MPLS Security: Acute Protection of MPLS Networks from Outside Attacks

Israr-Ul-Maqbool, K.Venkatesh

Abstract— **Multi-Protocol Label switching is the Evolving technique which is used in providing high speed networking and traffic engineering efficiently in the networks. This technology is very potent than the IP routing as it uses the Label switching technique. Label assignment is critical for the accurate delivery of data sent by the user. However the Protocols for label distribution are not secure. Thus, if an intruder compromises a node by intercepting and modifying, or more simply injecting false labels into the LIB were the labels are stored, the propagation of improperly labelled data flows could create instability in the entire network.**

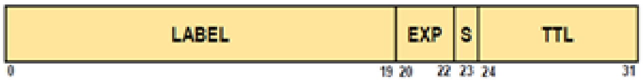
This paper gives an overview about the MPLS Security. The Security in MPLS networks depends on how to protect the data confidentiality, data integrity, and data availability. Since MPLS uses a Label Distribution protocol (LDP) and the path which the labels follow are the label switched paths. Therefore in order to protect the confidentiality, integrity and the availability of the labels. The cryptographic protocols and Ip sec tunnelling can be used to achieve it. A trust model is developed which tells us were to implement the security features and how to make control plane from were label comes secure.

***Index Terms*— Multi-Protocol Label, Label Distribution protocol (LDP), label comes secure.**

I. INTRODUCTION

Multi-Protocol Label Switching (MPLS) is a multiservice internet technology based on forwarding the packets using a specific packet label switching technique. Traffic entering an MPLS network is tagged with labels. A label is a short, four-byte, fixed-length, locally-significant identifier which is used to identify a Forwarding Equivalence Class (FEC). The label which is put on a particular packet represents the FEC to which that packet is assigned. The Mpls label format is shown as under:

Figure1



MPLS uses 32 bit field that contains the following information:

20-bit label: The actual label.

3-bit experimental field: It is used to define a class of service (i.e. IP precedence).

Bottom-of-stack bit: MPLS allows multiple labels to be inserted; this bit is used to determine if this is the last label in the packet

8-bit time-to-live (TTL) field: It has the same purpose as the TTL field in the IP header.

II. MPLS ARCHITECTURE

MPLS has two major components which are present in the edge and core routers based on these planes every function happens in MPLS networks. • **Control plane—** The control plane does following three functions:

Routing protocol: Responsible for exchange of routing information .It prepares IP routing table.

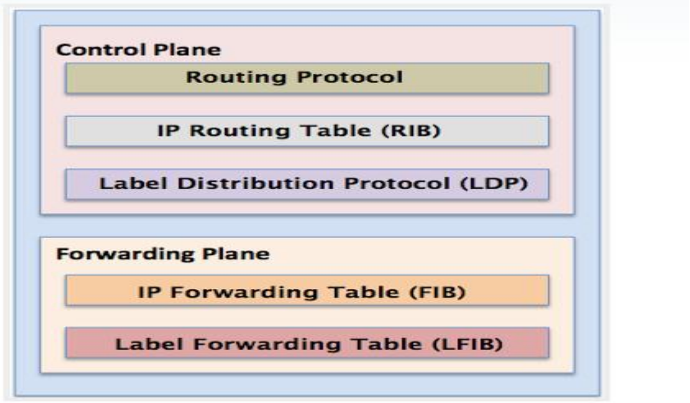
IP routing table: Responsible to build IP forwarding table (FIB) in Data Plane (Forwarding plane).

LDP: Responsible for exchange of labels between the peers. After exchanging the labels with LDP peer LFIB is formed in Data Plane (Forwarding Plane).

• **Data plane—**The data plane does following three functions:

1. As the IP packet comes in it will do IP routing lookup and check is any label is associated with particular FEC. If yes then label is imposed in the packet and process by LFIB as labelled packet.
2. If no label is associated with IP Packet then it is processed as normal IP Packet by FIB.
3. If incoming packet is labelled then by using LFIB the label is swapped and the packet is processed

Figure 2


Control Plane
Routing Protocol
IP Routing Table (RIB)
Label Distribution Protocol (LDP)
Forwarding Plane
IP Forwarding Table (FIB)
Label Forwarding Table (LFIB)

III. HOW MPLS WORKS

The figure 3 illustrates the working of the Packets in case of the MPLS Network.

Figure 3 MPLS Infrastructure

Manuscript received March 16, 2015.

