Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: January 14, 2013

L. Fang, Ed.
Cisco Systems
B. Niven-Jenkins, Ed.
Velocix
S. Mansfield, Ed.
Ericsson
R. Graveman, Ed.
RFG Security

July 14, 2012

MPLS-TP Security Framework
draft-ietf-mpls-tp-security-framework-04

Abstract

This document provides a security framework for Multiprotocol Label Switching Transport Profile (MPLS-TP). MPLS-TP extends MPLS technologies and introduces new OAM capabilities, a transport-oriented path protection mechanism, and strong emphasis on static provisioning supported by network management systems. This document addresses the security aspects relevant in the context of MPLS-TP specifically. It describes potential security threats, security requirements for MPLS-TP, and mitigation procedures for MPLS-TP networks and MPLS-TP interconnection to other MPLS and GMPLS networks.

This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunication Union Telecommunication Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionalities of a packet transport network.

This Informational Internet-Draft is aimed at achieving IETF Consensus before publication as an RFC and will be subject to an IETF Last Call.

[RFC Editor, please remove this note before publication as an RFC and insert the correct Streams Boilerplate to indicate that the published RFC has IETF Consensus.]

Status of this Memo

This Internet-Draft will expire on January 15, 2013.

Copyright Notice

Table of Contents

1. Introduction

1.1. Background and Motivation

This document provides a security framework for Multiprotocol Label Switching Transport Profile (MPLS-TP).

The MPLS-TP Requirements and MPLS-TP Framework are defined in [RFC5654] and [RFC5921], respectively. The intent of MPLS-TP development is to address the needs for transport evolution and the fast-growing bandwidth demand accelerated by new packet-based services and multimedia applications, from Ethernet Services, Layer 2 and Layer 3 VPNs, and triple play to Mobile Access Network (RAN) backhaul, etc. MPLS-TP is based on MPLS technologies to take advantage of this technology's maturity, and maintaining the transport characteristics of MPLS is an MPLS-TP requirement.

To focus on meeting transport requirements, MPLS-TP uses a subset of MPLS features and introduces extensions to reflect the characteristics of the transport technology. The added functionalities include in-band OAM, transport-oriented path protection and recovery mechanisms, etc. There is strong emphasis on static provisioning supported by network management systems (NMS) or Operation Support Systems (OSS). MPLS-TP and MPSL without TP also need to interwork.

The security aspects of the extensions particularly designed for MPLS-TP need to be addressed. The security models, threats, requirements, and defense techniques previously defined in [RFC5920] can be applied to reuse existing functionality in MPLS and GMPLS but are not sufficient to cover the TP extensions.

This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunication Union Telecommunication Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionality of a packet transport network.

1.2. Scope

This document addresses the security aspects specific to MPLS-TP. It defines security models that apply to various MPLS-TP deployment scenarios, identifies potential security threats and mitigation procedures for MPLS-TP networks and MPLS-TP interconnection to GMPLS or MPLS networks without TP, and provides security requirements for MPLS-TP. Inter-AS and Inter-provider security for MPLS-TP to MPLS-TP connections or MPLS-TP to MPLS connections without TP are discussed, because these connections present higher security risks than connections for Intra-AS MPLS-TP.

The general security analysis and guidelines for MPLS and GMPLS are addressed in [RFC5920], and the content of [RFC5920] that has no new impact on MPLS-TP is not repeated in this document. Other general security issues regarding transport networks that are not specific to MPLS-TP are also found elsewhere. Readers may also refer to the "Security Best Practices Efforts and Documents" Opsec Effort [opsec-efforts] and "Security Mechanisms for the Internet" [RFC3631] (if there are linkages to the Internet in the applications) for general network operations security considerations. This document does not define the specific mechanisms or methods that must be implemented to satisfy the security requirements.

The issues and areas addressed with respect to MPLS-TP security are:

- Attacks against G-Ach integrity, availability, or confidentiality

- Misuse of G-Ach to attack data plane resources

- ID spoofing attacks

- Attacks against the loopback mechanism and Authentication TLV

- Attacks against the network management system (NMS)

- NMS and CP interaction vulnerabilities

- MIP and MEP assignment and attacks on these mechanisms

- Topology discovery vulnerabilities

- Data plane authentication (using G-Ach or by other means)

- Label authentication

- DoS attacks on the data plane

- Performance monitoring vulnerabilities

1.3. Requirement Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119]. Although this document is not a protocol specification, the use of this language clarifies the instructions to protocol designers producing solutions that satisfy the requirements set out in this document.

