PHYSICAL SCIENCES

ISSN (Print): 24490954
ISSN (Online): 26364972

Improved Security Techniques in Multi-Protocol Label Switching

[1]Adoga H. U., [2]Imam H. A., [3]Dauda A., [4]Og-bonoko J. F., [5]Bako U. M., [6]Ochang P. A., [7]Agushaka J.O

[1 3 4 5 6 7] Department of Computer Science, Federal University Lafia, Nigeria
[2]Department of Engineering and Environment, Northumbria University Newcastle, United Kingdom

**Corresponding Email: Haruna.umar@science.fulafia.edu.ng*

Manuscript received:24/09/2018 Accepted: 11/06/2019 Published: June 2019

ABSTRACT

Multi-Protocol Label Switching has replaced Layer 2 ATM and Frame Relay technology for a while now, which provides high speed networking and traffic engineering. MPLS technology uses Label switching technique instead of IP routing when forwarding traffic to a destination, which makes it more scalable and flexible. However IP MPLS networks are not secure from outside threats and threats from within the network. In this paper, inherent security provided by a typical MPLS network is evalu-ated, and some combinations of security techniques are provided to improve upon it. To test some of the methods for enhancing the security of IP MPLS VPN network, two major attacks were carried out, i.e. Injection of IPv4 Routing Information, and Cracking of MD5 password with Authentication set to OFF and ON respectively. In order to protect the confidentiality, availability and integrity of data, in-herent security can be enhanced using step-by-step combination of the security techniques such as IP-Sec tunnels at the Customer Edge's routers and a complex MD5 authentication between routing proto-cols. The MPLS network design was carried out to capture two locations in the UK, i.e. Newcastle and London. GNS3 Network emulator was used to achieve the desired results, with real Cisco IOS images, and finally, some thoughtful recommendations were provided, which are aimed at providing a better implementation of MPLS VPN on computer networks.

Keywords:*MPLS, Network Security, MPLS VPN, MPLS security, IPSec, MPLS Authentication, computer networks.*

INTRODUCTION

The demand for converged, scalable, and reliable IP-based MPLS VPN services has made security and privacy of service provider and enterprise customer networks a critical issue. MPLS enables service providers and enterprise customers to de-liver key value added services, while maintaining enhanced end-to-end Quality of Service (QoS) guarantees. A label-switched path according to Upul *et al.,* (2014), is defined as a one-way path that data follows from one particular node (a router able to do label switching) to a different node, where intermediate nodes can be traversed.

The goal of this work is to improve the security aspect of MPLS in a controlled network environment, by applying some combinations of security methods and attempt some attacks. Furthermore we will discover general effect of deploying some of the methods on the proposed network.

Huge amount of traffic are sent from one custom-er location to another with different requirements such as speed, security, confidentiality (Palmeiri et al, 2007). MPLS has proven to be a stable solu-tion that provides different features such as Layer 2 and 3 VPN, Traffic Engineering, QoS and sig-naling protocols for information exchange between network devices within the MPLS domain.

MPLS encapsulates IP packets in an MPLS pack-et, which forms a virtual circuit called label switched path (LSP) in the IP backbone. This process is performed on two different types of routers, label switch router (LSR) and the label edge router (LER). The provider edge router (in-gress) performs a routing lookup and interfaces the customer edge (CE) router and the IP MPLS network. When an unlabeled packet is received by an LER, the LER inserts MPLS labels into the packet's new MPLS header using a push opera-tion and then passes it on to the next hop router (LSR) along the path. The next hop router (LSR) that receives the packet examines the MPLS label and performs a swap or pop operation on it (Jacob, D *et al.,* 2017).

The P router switch packets based on swap labels and label lookups, then makes forwarding decisions through the label switched path (LSP) to the provider edge (PE 2 egress) router. When the egress router received the packets, label is re-moved then the packet is sent to the destination network (Israr-Ul-Maqbool *et al,* 2015). Fig 1 shows how MPLS forwarding mechanism traffic works.

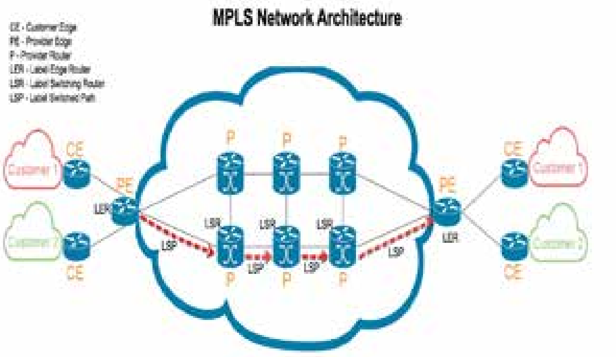


Fig 1. MPLS Network Architecture (Is-rar-Ul-Maqbool *et al,* 2015).

