Network Working Group
Internet Draft
Intended status: Informational
Expires: Jan. 6, 2009

Luyuan Fang
Cisco Systems
Ben Niven-Jenkins
BT

July 6, 2009

Security Framework for MPLS-TP
draft-fang-mpls-tp-security-framework-00.txt

Status of this Memo

Copyright Notice

Abstract

MPLS-TP Security framework
July 2009

This document provides a security framework for Multiprotocol Label Switching Transport Profile (MPLS-TP). MPLS-TP Requirements and MPLS-TP Framework are defined in [MPLS-TP REQ] and [MPLS-TP FW]. Extended from MPLS technologies, MPLS-TP introduces new OAM capabilities, transport oriented path protection mechanism, and strong emphasis on static provisioning supported by network management systems. This document addresses the security aspects that are relevant in the context of MPLS-TP specifically. It describes the security requirements for MPLS-TP; potential securities threats and migration procedures for MPLS-TP networks and MPLS-TP inter-connection to MPLS, GMPLS networks. The general security analysis and guidelines for MPLS and GMPLS are addressed in [MPLS/GMPLS Security FW], will not be covered in this document.

Table of Contents

Requirements Language

Although this document is not a protocol specification, 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 RFC 2119 [RFC 2119].

1. Introduction

1.1. Background and Motivation

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

MPLS-TP Requirements and MPLS-TP Framework are defined in [MPLS-TP REQ] and [MPLS-TP FW]. The intent of MPLS-TP development is to address the needs for transport evolution, the fast growing bandwidth demand accelerated by new packet based services and multimedia applications, from Ethernet Services, Layer 2 and Layer 3 VPNS, triple play to Mobile Access Network (RAN) backhaul, etc. MPLS-TP is based on MPLS technologies to take advantage of the maturity, and it is required to maintain the transport characteristics.

Focused on meeting the transport requirements, MPLS-TP uses a subset of MPLS features, and introduces extensions to reflect the transport technology characteristics. 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 System (NMS) or Operation Support System (OSS). Of course, there are needs for MPLS-TP and MPLS interworking.

The security aspects for the new extensions which are particularly designed for MPLS-TP need to be addressed. The security models, requirements, threat and defense techniques previously defined in [MPLS/GMPLS SEC FW] can be used for the re-use of the existing functionalities in MPLS and GMPLS, but not sufficient to cover the new extensions.

1.2. Scope

This document addresses the security aspects that are specific to MPLS-TP. It intends to provide the security requirements for MPLS-TP; defines security models which apply to various MPLS-TP deployment scenarios; identifies the potential securities threats and migration procedures for MPLS-TP networks and MPLS-TP inter-connection to MPLS, GMPLS networks. Inter-AS and Inter-provider security for MPLS-TP to MPLS-TP connections or MPLS-TP to MPLS connections are discussed, there connections present higher security risk factors are than Intra-AS MPLS-TP connections.

The general security analysis and guidelines for MPLS and GMPLS are addressed in [MPLS/GMPLS Security FW], the content which has no new impact to MPLS-TP will not be repeated in this document. Other general security issues regarding transport networks but not specific to MPLS-TP is out of scope as well. Readers may also refer to the "Security Best Practices Efforts and Documents" [opsec effort] and "Security Mechanisms for the Internet" [RFC3631] (if there are linkage to internet in the applications) for general network operation security considerations. This document does not intend to define the specific mechanisms/methods which must be implemented to satisfy the security requirements.

1.3. Terminology

This document uses MPLS, MPLS-TP, and Security specific terminology. Detailed definitions and additional terminology for MPLS-TP may be found in [MPLS-TP REQ], [MPLS-TP FW], and MPLS/GMPLS security related terminology in [MPLS/GMPLS SEC FW].

