MSEC Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 14, 2011

D. McGrew
B. Weis
Cisco Systems

September 10, 2010

Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic

draft-ietf-msec-ipsec-group-counter-modes-06

Abstract

Counter modes have been defined for block ciphers such as the Advanced Encryption Standard (AES). Counter modes use a counter, which is typically assumed to be incremented by a single sender. This memo describes the use of counter modes when applied to the Encapsulating Security Payload (ESP) and Authentication Header (AH) in multiple-sender group applications.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on March 14, 2011.

Copyright Notice

Copyright (c) 2010 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction

The IP Encapsulating Security Payload (ESP) specification [RFC4303] and Authentication Header (AH) [RFC4302] are security protocols for IPsec [RFC4301]. Several new AES encryption modes of operation have been specified for ESP: Counter Mode (CTR) [RFC3686], Galois/Counter Mode (GCM) [RFC4106], Counter with CBC-MAC Mode (CCM) [RFC4309]; and one that has been specified for both ESP and AH: the Galois MAC Mode (GMAC) [RFC4543]. A Camellia counter mode [RFC5528] and a GOST counter mode [RFC4357] have also been specified. These new modes offer advantages over traditional modes of operation. However, they all have restrictions on their use in situations in which multiple senders are protecting traffic using the same key. This document addresses this restriction and describes how these modes can be used with group key management protocols such as the Group Domain of Interpretation (GDOI) protocol [RFC3547] and the Group Secure Association Key Management Protocol (GSAKMP) [RFC4535].

1.1. Requirements notation

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. Problem Statement

The counter mode of operation (CTR) [FIPS.800-38A.2001] has become important because of its performance and implementation advantages. It is the basis for several modes of operation that combine authentication with encryption, including CCM and GCM. All of the counter-based modes require that, if a single key is shared by multiple encryption engines, those engines must coordinate to ensure that every initialization vector (IV) used with that key is distinct. That is, for each key, no IV value can be used more than once. This restriction on IV usage is imposed on ESP CTR, ESP GCM, and ESP CCM. In cryptographic terms, the IV is a nonce. (Note that CBC mode [RFC3602] requires IVs that are unpredictable. CTR, GCM, GMAC, and CCM do not have these restrictions.)

All ESP and AH transforms using a block cipher counter mode have a restriction that an application must not use the same key, IV, and Salt values to protect two different data payloads. Notwithstanding this security condition, block cipher counter mode transforms are often preferred because of their favorable performance characteristics as compared to other modes.

Each of the block cipher counter mode transforms specify the construction of keying material for point-to-point applications which are keyed by the Internet Key Exchange version 2 (IKEv2) [RFC4306]. The specified constructions guarantee that the security condition is not violated by a single sender. Group applications of IPsec [RFC5374] may also find counter mode transforms to be valuable. Some group applications can create a IPsec SA per sender, which meets the security condition, and no further specification is required. However, IPsec can be used to protect group applications known as Many-to-Many Applications [RFC3170], where a single IPsec Security Association (SA) is used to protect network traffic between members of a multiple-sender IP multicast application. Some Many-to-Many Applications are comprised of a large number of senders, in which case defining an individual IPsec SA for each sender is unmanageable.