Israr-Ul-Maqbool, M-Tech (ISCF), Department of Information Technology, SRM University

K.Venkatesh, Assistant Professor (Sr.G), Department of Information Technology, SRM University

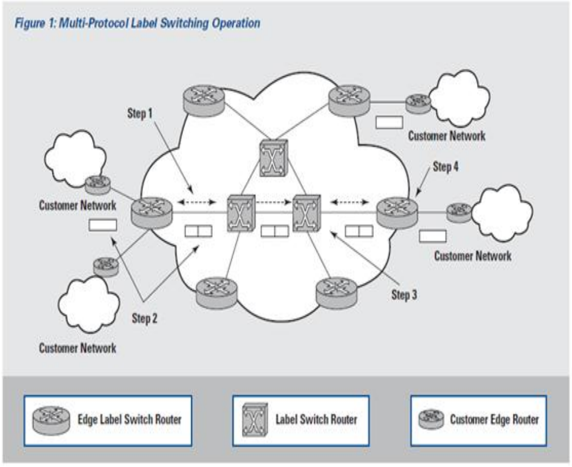


Figure 1: Multi-Protocol Label Switching Operation

In MPLS network the decision made to route the packet will take place at a point the packet enters the core Network. The Router which is the Label Edge Router (LER) also called ingress router makes a decision of path by looking into its Label information base (LIB) table and decides the path which packet should take in the network in order to reach to its destination the packet can go through core MPLS Routers were Label swapping takes place and the packet is sent through another Label Edge Router (LER) also called the egress router to reach to its destination. All the packets that share the same path are said to be in the same Forward Equivalence Class (FEC). The forwarding decision is based on the destination ip to which the packet needs to be send and the packet can travel along the Label Switched paths (LSP) in order to reach to the destination. The path followed by the label is decided by the (LER) that sends the packet along the (LSP) which helps the packet to reach to the final destination. A packet enters the ingress Edge Label Switching Router (LSR) where it is processed to determine which Layer 3 services it requires, such as Quality of Service (QoS) and bandwidth management. Based on routing and policy requirements, the Edge LSR selects and applies a label to the packet header and forwards the packet.

The LSR in the core reads the label on each packet, replaces it with a new one as listed in the table and forwards the packet. This action is repeated at all core and distribution "hops." The Egress Edge LSR strips the label, reads the packet header and forwards it to its final destination. A set of devices which engage in MPLS forwarding interaction is known as MPLS domain.

An important type of protocol which is used in the MPLS Networks is the Label Distribution Protocol (LDP).This is used to communicate the Labels associated with different FEC to other LSR within the MPLS infrastructure.

Despite the massive growth of MPLS networks, very little research has focused on the security aspects of core protocols such as the Label Distribution Protocol (LDP). LDP is the primary mechanism for transforming IP routes into high-speed "autobahns" within the MPLS paradigm. Weaknesses in LDP can be exploited by an attacker to achieve a wide range of strategic effects, including disrupting voice, global data and emergency communications.

Label Distribution Protocol

LDP is designed to distribute information about available routes within an MPLS network. The edge routers begin the process by distributing label information about their external adjacent network.

IV. LDP MESSAGES

Four message classes in LDP are used to facilitate session management and label distribution (i) Discovery messages that establish network adjacencies

(ii) Session messages that initialize and maintain LDP connections

(iii)Advertise messages that establish and remove LSP

(iv)Notification messages that specify advisories and errors.

Discovery Class Messages

Hello: Hello messages are exchanged among LSRs during the discovery process using UDP. There are two types of messages: (i) Link Hello messages and (ii) Extended Hello messages. Link Hello messages are sent between directly-linked LSRs by addressing the messages to the subnet broadcast address. Extended Hello messages are exchanged between no directly-linked LSRs by addressing the messages directly to peers.

Initialization: Once an adjacency is discovered, the LSR peers establish a TCP connection. Initialization messages are then used to exchange session parameters (e.g., retention mode or label distribution mode) between the LSRs.

Keep Alive: Keep Alive messages facilitate the detection of network errors. LSR periodically transmit these messages to indicate that a link is still working. An error condition is assumed to have occurred when an LSR does not receive a message from a peer within an allotted timeout period, this results in the termination of the established session and the removal of associated labels.

Address: Address messages provide neighbouring LSRs with mapping Information about LSR IDs to interface IP addresses. This information is used to identify the label mappings that correspond to the least cost path.

Label Mapping: Label Mapping messages are used to distribute FEC to label bindings from a downstream LSR to an upstream peer. This

message is the primary mechanism for constructing LSP.