Term	Definition
APS	Automatic Protection Switching
ATM	Asynchronous Transfer Mode
BFD	Bidirectional Forwarding Detection
CE	Customer-Edge device
CM	Configuration Management
CoS	Class of Service
CPU	Central Processing Unit
DNS	Domain Name System
DoS	Denial of Service
EMF	Equipment Management Function
ESP	Encapsulating Security Payload
FEC	Forwarding Equivalence Class
FM	Fault Management
GAL	Generic Alert Label
G-ACH	Generic Associated Channel

GMPLS	Generalized Multi-Protocol Label Switching
GCM	Galois Counter Mode
IKE	Internet Key Exchange
LDP	Label Distribution Protocol
LMP	Link Management Protocol
LSP	Label Switched Path
MD5	Message Digest Algorithm
MEP	Maintenance End Point
MIP	Maintenance Intermediate Point
MPLS	MultiProtocol Label Switching
NTP	Network Time Protocol
OAM	Operations, Administration, and Management
PE	Provider-Edge device
PM	Performance Management
PSN	Packet-Switched Network
PW	Pseudowire
QoS	Quality of Service
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol with Traffic Engineering Extensions
SCC	Signaling Communication Channel
SDH	Synchronous Digital Hierarchy
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
S-PE	Switching Provider Edge
SRLG	Shared Risk Link Group
SSH	Secure Shell
SSL	Secure Sockets Layer
SYN	Synchronize packet in TCP
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TE	Traffic Engineering
TLS	Transport Layer Security
TTL	Time-To-Live
T-PE	Terminating Provider Edge
UDP	User Datagram Protocol
VPN	Virtual Private Network
WG	Working Group of IETF
WSS	Web Services Security

1.4. Structure of the document

Section 1: Introduction
Section 2: MPLS-TP Security Reference Models
Section 3: Security Requirements
Section 4: Security threats

Section 5: Defensive/mitigation techniques/procedures

Note that this document is currently work in progress, not all requirements and security discussions are included, some sections will be filled in later revision.

2. Security Reference Models

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

The models are built on the architecture of MPLS-TP defined in [MPLS-TP FW]. The SP boundaries play the important role to determine the security models for any particular deployment.

This document defines the zone where the single SP has the total operational control to be a trusted zone for that SP. 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 the reference model 1, a single SP has the total control of PE/T-PE to PE/T-PE of the MPLS-TP network.

Security reference model 1(a):

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

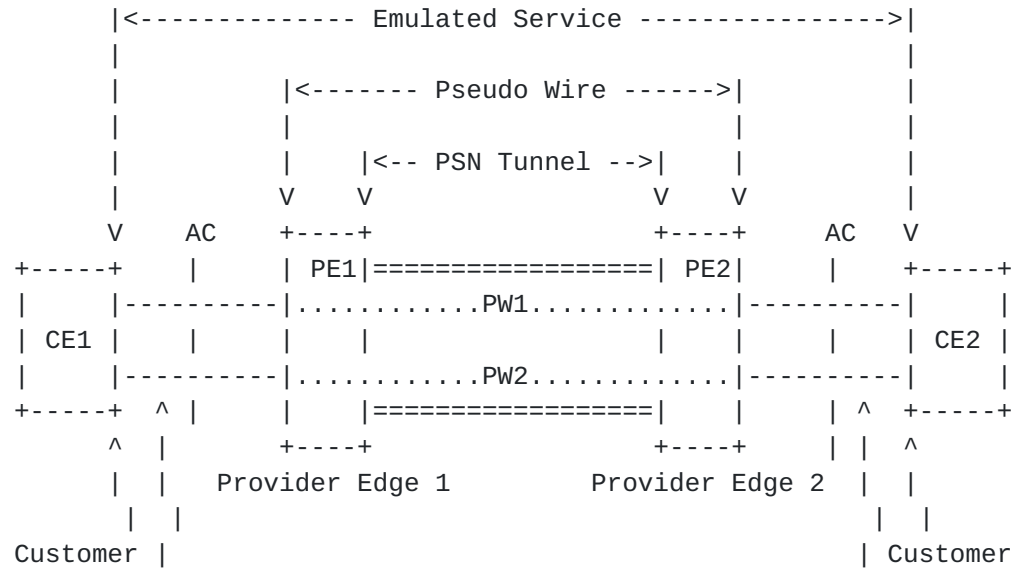


Figure 1: MPLS-TP Security Model 1 (a)

Security reference model 1(b):

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 Figure 2.