Below are some of the possible attacks on control and data planes of on MPLS network, which were listed by Paul (2014).

- Injection of IPV4 routing information
- Inject routes into VPN
- Denial of service
- Inject labeled packets
- Disable IP TTL
- Traffic Engineering
- Insertion /deletion or modification of packets

Related Work

Discussions from (Cisco 2014; Behringer *et al.,* 2005) have shed enormous light on MPLS security, between the security provided on MPLS based VPN to layer 2 VPN. Behringer *et al.,* (2005), suggested some practical ways to harden the MPLS network. They assumed the MPLS core to be trusted and secure, but it leads to some security problems, and that there is no guarantee that VPN data are not sniffed or read in transit over the MPLS core. They further explained the way to tackle the current threats in MPLS network was by enhancing it using some methods such as authentication through MD5, access control, encryption using IPSec tunnel.

According to (Davie, B. S. and A. Farrel 2008; Feng *et al.,*2004), MPLS do not provide authentication, encryption, anti-replay and protection from the Internet or within the core. However, they suggested some security techniques that can be used to tackle the security threats.

Feng *et al.,* (2004), Implemented and analyzed an MPLS VN based on IPSec and concluded that if Internet Key Exchange (IKE), Certificate Authority (CA) and IPSec are used, the VPN security will be high but will consume router resources.

Mende *et al,*. (2011), also implemented a practical attack in MPLS networks using a tool called Loki to exploit the vulnerabilities of the control plane protocol such as BGP and LDP session with the core routers, injecting IPv4 routing information, injecting MPLS VPN routing information.

According to Saad *et al.,*(2006), they discussed the effect of MPLS-based tunnels on end-to-end virtual connection service and security; it reduces throughput of TCP flow and add more overhead. David *et al,.*(2003), proposed a cryptographic protocol to protect the MPLS labels by encryption on labels to prevent header modification but do not provide confidentiality of data.

Cisco, (2014), reiterate the use of encryption pro-tocol such as HTTPS and SSH instead of MD5 for authenticating protocols, Telnet, HTTP and any protocol that will expose the core devices in the backbone to malicious users to be disabled. Since the MPLS core does not provide such, au-thentication and encryption methods are used in the MPLS architecture.

(Cisco and Aprcot, 2015; Lin *et al.,* 2010), emphasized that the control plane has to be secure using MD5 authentication for guaranteeing the security of the routing information and isolation of the routing. The MPLS GNS3 LAB control plane that will be authenticated are; MD5 authentication for LDP with key chain, MD5 authentica-tion between

PE-to-PE MP-BGP (iBGP) between PEs and IGP (Core IGP, PE to CE) that is OSPF.

The core devices runs LDP sessions and key chains management are now available and each specific series of key has a lifetime duration and rotates from one key to another, this lessening the possibility of a key being compromised, compared to basic LDP TCP MD5 Cisco, 2011; Lin *et al,.* 2010).

Working along the same line, that is, to enhance QoS and security for delay sensitive traffic, Awais *et al,.* (2015), employed the technique of Traffic Engineering (TE) using MPLS and com-paring it to MPLS without TE concepts on a high loaded network. The work proposed the design and simulation of network around TE concepts using Interior Gateway Protocol (IGP).

Mushtag *et al.,* (2014), used a combo of MPLS and DiffServ to enhance QoS in New Generation Networks (NGN) taking advantage of the Traffic Engineering capabilities of MPLS. The DiffServ was used to address the limitation of non-differentiation of Services by MPLS.

(Davie *et al,.* 2008; Farell and Farrel 2015) also explained that the security in MPLS network can be enhanced using multi-path routing with the combination of (k, n) threshold secret sharing scheme, which will not be possible for an attacker to intercept all the data packets. Another point on multi-path is when an IP packet is received on MPLS ingress router, the packet can be split into n shadow (shared) packets, then assigned to maximally-node disjoint paths through the MPLS provider network and reconstructed at the egress router. From a network point of view, it's impos-sible for the attacker to tap at least 'K' paths to reconstruct the packet, therefore reduce the risk of man-in-the-middle attack.

Upul *et al.*, (2014), in their work, focused on the security vulnerabilities of the MPLS Transport Profile (MPLS-TP). Their approach to the security of MPLS is on the implementation of smart grid. Upul *et al.,* (2014), Further observed that the Cisco IOS does not implement security recom-mendations for OAM protocols, such as BFD and PSC, thus exposing them to different spoofing attacks. Based on the work done by Upul *et al.*, (2014), "An alternative solution for preventing spoofing attacks on BFD and PSC messages in non-IP MPLS core networks is to use hop-by-hop security (MACsec)." We however noticed that Upul *et al.,* (2014), did not consider attacks on the MPLS core such as IP route injection and MD5 password cracking.

