Enhancing Security in Cloud Computing Structure by Hybrid Encryption".*International Journal of Recent Scientific Research.Vol. 5,* No.1, pp. 128 -132.

Usman, S. H. (2013). "A Review of Responsibilities of Internet Service Providers toward their customers network Security".*Journal of Theoretical and Applied Information Technology.Vol.49,* No.1, pp. 70 -78.

Veni, S. and Kadhar-Nwaz, G. M. (2012). "A new Approach to Enhance Security in MPLS network".*Advanced Computing: An International Journal, Vol.3,* No.3, pp. 75 – 80.