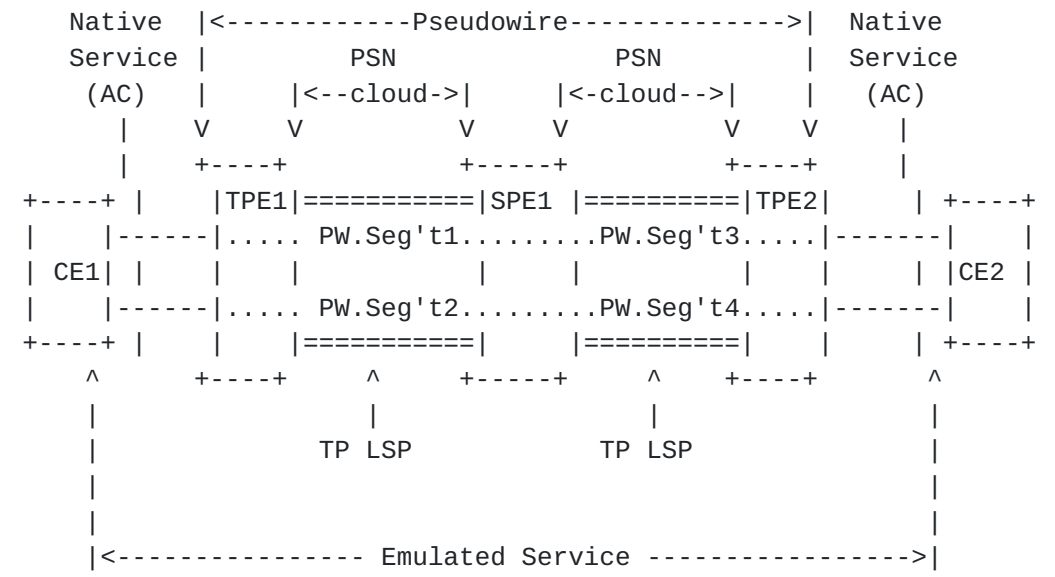


Figure 2: MPLS-TP Security Model 2 (b)

2.2. Security Reference Model 2

In the reference model 2, a single SP does not have the total control of PE/T-PE to PE/T-PE of the MPLS-TP network, S-PE and T-PE may be owned by different SPs or SPs and their customers. The MPLS-TP network is not contained in one trusted zone.

Security Reference Model 2(a)