Finally, we can conclude that there are security gaps, flaws and threats in MPLS VPN deployments, and have suggested some combination of techniques that will combat these flaws.

MATERIALS AND METHODS

This part of the paper explains the methods used to investigate some of the MPLS security tech-niques on MPLS VPN and IP/MPLS on layer 3 applications. The Graphical Network Simulator 3 (GNS3) emulator version 1.5.3 was used due to its stability and availability of virtual device options. The diagram below in Fig 2 shows the MPLS topology that will be used for the implementation in GNS3. This forms the basis for our investigation into MPLS security, using real Cisco router IOS im-ages.

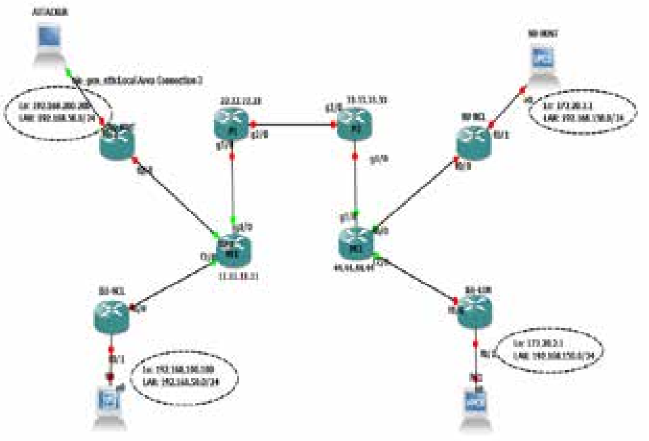


Fig 2. MPLS Network Topology in GNS3

A remote PC was used to emulate the connection using local NIC loopback interface, and some virtual link interfaces were created at the remote end of the connection. The design consists of two VPN sites for different customers that will be connected via the same service provider MPLS backbone network. Cisco IOS image C3725-adventerprisek9-mz.124-15.T5.bin-200 was used for CE router and C7200-jk9s-mz.124-13b.bin-512 was used for the P and PE routers, because they are stable, with firewall capabilities and high CPU speed. The topology in fig 2 shows two sites, Northumbria University and IEE, both have VPN sites that are terminated in Newcastle and London, with New-castle being the headquarters.

Northumbria University in Newcastle (NUNWC) will be using OSPF between CE and the peering PE, and the London branch will be using OSPF routing protocol between CE and PE router. The IEE in Newcastle and the branch in London will be using Static routing between CE and peering PE router. The Provider Edge (PE) and the Pro-vider (P) router will be running OSPF and Border Gateway Protocol (BGP) in the MPLS backbone as shown in fig 3 below. The figure below shows a graphical representation of the routing protocols that are implemented in the MPLS network design used in this paper.

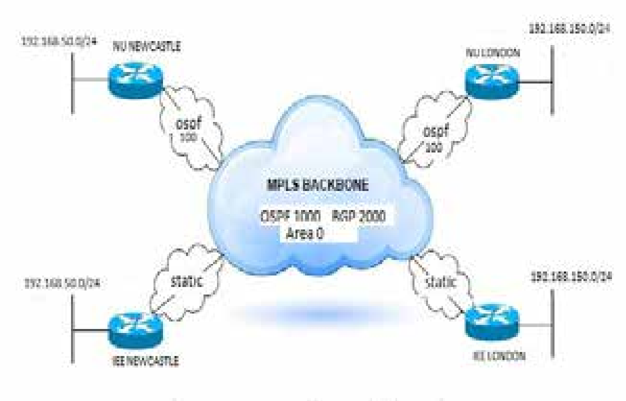


Fig 3. Routing Protocol used in the MPLS VPN experiment

To test if MPLS truly provides privacy, overlap-ping IP addresses were used between both Northumbria and IEE to test if there will be con-flict. Table 1 below shows the IP address scheme that was used for the router interfaces, using dif-ferent class of IP address for easy troubleshooting and analysis. The P and PE routers are configure with class A IP address and a separate block of IP address was configure on the PE loopback so that they are not unintentionally summarized in the backbone.