Label Release: Label Release messages notify downstream peers that an LSR has removed a particular label mapping. An LSR may remove bindings, for example, when an IP table changes or a Label withdraw message is received.

Notification Class Messages

Notification: Notification messages convey errors and advisories among peer LSRs. If the message indicates a fatal error, the sending and receiving LSRs terminate the LDP session and remove all associated label bindings.

LDP Vulnerabilities

In general, attacks may exploit weaknesses in:

(i)The LDP specification

(ii)Service provider implementations

(iii) Underlying infrastructure attacks on the LDP specification leverage inherent weaknesses in the design of the protocol. Any network that conforms to the protocol standard is susceptible to this class of attacks.

Attacks on service provider implementations exploit configuration errors or code flaws. LDP includes several undefined and reserved fields that can be exploited in attacks. LDP also uses a nested structure of Type-Length-Value fields, which offers numerous opportunities for buffer overflow attacks.

Our analysis does not focus on implementation vulnerabilities; nevertheless, we note that all implementations should undergo extensive fuzz testing. Attacks on the underlying infrastructure exploit vulnerabilities in information technology and network assets or weak security policies. For example, LDP relies on IP to provide session communication and routing information. An attack on the underlying IP protocols may be used to reroute a target LSP or hijack a session. Because these attacks do not explicitly exploit LDP messages, they are not considered in this paper.

Our analysis focuses primarily on how an attacker can use LDP messages to exploit MPLS networks. Given only link access, we discuss several vulnerabilities in the LDP specification that could enable an attacker to deny service to various network assets or to reroute traffic.

Threat Model

A compromised LSR can be used to do the following:

1. Establish unauthorized label switched paths (LSPs). An LSP that advertises connectivity to an IP subnet can be re-routed in manner that allows examination of traffic.

2. Advertise false routing information or LSP/label mappings. Not only does this facilitate re-routing, but it also corrupts correct routing of LSPs, resulting in

Denial of service. Also important is a consideration of what is not in the threat model.

Where are the Security Issues

Devices Outside the core

Label Information Disclosure

The segregation of traffic within an MPLS is based on labels attached to the data packets. If the correct labels are known, the labels can be attached to the data packets before they are sent before they are sent potentially allowing for two attack scenarios Rogue path switching and Rogue Destination Switching.

V. Rogue Path Switching

If traffic follows a path it was not intended to then this path is called a "rogue path". If attackers outside the MPLS core find a way about the label information for the rogue path, attaching those labels could help attackers to predetermine the path of traffic towards that rogue path.

Rogue Destination Switching

If a traffic reaches a destination host which it was not intended to then this destination is called the "rogue destination". If attackers outside the MPLS core find a way about the label information for the rogue destination, attaching those labels could help attackers to predetermine the path of traffic towards that rogue destination.

Enumeration of Labels

If an MPLS device accepts packets from outside the core the attacker could be able to enumerate the labels, potentially allowing for two attacking scenarios (i) Enumeration of label paths (ii) Enumeration of target

(i) Enumeration of Label Paths

If a target's Ip address was known Knowledge of the label for LSP to reach is desired, a fixed Ip address could be used for the packets sent
then the label incremented until the reply from the target was received. The reply could be then decoded to retrieve the preserved label switching information.

(ii) Enumeration of Targets

It must be desirable to locate certain type of target on an MPLS network, for example web servers. Here we can set the TCP Port no to 80 and increment the target IP address over time.

Label Information Base Poisoning

Label distribution protocols are generally not authenticated. This means that if an MPLS device accepts LDP information from outside it is possible for an attacker to manipulate the label information base of one or more MPLS devices leading to the two attack scenarios on MPLS devices (i)Denial of Service (ii) Malicious Collaborator

Denial of Service

The Label information base could be manipulated in such a way which causes Denial of Service conditions. An example for this would be to redirect traffic with real time requirement into congested paths, effectively rendering such service useless.

Malicious Collaborator

If an attacker can poison the LIB of MPLS domain a device under their control might be established a member of that domain. Taking advantage of this situation, the attacker might change the LIB to have interesting traffic forwarded to a specific device where this traffic can be captured and stored for later perusal before forwarding it back into the MPLS infrastructure.

Unauthorised Access to the LER

If the network device which provides access to the MPLS network for the customer has been hardened with respect to security then the unauthorised access can be gained which could provide details of connectivity to the core infrastructure.

