

Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 1, 2007

Y(J). Stein
RAD Data Communications
Feb 28, 2007

Requirements for PW Security
draft-stein-pwe3-sec-req-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on September 1, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

To date IETF's security suite has been entirely IP-centric, IPsec only being applicable to IP packets. This document addresses security requirements for MPLS pseudowires. We investigate security considerations arising from the PWE3 architecture, and discuss example threats, authentication, and confidentiality.

Internet-Draft

pwe3-sec-req

Feb 2007

1. Introduction

Although the IP suite is obviously its main focus, the IETF has standardized other protocols, notably MPLS [[1](#)] and MPLS pseudowires (PWs) [[3](#)]. On the other hand, IETF's security suite is entirely IP-centric, IPsec only being applicable to IP packets. Security aspects of MPLS networks have been addressed in various RFCs, and PPVPN security is been discussed in [[4](#)]; work is in progress on an MPLS/GMPLS security framework [[7](#)]. Security considerations of the MPLS control plane will most likely be applicable to the PWE3 control protocol [[5](#)] as well. On the other hand security of the user plane for non-IP traffic such as PWs has not yet been addressed in the IETF.

The PWE3 architecture [[3](#)] defines a pseudowire (PW) connecting customer networks over a provider network. The customer networks run a native service, which may be Ethernet, ATM, frame relay, TDM, etc. On both sides of the PW a customer edge (CE) connects to a provider edge (PE) via an attachment circuit (AC). The PW itself is a tunnel that transports the native service data across the provider network, here assumed to be based on MPLS. PW tunnels are set up using the PWE control protocol based on LDP [[2](#)].

PW packets contain at least one MPLS label (the PW label) and may contain one or more MPLS tunnel labels. After the label stack there is a four-byte control word (which is optional for some PW types), followed by the native service payload. It must be stressed that encapsulation of MPLS PW packets in IP for the purpose of enabling use of IPsec mechanisms is not a valid option.

For the purpose of the present discussion, the customer networks will be considered walled gardens, under the control of the customer. The provider network is under the control of the provider, but accessible to multiple customers. The customer expects the provider to ensure that its data traversing the provider's network be afforded security similar to that of a (virtual) connection of the native service.

The following will be considered explicitly out-of-scope of the present treatment:

- security considerations of the customer networks,
- security considerations of the attachment circuits,
- any security considerations that would exist were the customer networks connected via native service links,

security considerations common to all MPLS networks.

The following is a nonexhaustive list of threats to be considered:

Stein

Expires September 1, 2007

[Page 2]

Internet-Draft

pwe3-sec-req

Feb 2007

unauthorized setting up a PW (e.g. to gain access to a customer network),
unauthorized tearing down of a PW (thus causing denial of service),
malicious rerouting of a PW,
forking of a PW to snoop PW packets,
unauthorized on-route snooping of PW packets,
traffic analysis of PW connectivity,
unauthorized insertion of PW packets,
unauthorized modification of PW packets,
unauthorized deletion of PW packets,
replay of PW packets,
denial of service or significantly impacting PW service quality.
These threats are not mutually exclusive, for example, rerouting can be used for snooping or insertion/deletion/replay, etc.

Special considerations arising for MS-PWs are for further study.

[2.](#) PW-specific Security Weaknesses and Strengths

The PW user plane suffers from the following inherent security weaknesses:

- the PW label is the only identifier in the packet (there is no authenticatable source address, cookies, etc.),
hence it is relatively easy to introduce seemingly valid foreign packets,
- the control word sequence number processing algorithm is susceptible to a DoS attack (the sequence number processing algorithm can cause dropping of late packets, so inserting a single future packet can cause a large number of legitimate packets to be discarded).

VPLS services built on Ethernet PWs and multisegment PWs introduce additional problems.

Even without the ability to observe PW packets, guessing a valid PW

label is not difficult. Many implementations start by assigning low PW labels, and thus a small number will usually correspond to a valid PW label. In any case there is no penalty to incorrect guessing, and if one can inject one thousand PW packets per second, then one exhausts the entire PW label space in about fifteen minutes.

The PWE control protocol introduces its own weaknesses:

- no (secure) peer autodiscovery technique has been standardized,
- PE authentication is not mandated, so an intruder can potentially impersonate a PE,

Stein

Expires September 1, 2007

[Page 3]

Internet-Draft

pwe3-sec-req

Feb 2007

after impersonating a PE, unauthorized PWs may be set up, consuming resources and perhaps allowing access to user networks, similarly, desired PWs may be torn down, giving rise to denial of service.

Despite these weaknesses, PWs have the following advantages:

- the most obvious attacks require compromising edge or core routers (although not necessarily those along PW path),
- adequate protection of the control plane messaging is sufficient to rule out many attacks,
- PEs are usually configured to reject MPLS packets from the outside the service provider network, thus ruling out insertion of PW packets from the outside (since IP packets can not masquerade as PW packets).