Table 1. IP Addressing scheme used for the MPLS topology

Router Name	Status	Inter-face	IP Address
NU – NCL	CE	Lo 0	192.168.200.200/32
		Fa 0/0	10.1.1.9/30
		Fa 0/1	192.168.50.1/24
NU – LON	CE	Lo 0	172.20.2.1/32
		Fa 0/0	10.1.2.2.30
		Fa 0/1	192.168.150.1/24
IEE – NCL	CE	Lo 0	192.168.100.100/32
		Fa 0/0	10.1.1.9/32
		Fa 0/1	192.168.50.1/24
IEE – LON	CE	Lo 0	172.20.1.1/32
		Fa 0/0	10.1.2.2/30
		Fa 0/1	192.168.150.1/24
PRO-VIDER EDGE 1	PE	Lo 0	44.44.44.44/32
		Fa 0/0	10.1.2.1/30
		Fa 2/0	10.1.2.1/30
		Gig 1/0	10.30.10.4/24
PRO-VIDER EDGE 2	PE	Lo 0	44.44.44.44/32
		Fa 0/0	10.1.2.1/30
		Fa 2/0	10.1.2.1/30
		Gig 1/0	10.30.10.4/24
PRO-VIDE 1	P	Lo 0	22.22.22.22/32
		Gig 1/0	10.10.10.2/24
		Gig 2/0	10.20.10.2/24
PRO-VIDER 2	P	Lo 0	33.33.33.33/32
		Gig 1/0	10.30.10.3/24
		Gig 2/0	10.20.10.3/24

MPLS Configurations – Enabling MPLS

Before MPLS starts running and functioning fully, the service will be enabled on the backbone routers, PE2, P2, P1, PE, and on all the interfaces in the backbone excluding those peering with the customer edge (CE) device.

Secondly, CEF has to be enabled before running MPLS and Label Distribution Protocol (LDP) needs to be enabled, so that labels are distributed. Interfaces that will participate and distribute la-bels in MPLS will need to be enabled using the command ‘mpls ip’ globally.

Virtual Routing & Forwarding (VRF) Config-uration

VRF configurations and parameters for the two MPLS VPN sites that were implemented on the LAB are in table 2 below.

Table 2. VRF parameters

	PE1	PE2
VRF Name		
NU-NCL	100:NU - NCL	100:NU – LON
IEE-NCL	200:IEE - NCL	200: IEE - LON
Route Targets		
NU-NCL Export	100:1	100:1
NU-NCL Import	100:1	100:1
IEE – NCL Export	200:2	200:2
IEE – NCL Import	200:2	200:2
Route Dis-tinguishers		
NU – NCL	100:1	100:1
IEE - NCL	200:2	200:2
Interfaces		
NU – NCL	FastEthernet 0/0	FastEthernet 0/0
IEE – NCL	FastEthernet 2/0	FastEthernet 2/0

PE -to– PE Configuration

Nowadays, most threats are from the Internet, service provider's nightmare is to protect their core. In MPLS network, most likely point for an attack is between the PE – PE device in the MPLS core using a MITM attack.

CE-to- PE Configuration

The link between the CE and the PE can use any routing protocol as stated earlier, in our scenario the link between CE's and PE's for NU-NCL and NU – LON will be running the Open Shortest Path First (OSPF) protocol, while static routing will be used for IEE – NCL and IEE – LON re-spectively.

Loki Tool

A tool called Loki that is used in attacking the Control or Data Plane was installed on a laptop that runs windows 7 operating system, and was connected to the NU–NCL LAN using a loop-back adapter. Loki tool has a uGraphical User Interface (GUI) that can be used in carrying out attacks, such as Injection of IPv4 routing information, LDP session, and Injecting MPLS-VPN routing information, and cracking MD5 secret.

MPLS Access Control Security Technique

Extended access list 'AHMAD-SEC' was created and configured at the ingress interface FA0/0 and Fa0/0 of the PE router to filter traffic that is not meant to enter the PE router, and permit only OSPF routing protocol then block all other traffic from the CE router.

MPLS Physical Security Technique

All passwords set on the MPLS routers on GNS3 were configured using 'service pass-word-encryption', to prevent from being read by an attacker in case he/she retrieves a copy of the configuration file. Another point is to implement 'no service password-recovery' on the core device, especially the critical devices on the backbone.

MPLS Authentication Technique

The routing protocol that was used in the MPLS LAB within the MPLS backbone is MP-BGP, LDP and IGP (OSPF), and those used between the CE-to-PE are OSPF and static routing. All interfaces that connect to the CE devices that run a routing protocol on the links will be authenti-cated with its peering interface on the PE device.

Loki starts a background thread, which sends keep-alive packages to open the connection. Then takes part in the neighbor discovery process by sending a hello message after activating the hello button.

MPLS Encryption Technique

Static IPSec tunnels were configured between NU-NCL router and NCL-LON router and also between IEE-NCL and IEE-LON router on the MPLS GNS3 LAB.

MPLS Isolated Infrastructure Technique

Enterprise customers mostly isolate additional services such as Internet with their Service Pro-vider network, which can expose the client net-work and devices. Cisco, (2011) Recommends separating and isolating different services such as Internet and VPN at the customer and service provider edge to use dedicated router for each service rendered, this has been implemented on the proposed MPLS network topology.

