IPSECME
Internet-Draft
Updates: RFC4307
(if approved)
Intended status: Standards Track
Expires: October 3, 2010

S. Shen
Huawei
Y. Mao
H3C
NSS. Murthy
Freescale Semiconductor

April 1, 2010

Using Advanced Encryption Standard (AES) Counter Mode with IKEv2
draft-ietf-ipsecme-aes-ctr-ikev2-07

Abstract

This document describes the usage of Advanced Encryption Standard Counter Mode (AES-CTR), with an explicit initialization vector, by IKEv2 for encrypting the IKEv2 exchanges that follow the IKE_SA_INIT exchange.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and 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/1id-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 October 3, 2010.

Copyright Notice

Table of Contents

1. Introduction

IKEv2 [RFC4306] is a component of IPsec used for performing mutual authentication and establishing and maintaining security associations (SAs). [RFC4307] defines the set of algorithms that are mandatory to implement as part of IKEv2, as well as algorithms that should be implemented because they may be promoted to mandatory at some future time. [RFC4307] requires that an implementation "SHOULD" support Advanced Encryption Standard [AES] in Counter Mode [MODES] (AES-CTR) as a Transform Type 1 Algorithm (encryption).

Although the [RFC4307] specifies that the AES-CTR encryption algorithm feature SHOULD be supported by IKEv2, no existing document specifies how IKEv2 can support the feature. This document provides the specification and usage of AES-CTR counter mode by IKEv2.

1.1. Conventions Used In This Document

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].

2. IKEv2 Encrypted Payload

Section 3.14 of IKEv2 [RFC4306] explains the IKEv2 Encrypted Payload. The encrypted Payload, denoted SK{...} contains other IKEv2 payloads in encrypted form.

The payload includes an Initialization Vector (IV) whose length is defined by the encryption algorithm negotiated. It also includes Integrity Checksum data. These two fields are not encrypted.

The IV field MUST be 8 octets when the AES-CTR algorithm is used for IKEv2 encryption. The requirements for this IV are same as what is specified for ESP in Section 3.1 of [RFC3686].

IKEv2 requires Integrity Check Data for the Encrypted Payload as described in section 3.14 of [RFC4306]. The choice of integrity algorithms in IKEv2 is defined in [RFC4307] or its future update documents.

When AES-CTR is used in IKEv2, no padding is required. The Padding field of the Encrypted Payload SHOULD be empty and the Pad Length field SHOULD be zero. However, according to [RFC4306], the recipient MUST accept any length that results in proper alignment. It should be noted that the ESP [RFC4303] Encrypted Payload requires alignment on a 4-byte boundary while the IKEv2 [RFC4306] Encrypted Payload does not have such a requirement.

The Encrypted Payload is the XOR of the plaintext and key stream. The key stream is generated by inputting Counter Blocks into the AES

algorithm. The AES counter block is 128 bits including 4 octets nonce, 8 octets Initialization Vector and 4 octets Block counter in order. The block counter begins with the value of one and increments by one to generate next portion of the key stream. The detailed requirements for the counter block is the same as what is specified in Section 4 of [RFC3686].

3. IKEv2 Conventions

The use of AES-CTR for the IKE SA is negotiated in the same way as AES-CTR for ESP. The Transform ID (ENCR_AES_CTR) is the same; the key length transform attribute is used in the same way; and the keying material (consisting of the actual key and the nonce) is derived in the same way. Check Section 5 of [RFC3686] for the detailed descriptions.

4. Security Considerations

Security considerations explained in section 7 of [RFC3686] are entirely relevant for this draft also. The security considerations on fresh keys and integrity protection in section 7 of [RFC3686] are totally applicable on using AES-CTR in IKEv2; see [RFC3686] for details. As static keys are never used in IKEv2 for IKE_SA and integrity protection is mandatory for IKE_SA, these issues are not applicable for AES-CTR in IKEv2 when protecting IKE_SA.

Additionally, since AES has a 128-bit block size, regardless of the mode employed, the ciphertext generated by AES encryption becomes distinguishable from random values after 2^64 blocks are encrypted with a single key. Since IKEv2 SA cannot carry that much of data (because of the size limit of message ID of IKEv2 message and the

requirements for the message ID in Section 4 of [RFC4306]), this issue is not a concern here.

For generic attacks on AES, such as brute force or precalculations, the requirement of key size provides reasonable security [Recommendations].

5. IANA Considerations

IANA [IANA-Para] has assigned an Encryption Transform ID for AES-CTR encryption with an explicit IV for IKEv2: 13 as the number and ENCR_AES_CTR as the name. IANA is asked to add a reference to this RFC in that entry.

6. Acknowledgments

The authors thank Yaron Sheffer, Paul Hoffman, Tero Kivinen and Alfred Hoenes for their direction and comments on this document.

This document specifies usage of AES-CTR with IKEv2, similarly as usage of AES-CTR with ESP as specified in [RFC3686]. [RFC3686] is referred for the same descriptions and definitions. The authors thank Russ Housley for providing the document.

During the production and modification of this document, both Huawei and CNNIC supported one of the author, Sean Shen. Both are appreciated as affiliations of the author.

7. References

7.1. Normative References

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.

[RFC4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.

[AES] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001, <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

[IANA-Para] Internet Assigned Numbers Authority, "Internet Key Exchange Version 2 (IKEv2) Parameters", September 2009, <http://www.iana.org/assignments/ikev2-parameters>.

[MODES] Dworkin, M., "Recommendation for Block Cipher Modes of Operation Methods and Techniques", NIST Special Publication 800-38A, December 2001, <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>.

7.2. Informative References

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

[RFC3686] Housley, R., "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)", RFC 3686, January 2004.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, December 2005.

[Recommendations] Barker, E., Barker, W., Burr, W., Polk, W., and M. Smid, "Recommendation for Key Management - Part1 - General (Revised)", NIST Special Publication 800-57, March 2007, <http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf>.

Authors' Addresses

Sean Shen
Huawei
4, South 4th Street, Zhongguancun
Beijing 100190
China

Email: shenshuo@cnnic.cn

Yu Mao
H3C Tech. Co., Ltd
Oriental Electronic Bld.
No.2 Chuangye Road
Shang-Di Information Industry
Hai-Dian District
Beijing 100085
China

Email: yumao9@gmail.com

N S Srinivasa Murthy
Freescale Semiconductor
UMA PLAZA, NAGARJUNA CIRCLE, PUNJAGUTTA
HYDERABAD 500082
INDIA

Email: ssmurthy.nittala@freescale.com