1.4. Terminology

This document uses MPLS, MPLS-TP, and security terminology. Detailed definitions and additional terminology for MPLS-TP may be found in [RFC5654] and [RFC5921]. MPLS/GMPLS security-related terminology can be found in [RFC5920].

- AC: Attachment Circuit

- BFD: Bidirectional Forwarding Detection

- CE: Customer-Edge device

- DoS: Denial of Service

- DDoS: Distributed Denial of Service

- GAL: Generic Alert Label

- G-ACh: Generic Associated Channel

- GMPLS: Generalized Multi-Protocol Label Switching

- LDP: Label Distribution Protocol

- LSP: Label Switched Path

- MCC: Management Communication Channel

- MEP: Maintenance End Point

- MIP: Maintenance Intermediate Point

- MPLS: MultiProtocol Label Switching

- OAM: Operations, Administration, and Management

- PE: Provider-Edge device

- PSN: Packet-Switched Network

- PW: Pseudowire

- RSVP: Resource Reservation Protocol

- RSVP-TE: Resource Reservation Protocol with Traffic Engineering Extensions

- S-PE: Switching Provider Edge

- SCC: Signaling Communication Channel

- SSH: Secure Shell

- TE: Traffic Engineering

- TLS: Transport Layer Security

- T-PE: Terminating Provider Edge

- VPN: Virtual Private Network

- WG: Working Group of IETF

- WSS: Web Services Security

1.5. Structure of the document

Section 1: Introduction

Section 2: MPLS-TP Security Reference Models

Section 3: Security Threats

Section 4: Security Requirements

Section 5: Defensive and mitigation techniques and procedures

2. Security Reference Models

This section defines reference models for security in MPLS-TP networks.

The models are built on the architecture of MPLS-TP defined in [RFC5921]. The Service Provider (SP) boundaries play an important role in determining the security models for any particular deployment.

This document defines a trusted zone as being where a single SP has total operational control over that part of the network. A primary concern is about security aspects that relate to breaches of security from the "outside" of a trusted zone to the "inside" of this zone.

2.1. Security Reference Model 1

In reference model 1, a single SP has total control of the PE/T-PE to PE/T-PE part of the MPLS-TP network.

Security reference model 1(a)

An MPLS-TP network with Single Segment Pseudowire (SS-PW) from PE to PE. The trusted zone is PE1 to PE2 as illustrated in MPLS-TP Security Model 1 (a) (Figure 1).

```
          |<-------------- Emulated Service ---------------->|
          |                                                  |
          |          |<------- Pseudo Wire ------>|          |
          |          |                            |          |
          |          |    |<-- PSN Tunnel -->|    |          |
          |          V    V                  V    V          |
          V    AC    +-----+                 +-----+    AC   V
    +-----+    |     | PE1|==================| PE2|     |    +-----+
    |     |----------|............PW1.............|----------|     |
    | CE1 |    |     |    |                  |    |     |    | CE2 |
    |     |----------|............PW2.............|----------|     |
    +-----+  ^ |     |    |==================|    |     | ^  +-----+
          ^  |       +-----+                 +-----+    | |  ^
          |  |   Provider Edge 1         Provider Edge 2  |  |
          |  |                                            |  |
    Customer |                                            | Customer
    Edge 1   |                                            | Edge 2
             |                                            |
       Native service                               Native service

   ----Untrusted--- >|<------- Trusted Zone ----->|<---Untrusted----
```

MPLS-TP Security Model 1 (a)

Figure 1

Security reference model 1(b)

An MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE to T-PE. The trusted zone is T-PE1 to T-PE2 in this model as illustrated in MPLS-TP Security Model 1 (b) (Figure 2).

```
            Native  |<------------Pseudowire----------->|  Native
            Service |        PSN             PSN        |  Service
             (AC)   |    |<-cloud->|     |<-cloud->|    |   (AC)
               |    V    V         V     V         V    V     |
               |    +----+         +----+          +----+     |
        +----+ |    |TPE1|=========|SPE1|==========|TPE2|     | +----+
        |    |------|.....PW.Seg't1......PW.Seg't3..... |-------|    |
        | CE1| |    |    |         |    |          |    |     | |CE2 |
        |    |------|.....PW.Seg't2......PW.Seg't4..... |-------|    |
        +----+ |    |    |=========|    |==========|    |     | +----+
             ^      +----+    ^    +----+     ^    +----+       ^
             |                |               |                 |
             |              TP LSP            TP LSP            |
             |                                                  |
             |<---------------- Emulated Service -------------->|

    -- Untrusted-->|<---------- Trusted Zone ---------->|<--Untrusted--
```