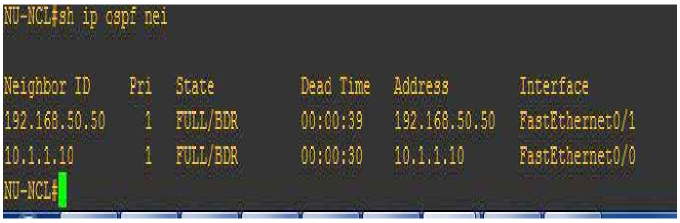
MPLS Control and Data plane Hardening

Usually the Provider Edge routers are prone to attack by means of squeezing the resources in the form of DoS attack, which leads to memory over flow and high CPU utilization and distorts the routing information from being sent properly. Hardening the routing protocol in the control plane can mitigate this form of attack.

RESULTS AND DISCUSSION

In the first attack carried out on the MPLS net-work topology, an assumption was made that an attacker was able to connect their system on NU-NCL LAN port, whereby the network admin did not enable port security on some few ports. The attacker used Loki tool and received an IP address of '192.168.50.50' from the DHCP server. Loki starts a background thread, which sends keep-alive packages to hold the connection open and the signaled data valid. Then takes part in the neighbor discovery process by sending a hello message after activating the hello button on the LOKI interface.

The NU-NCL router is running OSPF on Fa0/0 and Fa0/0 interface on the PE router, with no authentication between them. The CE router re-ceived the OSPF hello message from the attack as shown in figure 4, a 2way neighbor relationship was established, which shows the peer is '192.168.5.1' in state 'FULL' with router ID '192.168.200.200' in area 0. Fig 5 below shows the output from the CLI of NU-NCL router.



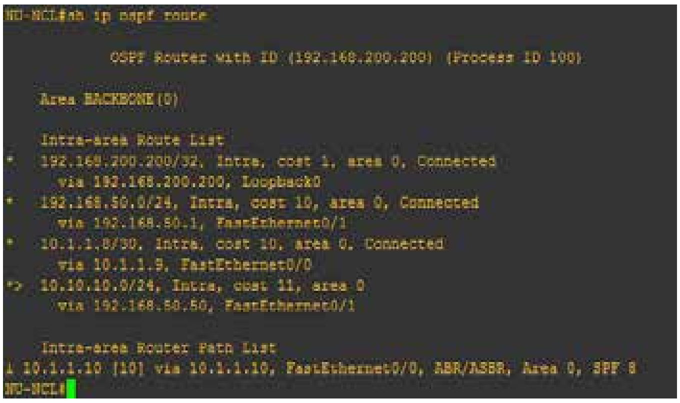
```
NU-NCL#sh ip ospf nei


Neighbor ID     Pri   State           Dead Time   Address         Interface
192.168.50.50     1   FULL/BDR        00:00:39    192.168.50.50   FastEthernet0/1
10.1.1.10         1   FULL/BDR        00:00:30    10.1.1.10       FastEthernet0/0
NU-NCL#
```

Fig 4. CLI Neighbor Relationship

Secondly, after making the neighbor relationship, the attacker attempted to inject IPv4 route from CE route, telling the router to get to the '10.10.10.0/24 network; send the traffic through me (the attacker's computer) as the de-fault gateway.

Second Attack with Authentication set to ON

In this scenario, the authentication was set to ON, both on Fa0/0 and Fa0/0 interface on NU-NCL and the PE router using 'ip ospf mes-sage-digest-key 1 md5 test'. The attacker initiated Loki tool and was able to crack the password 'test'. After cracking the MD5 password, the at-tacker then established a neighbor relationship with the CE (NU-NCL) router and injected net-work '10.10.10.0/24' into the routing table, saying to reach '10.10.10.0/24 network' send your traf-fic to '192.168.50.50'. Figure 5 below shows the ipv4 route that was injected into the routing table.



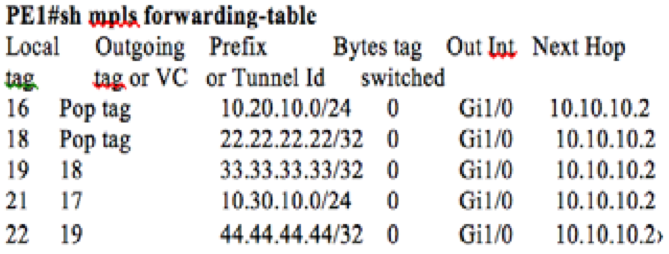
```
NU-NCL#sh ip ospf route

            OSPF Router with ID (192.168.200.200) (Process ID 100)

    Area BACKBONE(0)

    Intra-area Route List
*   192.168.200.200/32, Intra, cost 1, area 0, Connected
      via 192.168.200.200, Loopback0
*   192.168.50.0/24, Intra, cost 10, area 0, Connected
      via 192.168.50.1, FastEthernet0/1
*   10.1.1.8/30, Intra, cost 10, area 0, Connected
      via 10.1.1.9, FastEthernet0/0
*>  10.10.10.0/24, Intra, cost 11, area 0
      via 192.168.50.50, FastEthernet0/1

    Intra-area Router Path List
i 10.1.1.10 [10] via 10.1.1.10, FastEthernet0/0, ABR/ASBR, Area 0, SPF 8
NU-NCL#
```