3. IV formation for Counter Modes with Group Keys

This section specifies a particular construction of the IV that enables a group of senders to safely share a single IPsec SA. This construction conforms to the recommendations of [RFC5116]. A rationale for this method is given in Appendix A. In the construction defined by this specification, each IV is formed by concatenating a Sender Identifier (SID) field with a Sender-Specific IV (SSIV) field. The value of the SID MUST be unique for each sender, across all of the senders sharing a particular Security Association. The value of the SSIV field MUST be unique for each IV constructed by a particular sender for use with a particular SA. The SSIV MAY be chosen in any manner convenient to the sender, e.g. successive values of a counter. The leftmost bits of the IV contain the SID, and the remaining bits contain the SSIV. By way of example, Figure 1 shows the correct placement of an 8-bit SID within an Initialization Vector.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
!      SID      !                                               !
+-+-+-+-+-+-+-+-+                  SSIV                         !
!                                                               !
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-!
```

Figure 1. IV with an 8-bit SID

The number of bits used by the SID may vary depending on group policy, though for each particular Security Association, each SID used with that SA MUST have the same length. To facilitate interoperability, a conforming implementation MUST support SID lengths of 8, 12, and 16 bits. It should be noted that the size of the SID associated with an SA provides a tradeoff between the number of possible senders and the number of packets that each sending station is able to send using that SA.

4. Group Key Management Conventions

Group applications use a Group Key Management System (GKMS) composed of one or more Group Controller Key Server (GCKS) entities [RFC3740]. The GKMS distributes IPsec transform policy and associated keying material to authorized group members. This document RECOMMENDS that the GKMS both allocate unique SIDs to group members and distribute them to group members using a GKM protocol such as GDOI or GSAKMP. The strategy used by the GKMS does not need to be mandated in order to achieve interoperability; the GKMS is solely responsible for allocating SIDs for the group. Allocating SIDs sequentially is acceptable as long as the allocation method follows the requirements in this section.

The following requirements apply to a GKMS that manages SIDs. One example of such a GKMS is [I-D.ietf-msec-gdoi-update].

- For each SA for which sender identifiers are used, the GKMS MUST NOT give the same sender identifier to more than one active group member. If the GKMS is uncertain as to the SID associated with a group member it MUST allocate it a new one. If more than one entity within the GKMS is distributing sender identifiers, then the sets of identifiers distributed by each entity MUST NOT overlap.

- If the entire set of sender identifiers has been exhausted, the GKMS MUST refuse to allow new group members to join. Alternatively, the GKMS could distribute replacement ESP or AH security associations to all group members. When replacement SAs are distributed, the GKMS could also distribute larger SID values so that more senders can be accommodated.

- The GKMS SHOULD allocate a single sender identifier for each group member, and issue this value to the sender for all group SAs for which that member is a sender. This strategy enables both the GKMS and the senders to avoid managing SIDs on a per-SA basis. It also simplifies the rekeying process, since SIDs do not need to be changed or re-issued along with replacement SAs during a rekey event.

- When a GKMS determines that a particular group member is no longer a part of the group, then it MAY re-allocate any sender identifier associated with that group member for use with new group member. In this case, the GKMS MUST first delete and replace any active AH or ESP SAs with which the SID may have been used. This is necessary to avoid re-use of an IV with the cipher key associated with the SA.

5. IANA Considerations

Note to RFC Editor: this section may be removed on publication as an RFC.

This memo has no IANA considerations.

6. Security Considerations

This specification provides a method for securely using cryptographic algorithms that require a unique IV, such as a block cipher mode of operation based on counter mode, in a scenario in which there are multiple cryptographic devices that each generate IVs. This is done by partitioning the set of possible IV values such that each cryptographic device has exclusive use of a set of IV values. When the recommendation in this specification are followed, the security of the cryptographic algorithms is equivalent to the conventional case in which there is a single sender. Unlike CBC mode CTR, GCM, GMAC, and CCM do not require IVs that are unpredictable.

The security of a group depends upon the correct operation of the group members. Any group member using an SID not allocated to it may reduce the security of the system.

As is the case with a single sender, a cryptographic device storing keying material over a reboot is responsible for storing a counter value such that upon resumption it never re-uses counters. In the context of this specification, the cryptographic device would need to store both SID and SSIV values used with a particular IPsec SA in addition to policy associated with the IPsec SA.

A group member that reaches the end of its IV space MUST stop sending data traffic on that SA. This can happen if the group member does not notify the GKMS in time for the GKMS to remedy the problem (e.g., to provide the group member with a new SSID or to provide a new SA), or if the GKMS ignores the notification for some reason. In this case, the group member should re-register with the GCKS and expect to receive the SAs that it needs to continue participating in the group.

This specification does not address virtual machine rollbacks that may cause the cryptographic device to re-use nonce values.