MPLS-TP Security Model 1 (b)

Figure 2

2.2. Security Reference Model 2

In reference model 2, a single SP does not have total control of the PE/T-PE to PE/T-PE part of the MPLS-TP network. S-PE and T-PE may be under the control of different SPs, or their customers or may not be trusted for some other reason. The MPLS-TP network is not contained within a single trusted zone.

Security Reference Model 2(a)

An MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE to T-PE. The trusted zone is T-PE1 to S-PE, as illustrated in MPLS-TP Security Model 2 (a) (Figure 3).

```
            Native  |<------------Pseudowire----------->|  Native
            Service |         PSN              PSN      |  Service
             (AC)   |    |<cloud->|     |<-cloud-->|    |   (AC)
               |    V    V        V     V          V    V     |
               |    +----+         +----+          +----+     |
        +----+ |    |TPE1|=========|SPE1|==========|TPE2|     | +----+
        |    |------|.....PW.Seg't1......PW.Seg't3..... |-------|    |
        | CE1| |    |    |         |    |          |    |     | |CE2 |
        |    |------|.....PW.Seg't2......PW.Seg't4..... |-------|    |
        +----+ |    |    |=========|    |==========|    |     | +----+
             ^      +----+    ^    +----+     ^    +----+       ^
             |                |               |                 |
             |              TP LSP            TP LSP            |
             |                                                  |
             |<---------------- Emulated Service -------------->|

    -- Untrusted-->|<-- Trusted Zone -->|<---------Untrusted--------
```

MPLS-TP Security Model 2 (a)

Figure 3

Security Reference Model 2(b)

An MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from T-PE to T-PE. The trusted zone is the S-PE, as illustrated in MPLS-TP Security Model 2 (b) (Figure 4).

```
            Native  |<------------Pseudowire-------------->|  Native
            Service |         PSN              PSN         |  Service
             (AC)   |    |<cloud->|     |<-cloud-->|    |   (AC)
               |    V    V        V     V          V    V     |
               |    +----+         +----+          +----+     |
        +----+ |    |TPE1|=========|SPE1|==========|TPE2|     | +----+
        |    |------|.....PW.Seg't1......PW.Seg't3.... .|-------|    |
        | CE1| |    |    |         |    |          |    |     | |CE2 |
        |    |------|.....PW.Seg't2......PW.Seg't4..... |-------|    |
        +----+ |    |    |=========|    |==========|    |     | +----+
             ^      +----+    ^    +----+     ^    +----+       ^
             |                |               |                 |
             |              TP LSP            TP LSP            |
             |                                                  |
             |<---------------- Emulated Service -------------->|

    --------Untrusted------------>|<--->|< ------Untrusted--------
                                  Trusted
                                    Zone
```

MPLS-TP Security Model 2 (b)

Figure 4

Security Reference Model 2(c)

An MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from different Service Providers with inter-provider PW connections. The trusted zone is T-PE1 to S-PE3, as illustrated in MPLS-TP Security Model 2 (c) (Figure 5).

```
   Native  |<-------------------- PW15 --------------------->| Native
    Layer  |                                                 |  Layer
  Service  |    |<-PSN13->|    |<-PSN3X->|    |<-PSNXZ->|    | Service
     (AC1) V    V   LSP   V    V   LSP   V    V   LSP   V    V  (AC2)
           +----+   +-+   +----+         +----+   +-+   +----+
  +---+    |TPE1|   | |   |SPE3|         |SPEX|   | |   |TPEZ|   +---+
  |   |    |    |=========|    |=========|    |=========|    |   |   |
  |CE1|----|........PW1........|...PW3...|........PW5........|---|CE2|
  |   |    |    |=========|    |=========|    |=========|    |   |   |
  +---+    | 1  |   |2|   | 3  |         | X  |   |Y|   | Z  |   +---+
           +----+   +-+   +----+         +----+   +-+   +----+

           |<- Subnetwork 123->|         |<- Subnetwork XYZ->|

Untrusted->|<- Trusted Zone - >|<-------------Untrusted---------------
```