Fig 5. IPv4 Route Injection

Lastly, after replacing MD5 password on the interfaces between the NU-NCL and the peering PE routers from 'test' to 'ip ospf mes-sage-digest-key 1 md5 'Nu10-Ncl' on both Fa0/0 and Fa0/0, Loki could not crack the password and the attacker was disconnected from the neighbor relationship. This verifies the importance of implementing a strong password for MD5 authentication and has enhanced the security in method in the IP MPLS LAB.

MPLS verification Using Show Commands

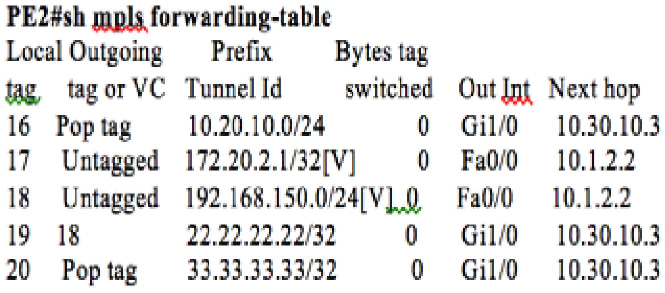
MPLS label bindings are distributed to FEC using 'show mpls-forwarding-table' as shown for PE1 and PE2 in figure 6 below.



```
PE1#sh mpls forwarding-table
Local   Outgoing    Prefix          Bytes tag   Out Int   Next Hop
tag     tag or VC   or Tunnel Id    switched
16      Pop tag     10.20.10.0/24   0           Gi1/0     10.10.10.2
18      Pop tag     22.22.22.22/32  0           Gi1/0     10.10.10.2
19      18          33.33.33.33/32  0           Gi1/0     10.10.10.2
21      17          10.30.10.0/24   0           Gi1/0     10.10.10.2
22      19          44.44.44.44/32  0           Gi1/0     10.10.10.2›
```

Fig 6. Show mpls forwarding-table output on PE1 router

The output of the show mpls forwarding-table command was also used on the PE2 router and the output is shown in figure 7 below.



```
PE2#sh mpls forwarding-table
Local Outgoing    Prefix                 Bytes tag
tag    tag or VC  Tunnel Id              switched   Out Int   Next hop
16     Pop tag    10.20.10.0/24          0          Gi1/0     10.30.10.3
17     Untagged   172.20.2.1/32[V]       0          Fa0/0     10.1.2.2
18     Untagged   192.168.150.0/24[V]    0          Fa0/0     10.1.2.2
19     18         22.22.22.22/32         0          Gi1/0     10.30.10.3
20     Pop tag    33.33.33.33/32         0          Gi1/0     10.30.10.3
```

Fig 7. Show mpls forwarding-table output on PE2 router

The output from NU London branch router has learned '192.168.200.200' (loopback address) of Newcastle router via '10.1.2.1' (PE2 Fa0/0) in-terface on the VRF interface peering with NU-London site.

The second test was LAN to LAN using simulat-ed PCs to verify connectivity between the two ends. The remote VPN PC is '192.168.150.50 (VPS1) on IEE-LON branch site.

IEE-NCL#ping192.168.150.50 so 192.168.50.100

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.150.50, timeout is 2 seconds:

.!!!