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

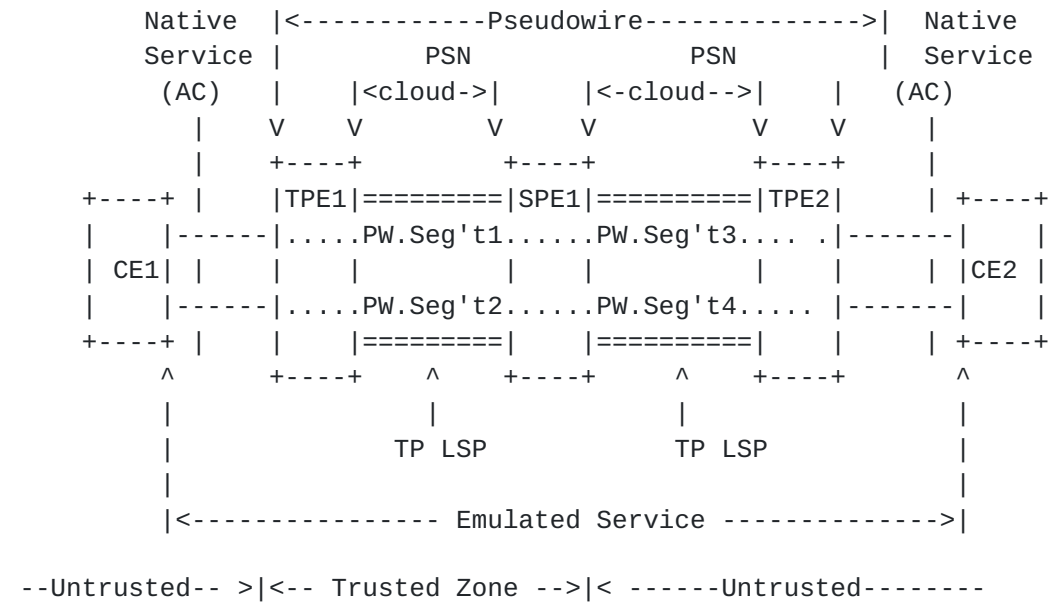
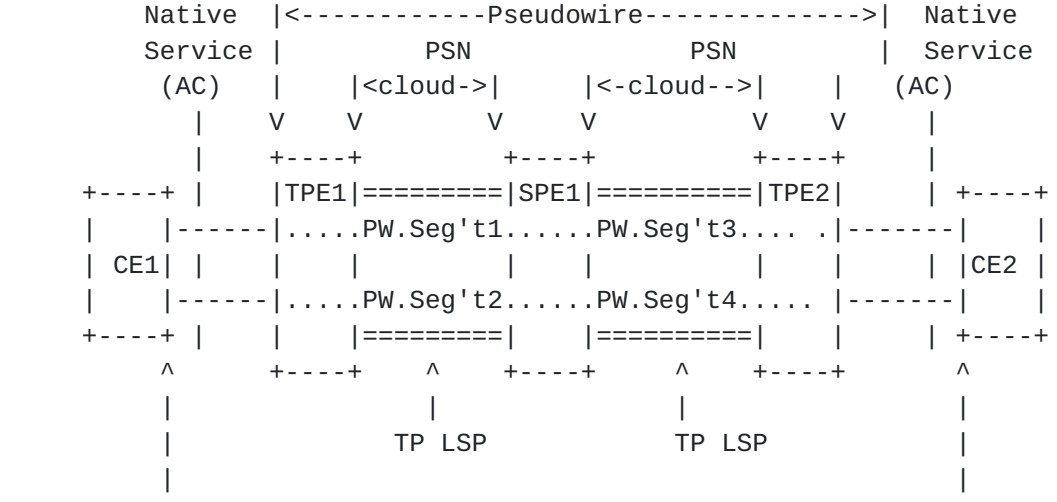


Figure 3: MPLS-TP Security Model 2(a)

Security Reference Model 2(b)

MPLS-TP network with Multi-Segment Pseudowire (MS-PW) from PE to PE. The trusted zone is S-PE, as illustrated in Figure 3.



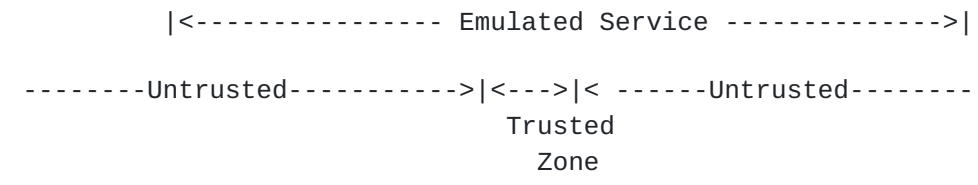


Figure 4: MPLS-TP Security Model 2(b)

Security Reference Model 2(c):