MPLS-TP Security Model 2 (c)

Figure 5

2.3. Security Reference Model 3

An MPLS-TP network with a Transport LSP from PE1 to PE2. The trusted zone is PE1 to PE2 as illustrated in MPLS-TP Security Model 3 (a) (Figure 6), where the two PEs and the devices in between them are under control of a single service operator.

```
            |<------------- Client Network Layer --------------->|
            |                                                    |
            |          |<----------- Packet --------->|          |
            |          |         Transport Service    |          |
            |          |                              |          |
            |          |                              |          |
            |          |          Transport           |          |
            |          |    |<------ LSP ------->|    |          |
            |          V    V                    V    V          |
            V    AC    +----+      +-----+       +----+     AC   V
      +-----+    |     | PE1|=======\   /========| PE2|     |    +-----+
      |     |----------|..Svc LSP1.| \ / |............|----------|     |
      | CE1 |    |     |    |      |  X  |       |    |     |    | CE2 |
      |     |----------|..Svc LSP2.| / \ |............|----------|     |
      +-----+  ^ |     |    |=======/   \========|    |     | ^  +-----+
            ^  |       +----+  ^   +-----+       +----+     | |  ^
            |  |      Provider |       ^         Provider     |  |
            |  |       Edge 1  |       |          Edge 2      |  |
      Customer |               |    P Router                  | Customer
       Edge 1  |             TE LSP                           |  Edge 2
               |                                              |
               |                                              |
         Native service                                 Native service

   -----Untrusted---- >|< ------ Trusted Zone ------ >|<---Untrusted----
```

MPLS-TP Security Model 3 (a)

Figure 6

2.4. Trusted-Zone Boundaries

The boundaries of a trusted zone should be carefully defined when analyzing the security properties of each individual network. As illustrated above, the security boundaries determine which reference model should be applied to analyze use cases.

A key requirement of MPLS-TP networks is that the security of a trusted zone MUST NOT be compromised by interconnecting one SP's MPLS-TP or MPLS infrastructure with another SP's core devices, T-PE devices, or end users.

In addition, neighboring nodes in the network may be trusted or untrusted. Neighbors may also be authorized or unauthorized. Even though a neighbor may be authorized for communication, it may not be trusted. For example, when connecting with another provider's S-PE to set up Inter-AS LSPs, the other provider is considered to be untrusted but may be authorized for communication.

```
                +---------------+        +----------------+
                |               |        |                |
                |    MPLS-TP   S-PE1----S-PE3  MPLS-TP    |
        CE1--T-PE1   Network    |        |     Network  T-PE2--CE2
                |    Provider  S-PE2----S-PE4 Provider   |
                |       A       |        |        B       |
                +---------------+        +----------------+

           For Provider A:
                   Trusted Zone: Provider A MPLS-TP network
                   Trusted neighbors: T-PE1, S-PE1, S-PE2
                   Authorized but untrusted neighbor: Provider B
                   Unauthorized and untrusted neighbors: CE2
```

MPLS-TP trusted zone and authorized neighbor

Figure 7

3. Security Threats

This section lists various network security threats that may endanger MPLS-TP networks. It emphasizes threats that are new to MPLS-TP networks or affect MPLS-TP networks in new ways.

A successful attack on a particular MPLS-TP network or on a SP's MPLS-TP infrastructure may cause one or more of the following adverse effects:

1. Observation (including traffic pattern analysis), modification, or deletion of a provider's or user's data, as well as replay or insertion of inauthentic data into a provider's or user's data stream. These types of attacks apply to MPLS-TP traffic regardless of how the LSP or PW is set up in a similar way to how they apply to MPLS traffic regardless how the LSP is set up.

2. Compromised GAL label or BFD messaging:

   a. GAL label or BFD label manipulation, which includes insertion of false labels or messages and modification, deletion, or replay of GAL labels or messages.

   b. DoS attack through in-band OAM G-ACh/GAL and BFD messages.

   c. Attacks via G-ACh to cause protection switchover, restoration, or locking of a transport connection.