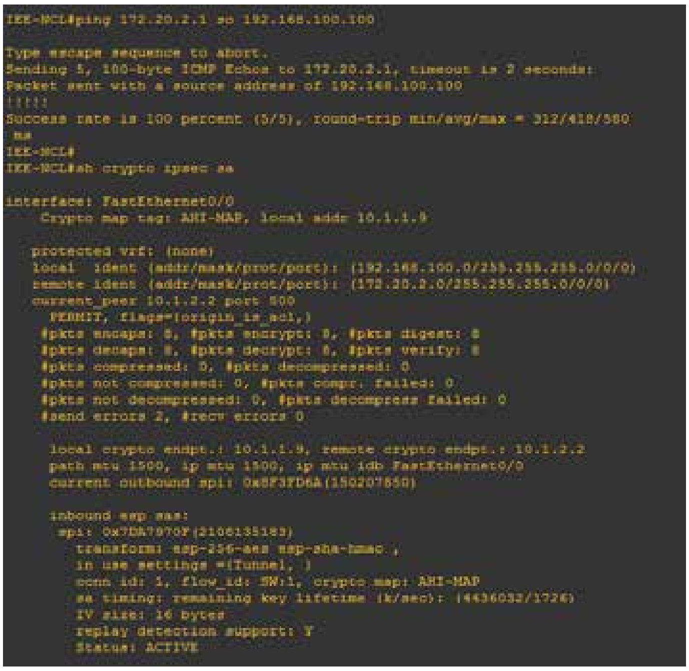
Success rate is 80 percent (4/5), round-trip min/avg/max = 1276/1276/1276 ms

Two VPN sites can have the same IP address but since they are on different VRF, a ping from one VPN to the other client VPN is not possible. This clearly shows how MPLS service provider net-work demarcates VPN connections, which is an inherent security feature that MPLS VPN pro-vides.

Evaluation of the Security Methods

Authentication - The first attack was there No Authentication on the interface between NU-NCL and PE1 VPN, whereby Loki was able to join the VPN connection and inject a route to the routing table. The second attack was the MD5 authentication was ON but the password was weak and set to 'test'. Loki was able to crack the test password using brute force attack but after changing the MD5 password to 'Nu10-Ncl' the attack was not successful because random pass-word mixed with uppercases, lowercases and numbers were used to prevent the password from being compromised.

Encryption – Static IPSec was implemented in our GNS3 LAB between each customer VPN on the CE's routers and can be tested by pinging IEE – LON loopback interface '172.20.2.1' using IEE – NCL loopback address of 192.168.100.100 as source address. From fig 20 below, the output can be seen using the 'show crypto IPsec sa details' as shown in figure 8 below, indicate packets being encrypted and decrypted through interface Fa0/0 and the IPSec tunnel is ACTIVE.



```
IEE-NCL#ping 172.20.2.1 so 192.168.100.100

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.100
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 312/418/580
 ms
IEE-NCL#
IEE-NCL#sh crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: AHI-MAP, local addr 10.1.1.9

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.100.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.20.2.0/255.255.255.0/0/0)
   current_peer 10.1.2.2 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 8, #pkts encrypt: 8, #pkts digest: 8
    #pkts decaps: 8, #pkts decrypt: 8, #pkts verify: 8
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 2, #recv errors 0

     local crypto endpt.: 10.1.1.9, remote crypto endpt.: 10.1.2.2
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x8F3FD6A(150207850)

     inbound esp sas:
      spi: 0x7DA7970F(2108135183)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, crypto map: AHI-MAP
        sa timing: remaining key lifetime (k/sec): (4436032/1726)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE
```

Fig. 8 Crypto IPSec for IEE-NCL

Access Control - The access list was configured at the PE ingress interface to limit access to only specific network prefix with the VPNS. Using the command 'Show access-list AHMAD-IN' and 'Show run | sec int Fa0/0' shows the output from PE1 router that is connected to Northumbria University in Newcastle and the access list that was configured to secure the interface. The ex-tended access list AHMAD-SEC allows only OSPF routing and prevent any connection to be made to the PE1 router other than Newcastle branch routes and the PE1.

The access list 'AHMAD-SEC' was tested by telnet and ping from IEE-NCL to PE1 router, which were both unsuccessful.

After many unsuccessful attempts and tests, the access list was disabled using the command 'no ip access-list AHMAD-SEC' on that specific inter-face on the PE! Router and run another ping and telnet session on the NU-NCL router and the re-sult was successful as shown below.

NU-NCL #ping 10.1.1.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 30/40/60 ms

NU-NCL #telnet 10.1.1.10
Trying 10.1.1.10 ... Open
User Access:
Password:

Physical Security - The MPLS GNS3 LAB used 'service –password encryption', whereby all passwords are encrypted on the routers. Also Cisco Discovery Protocol function was disabled with 'no cdp enable' under the interface configu-ration and 'no cdp run' in global configuration mode.

Control and Data plane Hardening - The con-trol and data hardening that were implemented include, maximum routes and BGP dampening for each VRFs, to limit injection of so many routes and BGP connections and re-initiate after a specific time frame to avoid bombardment from the VPN clients as explained in the previous sec-tion.