Other security considerations applying to IPsec SAs with multiple senders are described in [RFC5374].

7. Acknowledgements

The authors wish to thank David Black, Sheela Rowles, and Alfred Hoenes for their helpful comments and suggestions.

8. References

8.1. Normative References

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

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, December 2005.

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

8.2. Informative References

[FIPS.800-38A.2001] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation", FIPS PUB 800-38A, December 2001, <http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf>.

[H52] Huffman, D., "A Method for the Construction of Minimum-Redundancy Codes", Proceedings of the IRE, Volume:40, Issue:9, On page(s): 1098-1101, ISSN: 0096-8390, September 1952, <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4051119>.

[I-D.ietf-msec-gdoi-update] Weis, B., Rowles, S., and T. Hardjono, "The Group Domain of Interpretation", draft-ietf-msec-gdoi-update-06 (work in progress), July 2010.

[RFC3170] Quinn, B. and K. Almeroth, "IP Multicast Applications: Challenges and Solutions", RFC 3170, September 2001.

[RFC3547] Baugher, M., Weis, B., Hardjono, T., and H. Harney, "The Group Domain of Interpretation", RFC 3547, July 2003.

[RFC3602] Frankel, S., Glenn, R., and S. Kelly, "The AES-CBC Cipher Algorithm and Its Use with IPsec", RFC 3602, September 2003.

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

[RFC3740] Hardjono, T. and B. Weis, "The Multicast Group Security Architecture", RFC 3740, March 2004.

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, January 2005.

[RFC4106] Viega, J. and D. McGrew, "The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)", RFC 4106, June 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

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

[RFC4309] Housley, R., "Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP)", RFC 4309, December 2005.

[RFC4357] Popov, V., Kurepkin, I., and S. Leontiev, "Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms", RFC 4357, January 2006.

[RFC4535] Harney, H., Meth, U., Colegrove, A., and G. Gross, "GSAKMP: Group Secure Association Key Management Protocol", RFC 4535, June 2006.

[RFC4543] McGrew, D. and J. Viega, "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

[RFC5116] McGrew, D., "An Interface and Algorithms for Authenticated Encryption", RFC 5116, January 2008.

[RFC5374] Weis, B., Gross, G., and D. Ignjatic, "Multicast Extensions to the Security Architecture for the Internet Protocol", RFC 5374, November 2008.

[RFC5528] Kato, A., Kanda, M., and S. Kanno, "Camellia Counter Mode and Camellia Counter with CBC-MAC Mode Algorithms", RFC 5528, April 2009.

Appendix A. Rationale for the IV formation for Counter Modes with Group Keys

The two main alternatives for ensuring the uniqueness of IVs in a multi-sender environment are to have each sender include a Sender Identifier (SID) value in either the Salt value or in the explicit IV field (recall that the IV used as input to the crypto algorithm is constructed by concatenating the Salt and the explicit IV). The explicit IV field was chosen as the location for the SID because it is explicitly present in the packet. If the SID had been included in the Salt, then a receiver would need to infer the SID value for a particular AH or ESP packet by recognizing which sender had sent that packet. This inference could be made on the IP source address, if AH or ESP is transported directly over IP. However, if an alternate transport mechanism such as UDP is being used [RFC3948] (e.g. for NAT traversal), the method used to infer the sender would need to take that mechanism into account. It is simpler to use the explicit IV field, and thus avoid the need to infer the sender from the packet at all.

The normative requirement that all of the SID values used with a particular Security Association must have the same length is not strictly necessary, but was added to promote simplicity of implementation. Alternatively, it would be acceptable to have the SID values be chosen to be the codewords of a variable-length prefix free code. This approach preserves security since the distinctness of the IVs follows from the fact that no SID is a prefix of another; thus any pair of IVs has a subset of bits that are distinct. If a Huffman code [H52] is used to form the SIDs, then a set of optimal SIDs can be found, in the sense that the number of SIDs can be maximized for a given distribution of SID lengths. Additionally, there are simple methods for generating efficient prefix free codes whose codewords are octet strings. Nevertheless, these methods were disallowed in order to favor simplicity over generality.

Appendix B. Example

This section provides an example of SID allocation and IV generation, as defined in this document. A GCKS administrator determines that the group has one SA that is shared by all senders. The algorithm for the SA is AES-GCM using an SID of size 8 bits.

When the first sender registers with the GCKS, it is allocated SID 1. The sender subsequently sends AES-GCM encrypted packets with the following IVs (shown in network byte order): 0x0100000000000001, 0x0100000000000002, 0x0100000000000003, ... with a final value of 0x01FFFFFFFFFFFFFF. The second sender registering with the GCKS is allocated SID 2, and begins sending packets with the following IVs: 0x0200000000000001, 0x0200000000000002, 0x0200000000000003, ... with a final value of 0x02FFFFFFFFFFFFFF.

According to group policy, the GCKS may later distribute policy and keying material for a replacement SA. When group senders begin sending AES-GCM packets encrypted with the new SA each sender continues to use the SID value previously allocated to it. For example, the sender allocated SID 2 would being sending on a new SA with IV values of 0x0200000000000001, 0x0200000000000002, 0x0200000000000003, ... with a final value of 0x02FFFFFFFFFFFFFF.

Authors' Addresses

David A. McGrew
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-525-8651
Email: mcgrew@cisco.com

Brian Weis
Cisco Systems
170 W. Tasman Drive
San Jose, California 95134-1706
USA

Phone: +1-408-526-4796
Email: bew@cisco.com