3. Disruption of a provider's or user's connectivity, or degradation of a provider's service quality.

a. Attacks against a SP's connectivity:

+ In the case in which an NMS is used for LSP setup, the attacks occur through attacks on the NMS.

+ In the case in which dynamic provisioning is used, the attacks occur on the dynamic control plane. Most aspects of these are addressed in [RFC5920].

b. Attacks against user's connectivity. These are similar to PE/CE attacks against access in typical MPLS networks and are addressed in [RFC5920].

4. Probes of a provider's network to determine its configuration, capacity, or usage. These can occur through attacks against an NMS in the case of static provisioning or attacks against the control plane in dynamic MPLS-TP networks. They can also result from combined attacks.

It is helpful to consider that threats, whether resulting from malicious behavior or accidental errors, may come from different sources or categories of attackers. For example, they may come from:

o Users of the MPLS-TP network itself, who may attack the network or other users. These other users' services may be provided by the same or a different MPLS-TP core.

o The MPLS-TP SP or its employees.

o Other persons who obtain physical access to a MPLS-TP SP's site.

o Other persons who use social engineering to influence the behavior of a SP's personnel.

o Outsiders, e.g., attackers from the other sources, including the Internet (if connectivity can be obtained).

o Other SPs in the case of MPLS-TP inter-provider connection. The other provider may or may not be using MPLS-TP.

o Those who create, deliver, install, and maintain hardware or software for network equipment.

Security is a tradeoff between cost and risk, so it is useful to consider the likelihood of different attacks, the cost of preventing them, and the possible damage resulting from their occurrence. There is at least a perceived difference in the likelihood of most types of attacks being successfully mounted in different environments, such as:

- An MPLS-TP network inter-connected with another provider's core

- An MPLS-TP configuration inter-connected with the public Internet, e.g., for control or management functions

Most types of attacks become easier to mount and hence more likely as the shared infrastructure via which service is provided expands from a single SP to multiple cooperating SPs to the global Internet. Attacks that may not be of sufficient likeliness to warrant concern in a closely controlled environment often merit defensive measures in broader, more open environments. Even though surveys show that 40% to 60% of attacks originate from insiders, in closed communities, it is often practical to identify and to deal with misbehavior after the fact: employee misbehavoir can be corrected, for example.

The following sections list specific types of exploits that threaten MPLS-TP networks.

3.1. Attacks on the Control Plane

This category includes attacks that may compromise the availability of control plane capabilities, the integrity of these operations, and, potentially, the confidentiality of these operations for either in-band (G-ACh) or out-of-band (GMPLS) configurations. Attacks against GMPLS include attacks against its constituent protocols (i.e., RSVP-TE, LDP, OSPFv2, or PCEP). Attacks against G-ACh may be directed against the label mechanism (GAL) or any of the encapsulated signaling or management protocols (SCC, MCC, OAM, or protection). The following attacks may target the provisioning, management, or survivability functions of the control plane:

- Improper MPLS-TP LSP or PW creation or deletion. This may result from a failure of control plane authentication or authorization mechanisms or compromise of control plane traffic. One result might be improper cross-connection of different users' traffic.

- Improper use of MPLS-TP protection and restoration capabilities. This also may result from a failure of control plane authentication or authorization mechanisms or compromise of control plane traffic.

- Unauthorized observation of control plane traffic, which includes information about a SP's MPLS-TP configuration, equipment, or users.

- Denial of service attacks on the control plane or use of the control plane to carry out denial of service attacks against the data plane.

- Attacks on the SP's MPLS-TP equipment or software. These may occur during the normal lifecycle of the equipment and software or via management interfaces or other points of entry. These include social engineering attacks on the SP's infrastructure.

3.2. Attacks on the Data Plane

The general MPLS data plane attacks apply to MPLS-TP as well. These include the following:

- Denial of service, misconnection, loss of bandwidth, or other service disruptions.

- Unauthorized observation of data traffic, including LSP or PW message interception and traffic pattern analysis.

- Modification or deletion of data traffic, which may include insertion of inauthentic data traffic (spoofing or replay).

MPLS-TP supports data plane switching (e.g., from working to protect-path when a failure is detected) without the involvement of control plane or management system. Therefore, data plane attacks can potentially cause serious network instability.