CONCLUSION

We have noted that the basic IP MPLS imple-mentation cannot tackle the modern and current threats such as DoS attacks and MiTM attacks within the backbone. In this paper, we evaluated the current security level of MPLS VPN and was enhanced using a combination of security techniques. A tool called Loki was used in attacking the control plane of the MPLS network. Two attacks were carried out; we set MD5 authentication to ON and OFF, we then carried out IPv4 route injection on the de-signed network. Authentication using MD5 pass-word was set between the customer edge router and the provider edge router. After running Loki, a weak password was set and Loki cracked the password using a brute force attack and injected a route into the CE routing table. The second attack was carried out but this time a strong password was set, and the Loki tool could not crack the MD5 password because some combination of al-phanumeric characters and symbols were set as the password.

With respect to further recommendations, the use of IPSec encryption should be implemented be-tween the Customer Edge routers instead of the Provider Edge routers, to avoid burden on the PE routers to encrypt and decrypt data packets, as they pass through the backbone which can lead to high CPU utilization and memory overload. Au-thentication using MD5 with keychain within the routing should be implemented. ACL should be configured on the Provider Edge interface that is peering with the Customer Edge router and permit only routing protocol on the interface, this will prevent packets to be injected into the core.

REFERENCES

Awais Q., *et al.* (2015). “Traffic Engineering Using Multi Protocol Label Switching (MPLS) for Delay Sensitive Traffic”. 2015 IEEE Conference on Computational Intelligence and Communication Technology. DOI: 10.1109/CICT.

Behringer, M and Morrow, J. (2005). MPLS VPN Security. Cisco (2011). Cisco Live!: MPLS VPN Security BRKSEC-2145. [Online]. Available at: http://monsterdark.com/wp-content/uploads/MPLS-VPN-Security.pdf {Accessed: 24 Mar, 2016}

Cisco (2014). MPLS WAN Technology Design Guide. [Online]. Available at: http://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-MPLSWANDesignGuide AUG14.pdf {Accessed: 23 Mar, 2016}

Cisco and Apricot. (2015). MPLS Woorkshop https://nsrc.org/workshops/2015/apricot2015/raw- attachment/wiki/Track3MPLS/01-Apricot2015_Agenda.pdf {Accessed: 10 Feb, 2017}

David A. Barlow, Vasos Vassiliou, Henry L. Owen (2003), A Cryptographic Protocol to Protect MPLS Labels. Proceedings of the 2003 IEEE Workshop on Information Assurance. United States Mil-itary Academy, West Point, NY

Davie, B. S. and A. Farrel (2008). MPLS: next steps, Morgan Kaufmann.

Farrel, A. and Farrell, S., 2015. Opportunistic Security in MPLS Networks. Work in Progress, draftietfmplsopportunistic-encrypt-00.

Feng, D., Ma, K and Ren, R. (2004). “A Detailed Implementation and Analysis of MPLS VPN based on IPSEC,” in Proceeding of the IEEE Third International Conference on Machine Learning and Cybernetics, Shanghai.

Israr-Ul-Maqbool, K. V. (2015). “MPLS Security: Acute Protection of MPLS Networks from Outside Attacks.”

Jacob, D. (2017). A Quick Start To MPLS Fundamentals. Available:https://www.packetdesign.com/blog/quick-start-mpls-fundamentals/?cn-reloaded=1. Last ac-cessed 19th Feb 2019.

Lin, Chen. and W. Guowei (2010). Security research of VPN technology based on MPLS. Proceedings of the Third International Symposium on Computer Science and Computational Technology (ISCSCT’10), Citeseer.

Mende, D., Rey, E. and Schmidt, H. (2011). Practical Attacks against MPLS or Carrier Ethernet Networks [Online].ERNW Enno Rey Netzwerke GmbH. Available at: https://www.ernw.de/download/ERNW_MPLS-Carrier-Ethernet.pdf {Accessed: 18 Jan, 2016}

Mushtaq, U., *et al*. (2014). DiffServ-Aware Multi Protocol Label Switching Based Quality of Service in Next Generation Networks. 2014 IEEE International Advance Computing Conference (IACC)

Palmieri, F and Fiore, U. (2007). ‘Enhanced Security Strategies for MPLS Signaling’, Vol 2, No.5.

Paul C, (2014). Hijacking Label Switched Networks in the Cloud

Pepelnjak, I. and J. Guichard (2002). MPLS and VPN architectures, Cisco press.

Saad, T., Alawieh, B., Mouftah, H.T. and Gulder, S., 2006. Tunneling techniques for end-to-end VPNs: generic deployment in an optical testbed environment. IEEE Communications Magazine, 44(5), pp.124-132.

Upul Jayasinghe, Sergio Barreto, Miroslav Popovic, Teklemariam T. Tesfay, Jean-Yves Le Boudec (2014), Security Vulnerabilities of the Cisco IOS Implementation of the MPLS Transport Profile. SEGS’14, Scottsdale, Arizona, USA.