Devices inside the core

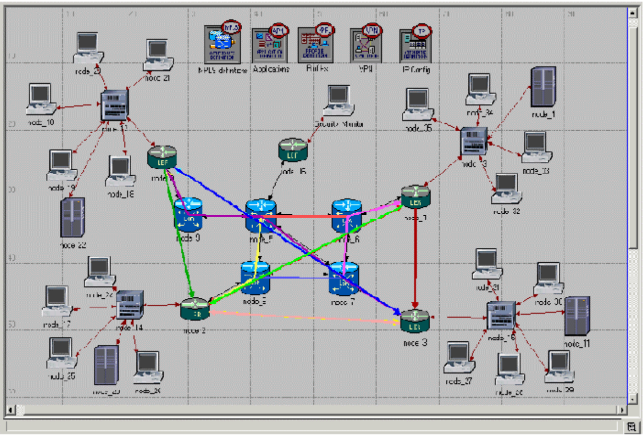
An attacker might be able to physically compromise the infrastructure and place a device on inside of the core but without the ability to modify the MPLS devices themselves. An example of this will be connecting a laptop to the span port to intercept the traffic passing through the device.

If attacker can get access inside the core of the MPLS device he can spoof the packet can send the packet to the desired destination and can get the information which he requires.

Security Approach

The overall security approach utilizes a link-by-link analysis of signalling information. It starts with the first PATH message generated from the Ingress router and ends when the Ingress router receives the final RESV message. Any message objects that are deleted, changed, or manipulated are detected and reported at the security monitor. Security monitor approach to LSP control plane tamper detection is dependent on hardening all Ingress and Egress routers associated with MPLS path setup. Along with hardening the edge devices IPsec tunnels are created from each LER and LSR device to the distant Monitor. This protects the reported signalling information from compromise.

Figure 4



Here in this MPLS network scenario, which is the first level in the OPNET program. Nodes are placed and are connected to each other to form a network. There are several workstations, servers, switches, and routers, each connected with either a red or black line. These lines represent either a 100 Base T Ethernet connection (red), or a T1 or T3 connection (black). Workstations look like workstations, while servers are the gray rectangles, switches are the gray squares, and the MPLS routers are the blue and green cylinders. The other lines that can be seen in various colors represent Label Switch Paths. To add to the assurance that reported information to the monitor has not been tampered with encryption in the form of IPsec tunnels are also included in the overall security architecture.

VI. Conclusion

As in the case of traditional networks, most security mechanisms are applied at the perimeter of MPLS networks. However, many of the attacks discussed above occur from within administrative domains. Therefore, it is essential to apply security mechanisms that protect the internal operations of MPLS networks. Many vulnerabilities in LDP stem from the lack of authentication, integrity and confidentiality mechanisms. LDP messages are sent in the clear, which enables an attacker to gather valuable network information, identify important targets and perform insidious attacks. Without integrity or authentication checks, LSRs are unable to discern the source of a message or verify that a message has not been modified or replayed. Adequate authentication and integrity mechanisms like implementing cryptographic protocols or implementing ipsec tunnelling between LER and LSR would mitigate the majority of attacks discussed above. However, implementing these mechanisms requires significant effort. An attack on MPLS networks could prove to be harmful for organisations using therefore proper security mechanisms are required to protect it.

References

[1]. Thorsten Fisher “Multiprotocol label Switching Security Overview" An IRM White Research Paper.

[2]. S. Alouneh, A. En-Nouaary, and A. Agarwal: MPLS security: an approach for unicast and multicast environments.

[3]. L. Anderson, P. Doolan, N. Feldman, A. Fredette and B. Thomas, LDP Specification, RFC 3036, 2001.

[4]. Ravi Sinha MPLS - VPN Services and Security May 29 2003

[5]. Daniel Guernsey, Aaron Engel, Jonathan Butts and Sujeet Shenoi Security Analysis of The MPLS Label Distribution Protocol.

[6]. E. Rosen et al., “Multiprotocol Label Switching Architecture,” IETF RFC-3031.

[7]. L. Ghein, MPLS Fundamentals, Cisco Press, Indianapolis, Indiana, 2007.

[8]. J. Chung, “Multiple LSP Routing Network Security for MPLS Networking,” IEEE-MWSCAS, 2002.

[9]. D. Barlow, V. Vassilio, H. Owen, “A cryptographic protocol to protect MPLS Labels”, Proceeding of IEEE Workshop of Information Assurance, 2003.

[10]. D.Awduche “Requirements for Traffic Engineering over MPLS”, IETF, RFC 2702