4. Security Requirements for MPLS-TP

This section covers requirements for securing an MPLS-TP network infrastructure. The MPLS-TP network can be operated without a control plane or via dynamic control plane protocols. The security requirements related to MPLS-TP OAM, recovery mechanisms, MPLS-TP interconnection with other technologies, and operations specific to MPLS-TP are addressed in this section.

A service provider may deploy the security options best fitting its network operations. This document does not mandate that MPLS-TP network operators must configure and use technical mechanisms to satisfy all of the security requirements listed in this document.

These requirements are focused on: 1) how to protect the MPLS-TP network from various attacks originating outside the trusted zone, including those from network users, both accidental and malicious; 2) prevention of operational errors resulting from misconfiguration within the trusted zone.

R01: MPLS-TP MUST support the physical and logical separation of the data plane from the control plane and the management plane. That is, if the control plane, management plane, or both are attacked and cannot function normally, the data plane should continue to forward packets without being impacted.

R02: MPLS-TP MUST support static provisioning of MPLS-TP LSPs and PWs without using control protocols (with or without a NMS). This is particularly important in cases where components of the provisioning process are not in the trusted zone (security model 2(a) and security model 2(b), where some or all T-PEs are not in the trusted zone and the inter-provider cases in security model 2(c), where the connecting S-PE is not in the trusted zone; see Figures 3, 4, and 5).

R03: MPLS-TP MUST support the IP loopback and non-IP path options that use the path ID compatible with ITU-T transport-based operations.

R04: MPLS-TP MUST support authentication, integrity, and replay protection for any control protocol used in an MPLS-TP network.

R05: MPLS-TP SHOULD support confidentiality, algorithm agility, and key management for any control protocol used in an MPLS-TP network.

R06: MPLS-TP MUST support authentication, integrity, and replay protection for dynamic MPLS network inter-connection protocols.

R07: MPLS-TP SHOULD support confidentiality, algorithm agility, and key management for dynamic MPLS network inter-connection protocols.

R08: MPLS-TP MUST support mechanisms to mitigate denial of service (DoS) attacks carried out over any control plane protocol or management protocol, including OAM and G-ACh, whether in-band or out-of band. This applies to denial-of-service attacks against the control or management protocol itself or against the data channel.

R09: MPLS-TP MUST provide secure ways to support Service Providers' requirements for hiding their infrastructure in all reference models using static configuration or a dynamic control plane, help to reduce risk of SP networks be attacked, (e.g. DoS attack).

R10: MPLS-TP SHOULD provide protection from operational errors. The extensive use of static provisioning with or without a NMS increases the likelihood of operational errors that result in misconfigurations that may compromise user's data, system security, or network security is greater.

R11: MPLS-TP MUST support event logging and auditing. Logging and auditing capabilities provide critical resources for tracking down problems and repairing the damage after a security incident.

Management security requirements are covered in [RFC5951]. This document mandates protocol security, access controls, and protection against denial of service attacks for all management protocols. [RFC3871] contains guidelines on appropriately strong and open cryptography.

R12: MPLS-TP MUST support authentication, integrity, and replay protection for the management communication channel (MCC) and all network traffic and protocols used to support management functions. This includes protocols used for configuration, monitoring, Configuration backup, logging, time synchronization, authentication, and routing.

R13: MPLS-TP SHOULD support confidentiality, algorithm agility, and key management for the management communication channel (MCC) and all network traffic and protocols used to support management functions. This includes protocols used for configuration, monitoring, Configuration backup, logging, time synchronization, authentication, and routing.

R14: The MCC MUST support access controls by protocol and port number.

5. Defensive Techniques for MPLS-TP Networks

The defensive techniques presented in this document are intended to describe methods by which some security threats can be addressed. They are not intended as requirements for all MPLS-TP deployments. The specific operational environment determines the security requirements for any instance of MPLS-TP. Therefore, protocol designers should provide a full set of security capabilities, which can be selected and used where appropriate. The MPLS-TP provider should determine the applicability of these techniques to the provider's specific service offerings, and the end user may wish to assess the value of these techniques to the user's service requirements.

The techniques discussed here include entity authentication for identity verification, encryption for confidentiality, message integrity and replay detection to ensure the validity of message streams, network-based access controls such as packet filtering and firewalls, host-based access controls, isolation, aggregation, protection against denial of service, and event logging. Where these techniques apply to MPLS and GMPLS in general, they are described in Section 5.2 of [RFC5920]. The remainder of this section covers aspects that apply particularly to MPLS-TP.

