

Network Working Group
Internet-Draft
Expires: April 16, 2007

Y(J) Stein
RAD Data Communications
Oct 13, 2006

Pseudowire Security (PWsec)
draft-stein-pwe3-pwsec-00.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 April 16, 2007.

Copyright Notice

Copyright (C) The Internet Society (2006).

Abstract

This document proposes an extension to the MPLS pseudowire format to enhance pseudowire user-plane security. The extension, called PWsec, provides confidentiality, data integrity, and source authentication. The extension is based on the National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) using the Galois/Counter Mode (GCM).

Internet-Draft

pwe3-pwsec

Oct 2006

Table of Contents

1.	Introduction	3
2.	AES/GCM	4
3.	PWsec encapsulation	6
4.	PWsec signaling	7
5.	Security Considerations	7
6.	IANA Considerations	7
7.	References	8
7.1	Normative References	8
7.2	Informative References	8
	Author's Address	9
	Intellectual Property and Copyright Statements	10

1. Introduction

The PWE3 architecture [[RFC3985](#)] 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 may be set up using the PWE control protocol [[RFC4447](#)].

Security threats specific to pseudowires were discussed in [PW-sec-req], where the following nonexhaustive list of user plane threats were considered:

- accidental connection to untrusted network compromising user traffic

- maliciously setting up a PW to gain access to a customer network

- forking of a PW to snoop PW packets

- malicious rerouting of a PW to snoop or modify PW packets

- unauthorized tearing down of a PW

- unauthorized snooping of PW packets

- traffic analysis of PW connectivity

- unauthorized deletion of PW packets

- unauthorized modification of PW packets

- unauthorized insertion of PW packets

replay of PW packets

denial of service or significantly impacting PW service quality.

In order to counter these threats, several security measures are needed. State-of-the-art encryption algorithms provide data confidentiality in order to frustrate snooping and prevent unintended data leakage. Mechanisms to ensure data integrity thwart packet insertion and modification. Source authentication may prevent malicious access to resources and denial of service attacks.

Stein

Expires April 16, 2007

[Page 3]

Internet-Draft

pwe3-pwsec

Oct 2006

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in [[RFC2119](#)].

[2.](#) AES/GCM

From 1976 to 2000 the Data Encryption Standard (DES) was the standard block cipher. In 2000, after an open competition for the selection of a successor to DES, the National Institute of Standards and Technology (NIST) announced that Rijndael had been selected as the basis for a new standard, and in 2001 the Advanced Encryption Standard (AES) was published [[AES](#)]. Agencies of the US government have certified that AES is sufficient to protect SECRET and even TOP SECRET classified information.

AES has a fixed block size of 128 bits and allows key sizes of 128, 192 or 256 bits. Like other block ciphers, in order to encrypt larger amounts of data, various 'modes of operation' may be used. The simplest mode is Electronic CodeBook (ECB), wherein the message is segmented into blocks each of which is separately encrypted. This mode is not recommended due to inherent weaknesses. Other modes, such as Cipher Block Chaining (CBC) and Output FeedBack (OFB) provide confidentiality but do not ensure overall message integrity, nor do they authenticate the claimed source. Newer modes, such as Offset CodeBook (OCB) and Counter (CTR) are designed to address these limitations.

The Galois/Counter Mode (GCM) has numerous advantages over other proposed modes of operation. Its most important characteristics:

encryption is provided by AES with a counter-type mode of operation

an Integrity Check Value (ICV) verifies the payload integrity

data that is not part of the packet payload (for example source identifiers) can be authenticated

encryption, integrity, and source authentication are performed by a single algorithm

authentication can be performed without encrypting data

the Initialization Vector (IV) nonce can be of arbitrary length

the algorithm can be efficiently implemented in software

Stein

Expires April 16, 2007

[Page 4]

Internet-Draft

pwe3-pwsec

Oct 2006

the computation can be pipelined and parallelized, enabling high speed hardware implementations

GCM mode is unencumbered by IPR claims.