[3.](#) Example Attacks

A PW man-in-the-middle occurs when an impostor causes two consecutive PWs to be set up instead of one, and stitches them at a provider router of which he has gained control. Such an impostor can then snoop, delete, insert, and change, PW packets. This is different from an MPLS man-in-the-middle attack, which results from an impostor compromising a provider LSR somewhere along the PW path. This latter attack can also compromise PW security, but must be dealt with as an MPLS attack, and is out of scope here.

In another scenario the attack involves compromising a forwarding device (router or Ethernet switch) that is not part of the PW path.

In this case the attack exploits the MPLS mechanism for tunnel merging. The attacker can now insert a packet with the PW label associated with any PW (as inner labels are not inspected by provider routers). By judicious choice of sequence number, the attacker may be able to force massive packet loss, as mentioned above.

[4.](#) Defensive Techniques

[4.1.](#) PW Packet Authentication

One way of ensuring that a packet is a valid PW packet, is to authenticate it by inserting a cryptographically derived field between the control word and the payload. It is envisaged that the insertion of such a field will be agreed upon between the two PEs using an extension to the PWE control protocol. This method will only be useful when the desired PW packets emanate from a PE with this capability, and when there is a secure key distribution infrastructure.

Stein

Expires September 1, 2007

[Page 4]

Internet-Draft

pwe3-sec-req

Feb 2007

In a light-weight version that may be sufficient for some applications, and which could be implemented entirely in software, a 32-bit cookie is inserted that is derived entirely from the control word, or (for SS-PWs), from the control word and PW label. The mapping of control word to cookie may make use of symmetric or public-key methods.

In a more heavy-weight version a 64-bit authentication cookie is inserted which results from a cryptographic hash on the entire PW payload. The authentication of this cookie should be hardware-assisted in order to avoid a denial of service attack based on sending invalid packets in order to overload computational resources.

[4.2.](#) PW Packet Encryption

In order to secure PW traffic from unauthorized observation we may encrypt it

- below the PW level (link encryption), or
- at the PW level, or
- above the PW level (service encryption).

Link encryption and service encryption are well understood, but PW

level encryption requires a new mechanism. The first question is what is encrypted at this layer. Since the PW label is part of the MPLS label stack, encrypting it would render the packet illegal from an MPLS point of view. The first nibble of the control word enables packet classification for ECMP, and thus encrypting it would disrupt ECMP mechanisms [6].

On the other hand, if only the payload is encrypted, PW level encryption becomes similar to service encryption. A universal mechanism for securing PW packets of all types is proposed in [8]. The main difference relates to the use of the sequence number. PW mechanisms do not provide packet reliability, thus encryption must function on a packet-by-packet basis, and recover from occasional lost packets. Hence service level encryptions based on stream ciphers may not directly be applicable. PW layer encryption may rely on the sequence number (when the control word is used) but not directly on the data stream, or even the number of bytes that have been transmitted.

[5.](#) Security Considerations

Since this entire document is about security considerations, a security consideration section would be superfluous.

Stein

Expires September 1, 2007

[Page 5]

Internet-Draft

pwe3-sec-req

Feb 2007

[6.](#) IANA Considerations

This Internet Draft does not propose a protocol, nor change any existing protocol, and thus no IANA considerations are raised.

[7.](#) Informative References

- [1] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", [RFC 3031](#), January 2001.
- [2] Andersson, L., Doolan, P., Feldman, N., Fredette, A., and B. Thomas, "LDP Specification", [RFC 3036](#), January 2001.
- [3] Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge

(PWE3) Architecture", [RFC 3985](#), March 2005.

- [4] Fang, L., "Security Framework for Provider-Provisioned Virtual Private Networks (PPVPNs)", [RFC 4111](#), July 2005.
- [5] Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", [RFC 4447](#), April 2006.
- [6] Swallow, G., Bryant, S., and L. Andersson, "Avoiding Equal Cost Multipath Treatment in MPLS Networks", [draft-ietf-mpls-ecmp-bcp-03.txt](#) (work in progress), August 2007.
- [7] Fang, L., Behringer, M., Callon, R., Le Roux, J.L., Zhang, R., and P. Knight, "Security Framework for MPLS and GMPLS Networks", [draft-fang-mpls-gmpls-security-framework-00.txt](#) (work in progress), August 2007.
- [8] Stein, Y(J)S., "Pseudowire Security (PWsec)", [draft-draft-stein-pwe3-pwsec-00.txt](#) (work in progress), October 2006.

Stein

Expires September 1, 2007

[Page 6]

Internet-Draft

pwe3-sec-req

Feb 2007

Author's Address

Yaakov (J) Stein
RAD Data Communications
24 Raoul Wallenberg St., Bldg C
Tel Aviv 69719
ISRAEL

Phone: +972 3 645-5389
Email: yaakov_s@rad.com

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).