5.1. Authentication

To prevent security issues arising from impersonation, masquerade, some denial-of-service attacks, or from malicious or accidental misconfiguration, it is critical that MPLS-TP devices should accept connections or control messages only from known sources. Authentication refers to methods for ensuring that the identities of message sources are properly verified by the devices with which they communicate. This section focuses on scenarios in which sender authentication is required and recommends authentication mechanisms for these scenarios.

5.1.1. Management System Authentication

Management system authentication includes the authentication of a PE to a centrally-managed network management or directory server when directory-based auto-discovery is used. It also includes authentication of a CE to the configuration server when a configuration server system is used. This type of authentication should be bi-directional. The PE or CE needs to be certain it is communicating with the right server.

5.1.2. Peer-to-Peer Authentication

Peer-to-peer authentication includes peer authentication for network control protocols and other peer authentication (e.g., authentication of one IPsec security gateway by another).

Authentication should be bi-directional, including S-PE, T-PE, PE, or CE to authentication to a configuration server so that a PE or CE can be certain it is communicating with the right server.

5.1.3. Cryptographic Techniques for Authenticating Identity

Cryptographic techniques offer several mechanisms for authenticating the identity of devices or individuals. These include the use of shared secret keys, one-time keys generated by accessory devices or software, user-ID and password pairs, and a variety of public-private key systems. Some of these use digital certificates binding a user's name and public key. One method of using digital certificates is within a hierarchical Certification Authority system.

5.2. Access Control Techniques

Many of the security issues related to management interfaces can be addressed through the use of authentication as described in Section 5.1. **However, additional security may be provided by controlling access** to management interfaces or to specific resources with an access control model. In addition to identification and authentication, access control deals with authorization.

SNMP security efforts have focused on access control models. For the Most recent version of SNMP security, see the work of the ISMS WG.

The Optical Internetworking Forum has worked on protecting interfaces to management systems with TLS, SSH, IPsec, WSS, etc. See Security for Management Interfaces to Network Elements [OIF-SMI-03.0].

Management interfaces, especially console ports on MPLS-TP devices, may be configured so they are only accessible out-of-band, through a system which is physically or logically separated from the rest of the MPLS-TP infrastructure.

Where management interfaces are accessible in-band within the MPLS-TP domain, filtering or firewalling techniques can be used to restrict unauthorized in-band traffic from having access to management interfaces. Depending on device capabilities, these filtering or firewalling techniques can be configured either on other devices through which the traffic might pass, or on the individual MPLS-TP devices themselves.

5.3. Use of Isolated Infrastructure

One way to protect the infrastructure used for support of MPLS-TP is to separate the resources for support of MPLS-TP services from the resources used for other purposes. For example, in security model 2 (Section 2.2), the potential risk of attacks on the S-PE or T-PE in the trusted zone may be reduced by using non-IP-based communication paths.

5.4. Use of Aggregated Infrastructure

In general, it is not feasible to use a completely separate set of resources for support of each service. In fact, one of the main reasons for MPLS-TP enabled services is to allow sharing of resources between multiple services and multiple users. Thus, even if certain services use a separate network from Internet services, nonetheless there will still be multiple MPLS-TP users sharing the same network resources.

In general, the use of aggregated infrastructure allows the service provider to benefit from stochastic multiplexing of multiple bursty flows, and also may in some cases thwart traffic pattern analysis by combining the data from multiple users. However, service providers must minimize security risks introduced from any individual service or individual users.

5.5. Mitigatoion of Denial of Service Attacks

It is possible to lessen the potential and impact of denial-of-service attacks by using secure protocols, turning off unnecessary processes, logging and monitoring, and using ingress filtering. See [RFC4732] for background on denial-of-service attacks in the context of the Internet.

5.6. Verification of Connectivity

To protect against deliberate or accidental misconnection, mechanisms can be put in place to verify both end-to-end connectivity and hop-by-hop resources. These mechanisms can trace the routes of LSPs in both the control plane and the data plane.