For these reasons, AES/GCM has been adopted by the IEEE as the default cipher suite for 802.1ae (MACsec), and has been specified for IPsec ESP [[RFC4106](#)] and AH [[RFC4543](#)]. It is also being considered by other bodies for applications where high-speed authenticated encryption is required. When used to provide security for MPLS PWs, we shall call it PWsec.

When encrypting, AES/GCM takes the following as input:

the plaintext to be encrypted (up to $2^{36} - 32$ bytes in length)

the encryption key (128 or 256 bits in length)

a per-packet randomly generated IV (12 bytes is recommended for efficiency)

additional data to be authenticated but not encrypted (between 0

and 2^{61} bytes)

and returns the following as output

the ciphertext, whose length is precisely that of the plaintext

the ICV (which we shall take to be 16 bytes in length).

For a given encryption key IV values SHOULD NOT be repeated. In MACsec, the IV consists of a 4-byte Packet Number (PN) and a 8-byte Secure Channel Identifier (SCI). The PN is increased from frame to frame, and a new encryption key must be supplied before the PN recycles. An alternative way of conforming to the requirement is selecting random IV values such that repetition is highly unlikely.

When decrypting, AES/GCM takes the following as input:

the ciphertext to be decrypted

the encryption key

the IV nonce that was used when encrypting

the ICV generated during encryption

and returns the following as output

Stein

Expires April 16, 2007

[Page 5]

Internet-Draft

pwe3-pwsec

Oct 2006

a boolean value specifying whether the integrity test passed or failed

if the integrity test passed, the plaintext.

3. PWsec encapsulation

PWsec may be employed whether or not the control word [[RFC4385](#)] is used. If the control word is used, it is not encrypted. If an RTP header is used [[RFC3985](#)], it is encrypted. The format of a PWsec encrypted packet is given in Figure 1. Note that unlike MACsec, PWsec does not use the sequence number as part of the IV.