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

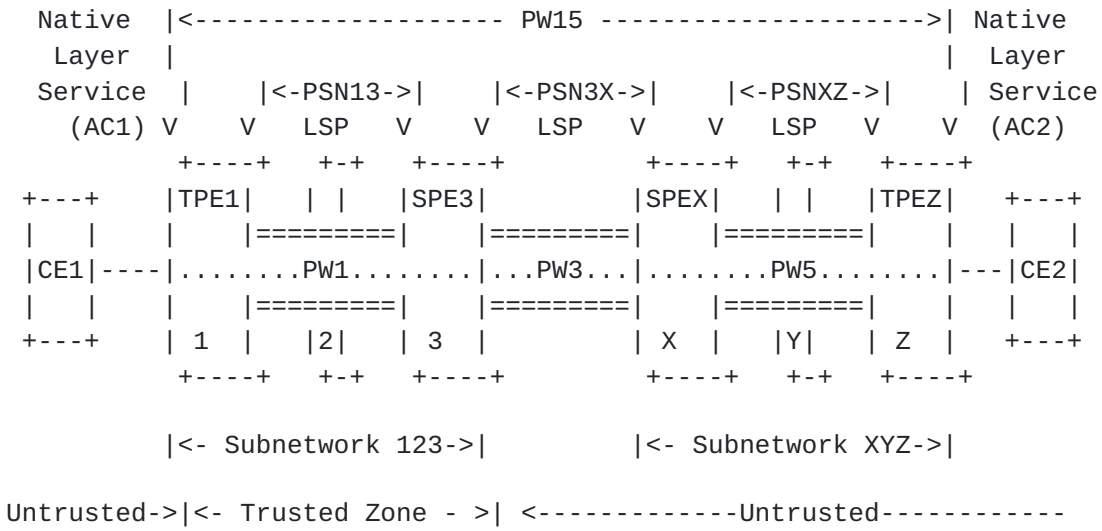
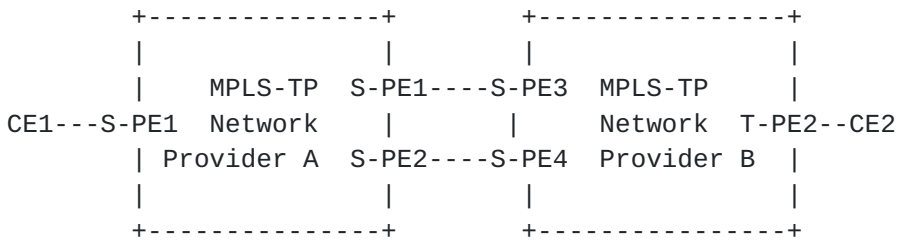


Figure 5: MPLS-TP Security Model 2(c)

The boundaries of a trust domain should be carefully defined when analyzing the security properties of each individual network, as illustrated from the above, the security boundaries determined which model would be applied to the use case analysis.

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

In addition, neighbors may be trusted or untrusted. Neighbors may 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 an untrusted but may be authorized neighbor.



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 neighbors: CE1, CE2

Figure 5. MPLS-TP trusted zone and authorized neighbor.

3. Security Requirements for MPLS-TP

This section covers security requirements for securing MPLS-TP network infrastructure. The MPLS-TP network can be operated without control plane or via dynamic control planes protocols. The security requirements related to new MPLS-TP OAM, recovery mechanisms, MPLS-TP and MPLS interconnection, and MPLS-TP specific operational requirements will be addressed in this section.

A service provider may choose the implementation options which are best fit for his/her network operation. This document does not state that a MPLS/GMPLS network must fulfill all security requirements listed to be secure.

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 accidentally and maliciously; 2) prevention of operational errors resulted from misconfiguration within the trusted zone.

3.1. Protection within the MPLS-TP Network

-
- MPLS-TP MUST support the physical and logical separation of data plane from the control plane and management plane. That is, if the control plane or/and management plane are attached and cannot function normally, the data plane should continue to forward packets without being impacted.
-
- MPLS-TP MUST support static provisioning of MPLS-TP LSP and PW with or without NMS/OSS, without using control protocols. This is particularly important in the case of security model 2(a) and 2(b) where the some or all T-PEs are not in the trusted zone, and in the inter-provider cases in security model 2(c) when the connecting S-PE is in the untrusted zone.

- MPLS-TP MUST support non-IP path options in addition to IP loopback option. Non-IP path option used in the model 2 may help to lower the potential risk of the S-PE/T-PE in the trusted zone to be attacked.