6. Monitoring, Detection, and Reporting of Security Attacks

MPLS-TP networks and services may be subject to attacks from a variety of security threats. Many types of threats are described in the Security Requirements (Section 4) section of this document. The defensive techniques described in this document and elsewhere provide significant levels of protection from many of these threats. However, in addition to employing defensive techniques silently to protect against attacks, MPLS-TP services can also add value for both providers and customers by implementing security monitoring systems to detect and report on any security attacks, regardless of whether the attacks are effective.

Attackers often begin by probing and analyzing defenses, so systems that can detect and properly report these early stages of attacks can provide significant benefits.

Information concerning attack incidents, especially if available quickly, can be useful in defending against further attacks. It can be used to help identify attackers or their specific targets at an early stage. This knowledge about attackers and targets can be used to strengthen defenses against specific attacks or attackers, or to improve the defenses for specific targets on an as-needed basis. Information collected on attacks may also be useful in identifying and developing defenses against novel attack types.

Also, extensive logging of normal processing, error conditions, and security events can be an invaluable source of information for tracking down attacks, recovering from them, and determining how to prevent future attacks. Different methods may be appropriate from case to case, and in fact comparing the same or similar information obtained in different ways (e.g., with syslog and SNMP) sometimes reveals subtle security flaws or actual intrusions. Implementations should also pay attention to the security of the logs themselves.

7. Security Considerations

Security considerations constitute the sole subject of this document and hence are discussed throughout.

The document describes a variety of defensive techniques that may be used to counter the potential threats. All of the techniques presented involve mature and widely implemented technologies that are practical to implement.

The document evaluates MPLS-TP security requirements from a customer's perspective as well as from a service provider's perspective. These sections re-evaluate the identified threats from the perspectives of the various stakeholders and are meant to assist equipment vendors and service providers, who must ultimately decide what threats to protect against in any given configuration or service offering.

8. IANA Considerations

This document contains no new IANA considerations.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3871] Jones, G., "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", RFC 3871, September 2504.

[RFC4732] Handley, M., Rescorla, E., and IAB, "Internet Denial-of-Service Considerations", RFC 4732, December 2006.

[RFC5654] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2509.

[RFC5951] Lam, K., Mansfield, S., and E. Gray, "Network Management Requirements for MPLS-based Transport Networks", RFC 5951, September 2510.

9.2. Informative References

[OIF-SMI-03.0]
Optical Internetworking Forum, "Security for Management Interfaces to Network Elements", OIF OIF-SMI-03.0, November 2011.

[RFC3631] Bellovin, S., Schiller, J., and C. Kaufman, "Security Mechanisms for the Internet", RFC 3631, December 2003.

[RFC5920] Fang, L., "Security Framework for MPLS and GMPLS Networks", RFC 5920, July 2010.

[RFC5921] Bocci, M., Bryant, S., Frost, D., Levrau, L., and L.
           Berger, "A Framework for MPLS in Transport Networks",
           RFC 5921, July 2010.

[opsec-efforts]
           "Security Best Practices Efforts and Documents",
           IETF draft-ietf-opsec-efforts-18.txt, April 2012.

Authors' Addresses

Luyuan Fang (editor)
Cisco Systems
111 Wood Ave. South
Iselin, NJ 08830
US
Email: lufang@cisco.com

Ben Niven-Jenkins (editor)
Velocix
326 Cambridge Science Park
Milton Road
Cambridge CB4 0WG
UK
Email: ben@niven-jenkins.co.uk

Scott Mansfield (editor)
Ericsson
300 Holger Way
San Jose, CA 95134
US
Email: scott.mansfield@ericsson.com

Richard F. Graveman (editor)
RFG Security, LLC
15 Park Avenue
Morristown, NJ 07960
US
Email: rfg@acm.org

Raymond Zhang
Alcatel-Lucent
701 Middlefield Road
Mountain View, CA 94043
US
Email: raymond.zhang@alcatel-lucent.com

Nabil Bitar
Verizon
40 Sylvan Road
Waltham, MA 02145
US
Email: nabil.bitar@verizon.com

Masahiro Daikoku
KDDI Corporation
3-11-11 Iidabashi, Chiyodaku,
Tokyo
Japan
Email: ms-daikoku@kddi.com

Lei Wang
Lime Networks
Strandveien 30, 1366 Lysaker
Norway
Email: lei.wang@limenetworks.no

Henry Yu
TW Telecom
10475 Park Meadow Drive
Littleton, CO 80124
US
Email: henry.yu@twtelecom.com