0

1

2

3

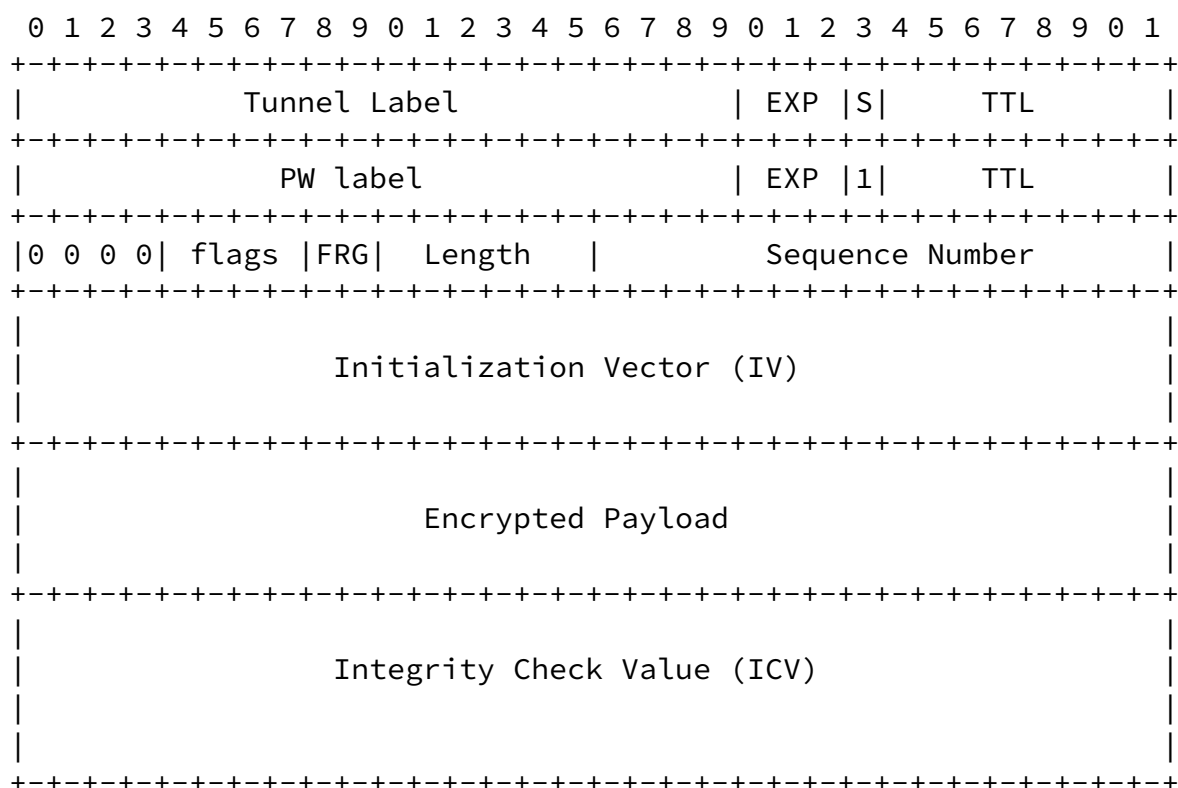


Figure 1. PWsec Packet Format

PWsec performs source authentication by using an identifier that uniquely identifies the source as additional data to be authenticated but not encrypted. If the control word is used and the sequence number is nonzero, the sequence number is authenticated in this way as well.

If the PW is set up using the PWE control protocol [\[RFC4447\]](#) using FEC 128, then the source identifier can be taken to be the source PE identifier plus the 4-byte Group ID plus the 4-byte PW ID. If the PW

is set up using the PWE control protocol using FEC 129, then the source identifier can be taken to be the source PE identifier plus the Attachment Identifier (AI); where the latter will usually consist of the Attachment Group Identifier (AGI) plus the Source Attachment Individual Identifier (SAII). For both cases, the entire contents of the FEC element MAY be authenticated. If the PW is statically provisioned, then a unique source identifier MUST be provisioned.

4. PWsec signaling

When setting up a PW to use PWsec using the PWE3 control protocol, a new TLV, called the PWsec TLV MUST be used in the LDP label mapping message. This TLV specifies the parameters of the encryption and authentication, including a code indicating the use of AES/GCM, the encryption key length (128 or 256 bits), the length of the IV (here a constant 12 bytes), the length of the ICV (here a constant 16 bytes), and the additional data to be authenticated. The format of this TLV will be specified in the next revision of this document.

The key used to encrypt and decrypt PW packets should be regularly changed. Methods for key distribution are beyond the scope of this document, but mechanisms such as the Internet Key Exchange (IKE) [[RFC4306](#)] are appropriate for this task.

5. Security Considerations

This document proposes a security mechanism for the MPLS PW user plane based on symmetric key cryptography. The mechanism is based on AES in GCM mode, which has been adopted by the IEEE as the default cipher suite for MACsec and has been specified for IPsec ESP [[RFC4106](#)] and AH [[RFC4543](#)]. Mechanisms for key distribution will be required, but were not specified.

Our discussion has focused on the PW user plane. To complement the proposed mechanism, security solutions for the PWE3 control protocol and for the management plane will be required.

6. IANA Considerations

In order to signal the use of PWsec, a new TLV to be used in the LDP label mapping message of the PWE3 control protocol [[RFC4447](#)] will be required.

7. References

7.1 Normative References

- [AES] NIST, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001.
- [GCM] McGrew, D. and J. Viega, "The Galois/Counter Mode of Operation (GCM)", January 2004.
Downloadable from <http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec.pdf>
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", [RFC 4106](#), June 2005.
- [RFC4447] 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.
- [RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", [RFC 4543](#), May 2006.

7.2 Informative References

- [PW-sec-req] Stein, Y(J)., "Requirements for PW Security", [draft-stein-pwe3-sec-req-00.txt](#) (work in progress), February 2006.
- [RFC3985] Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", [RFC 3985](#), March 2005.
- [RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", [RFC 4306](#), December 2005.
- [RFC4385] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", [RFC 4385](#), February 2006.

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

Internet-Draft

pwe3-pwsec

Oct 2006

Intellectual Property Statement

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.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2006). 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.