- MPLS-TP MUST support authentication of the any control protocol used for MPLS-TP network, as well as MPLS-TP network to dynamic MPLS network inter-connection.

- MPLS-TP MUST support mechanisms to prevent DOS attack through in-band OAM GACH/GAL.

- MPLS-TP MUST support hiding of the Service Provider infrastructure for all reference models regardless using static configuration or dynamic control plane.

- Security management requirements [MPLS-TP NM REQ]:

    o MPLS-TP must support management communication channel security secure communication channels MUST be supported for all network traffic and protocols used to support management functions. This MUST include protocols used for configuration, monitoring, configuration backup, logging, time synchronization, authentication, and routing. The MCC MUST support application protocols that provide confidentiality and data integrity protection. Support the use of open cryptographic algorithms [RFC 3871]; Authentication - allow management connectivity and activity only from authenticated entities, and port access control.
    o Distributed Denial of Service: It is possible to lessen the impact and potential for DoS and DDoS by using secure

protocols, turning off unnecessary processes, logging and monitoring, and ingress filtering. [RFC 4732] provides background on DOS in the context of the Internet.

(more to be added)

- Protection of Operational error

Due to the extensive use of static provisioning with or without NMS and OSS, the prevention of configuration errors should be addressed as major security requirements.

(to be added)

4. Security Threats

This section discusses the various network security threats that may endanger MPLS-TP networks. The discussion is limited to those threats that are unique to MPLS-TP networks or that affect MPLS-TP network in unique 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 ill effects:

- Observation, modification, or deletion of a provider's or user's data.
- Replay of a provider's or user's data.
- Injection of inauthentic data into a provider's or user's traffic stream.
- Traffic pattern analysis on a provider's or user's traffic.
- Disruption of a provider's or user's connectivity.
- Degradation of a provider's service quality.
- Probing a provider's network to determine its configuration, capacity, or usage.

It is useful to consider that threats, whether malicious or accidental, may come from different categories of sources. For example they may come from:

- Other users whose services are provided by the same MPLS-TP core.
- The MPLS-TP SP or persons working for it.
- Other persons who obtain physical access to a MPLS-TP SP's site.
- Other persons who use social engineering methods to influence the behavior of a SP's personnel.
- Users of the MPLS-TP network itself.

- Others, e.g., attackers from the other sources, Internet if connected.
- Other SPs in the case of MPLS-TP Inter-provider connection. The provider may or may not be using MPLS-TP.
- Those who create, deliver, install, and maintain software for network equipment.

Given that security is generally a tradeoff between expense and risk, it is also useful to consider the likelihood of different attacks occurring. There is at least a perceived difference in the likelihood of most types of attacks being successfully mounted in different environments, such as:

- A MPLS-TP network inter-connecting with another provider's core
- A MPLS-TP configuration transiting the public Internet

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. In closed communities, it is often practical to deal with misbehavior after the fact: an employee can be disciplined, for example.

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

4.1. Attacks on the Control Plane

- MPLS-TP LSP creation by an unauthorized element

- LSP message interception

- Attacks against LDP

- Attacks against RSVP-TE

- Attacks against GMPLS

- Denial of Service Attacks on the Network Infrastructure

- Attacks on the SP's MPLS/GMPLS Equipment via Management Interfaces
- Social Engineering Attacks on the SP's Infrastructure
- Cross-Connection of Traffic between Users
- Attacks against Routing Protocols
- Other Attacks on Control Traffic

4.2. Attacks on the Data Plane

This category encompasses attacks on the provider's or end user's data. Note that from the MPLS-TP network end user's point of view, some of this might be control plane traffic, e.g. routing protocols running from user site A to user site B via IP or non-IP connections, which may be some type of VPN.

- Unauthorized Observation of Data Traffic
- Modification of Data Traffic
- Insertion of Inauthentic Data Traffic: Spoofing and Replay
- Unauthorized Deletion of Data Traffic
- Unauthorized Traffic Pattern Analysis
- Denial of Service Attacks
- Misconnection

5. Defensive Techniques for MPLS-TP Networks

The defensive techniques discussed 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 implementations. 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 operational environment determines the security requirements. Therefore, protocol designers need to provide a full set of security services, which can be used where appropriate.

The techniques discussed here include encryption, authentication, filtering, firewalls, access control, isolation, aggregation, and others.

5.1. Authentication

To prevent security issues arising from some DoS attacks or from malicious or accidental misconfiguration, it is critical that devices in the MPLS-TP should only accept connections or control messages from valid sources. Authentication refers to methods to ensure that message sources are properly identified by the MPLS-TP devices with which they communicate. This section focuses on identifying the 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.

Authentication should be bi-directional, including PE or CE to configuration server authentication for PE or CE 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 (i.e., authentication of one IPsec security gateway by another).

Authentication should be bi-directional, including S-PE, T-PE, PE or CE to configuration server authentication for PE or CE to 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 range of public-private key systems. Another approach is to use a hierarchical Certification Authority system to provide digital certificates.

5.2. Access Control Techniques

- Access Control to Management Interfaces

Most of the security issues related to management interfaces can be addressed through the use of authentication techniques as described in the section on authentication. However, additional security may be provided by controlling access to management interfaces in other ways.

The Optical Internetworking Forum has done relevant work on protecting such interfaces with TLS, SSH, Kerberos, IPsec, WSS, etc. See OIF-SMI-01.0 "Security for Management Interfaces to Network Elements" [OIF-SMI-01.0], and "Addendum to the Security for Management Interfaces to Network Elements" [OIF-SMI-02.1]. See also the work in the ISMS WG.

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

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. Service Provider Quality Control Processes

5.6. Verification of Connectivity

In order 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 network and service may be subject to attacks from a variety of security threats. Many threats are described in Section 3 of this document. Many of the defensive techniques described in this document and elsewhere provide significant levels of protection from a variety of 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.

7. Security Considerations

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

The document describes a variety of defensive techniques that may be used to counter the suspected 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. Normative References

[MPLS-TP REQ], Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "MPLS-TP Requirements", draft-ietf-mpls-tp-requirements-09 (work in progress), June 2009.

[MPLS-TP FW] Bocci, M., Bryant, S., and L. Levrau, "A Framework for MPLS in Transport Networks", draft-ietf-mpls-tp-framework-01 (work in progress), June 2009.

[RFC 3871] Jones, G., "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", RFC 3871, September 2004.

[RFC 4732] Handley, M., et al, "Internet Denial-of-Service Considerations", RFC 4732, November 2006.

10. Informative References

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

[OIF-SMI-01.0] Renee Esposito, "Security for Management Interfaces to Network Elements", Optical Internetworking Forum, Sept. 2003.

[OIF-SMI-02.1] Renee Esposito, "Addendum to the Security for Management Interfaces to Network Elements", Optical Internetworking Forum, March 2006.

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

[MFA MPLS ICI] N. Bitar, "MPLS InterCarrier Interconnect Technical Specification", IP/MPLS Forum 19.0.0, April 2008.

[opsec efforts] C. Lonvick and D. Spak, "Security Best Practices Efforts and Documents", draft-ietf-opsec-efforts-08.txt, June 2008.

[MPLS/GMPLS SEC FW] L. Fang, et al, Security Framework for MPLS and GMPLS Networks, draft-ietf-mpls-mpls-and-gmpls-security-framework-05.txt, March 2009.

[MPLS-TP NM REQ] Hing-Kam Lam, Scott Mansfield, Eric Gray, MPLS TP Network Management Requirements, draft-ietf-mpls-tp-nm-req-02.txt, June 2009.

11. Author's Addresses

Luyuan Fang
Cisco Systems, Inc.
300 Beaver Brook Road
Boxborough, MA 01719
USA

Email: lufang@cisco.com

Ben Niven-Jenkins
BT
208 Callisto House
Adastral Park, Ipswich IP5 3RE
UK

Email: benjamin.niven-jenkins@bt.com