Network Working Group
Internet Draft
Intended status: Informational
Expires: Dec 28, 2010

K. Grewal
Intel Corporation
M. Long
Intel Corporation

June 28, 2010

AES-GCM using two independent keys
draft-grewal-aes-gcm-bifurcated-key-00.txt

Status of this Memo

Copyright Notice

Abstract

This document describes modifications to the AES-GCM algorithm to allow separation of the data authenticity and data confidentiality keys, while preserving the performance benefits

such as IPsec and TLS, separation of these keys allows the data confidentiality key to be shared with trusted intermediary nodes on the network, while preserving the data authenticity functions in an end-to-end manner. The current definition of AES-GCM uses a single key for confidentiality and authenticity hence it is not possible to share the key with trusted network nodes, without compromising the data authenticity functions.

Table of Contents

1. Introduction

AES-GCM is a combined mode algorithm [GCM], that is widely used in network security protocols such as IPsec ESP [rfc4106] and TLS [rfc5288], among other usages where high speed operation is of paramount importance. The algorithm leverages a single key to provide data confidentiality and integrity for these network security protocols. Enterprises using network security protocols are often faced with a conflicting requirement of employing network security protocol and maintaining the working operation of network management tools, which are blind to the payload when encryption is employed. This draft introduces modifications to the AES-GCM algorithm to employ two independent keys, one for data confidentiality and another for data integrity. This 'bifurcated key' approach allows sharing the data confidentiality key with authorized network appliances, while preserving the end-to-end data integrity of the payload.

1.1. Requirements Language

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 [RFC2119].

1.2. Applicability Statement

The document describes modifications to the AES-GCM algorithm in order to leverage two discrete keys for data confidentiality and data authenticity, while preserving a single parse operation over the input data for performance benefits. The existing definition of AES-GCM leverages a single key for both data confidentiality and data authenticity.

AES-GCM has many different usage cases but the primary usage today is within network security protocols such as IPsec and TLS. To enable deployment of these protocols within an Enterprise environment, it is sometimes desirable to provide traffic visibility for existing network functions such as intrusion detection / protection systems (IDS/IPS), auditing and networking monitoring tools. Data encryption provided by network security protocols works against these existing network management tools, which require visibility into the clear text payload of a given network datagram. This can be achieved with legacy discrete mode cryptographic algorithms (e.g. AES, SHA-1) by sharing the data confidentiality key with the network appliance, while keeping the data authenticity key a secret between the end-to-end communicating nodes. For high speed networks operating at 10Gbps and beyond, combined mode algorithms such as AES-GCM are employed due to their greater efficiency, primarily due to a single pass operation over the datagram. However, the data visibility requirements for intermediary network nodes is incompatible with GCM mode's optimizations for high speed operation, as it is not possible to share the single AES-GCM key with the network nodes without compromising data authenticity assertions (the intermediary network node has the ability to modify the packet without detection by the recipient node). To overcome this, we define a hybrid mode of operation for AES-GCM, where we define separate data confidentiality and data authenticity keys, while

preserving the performance benefits of the combined mode algorithm.

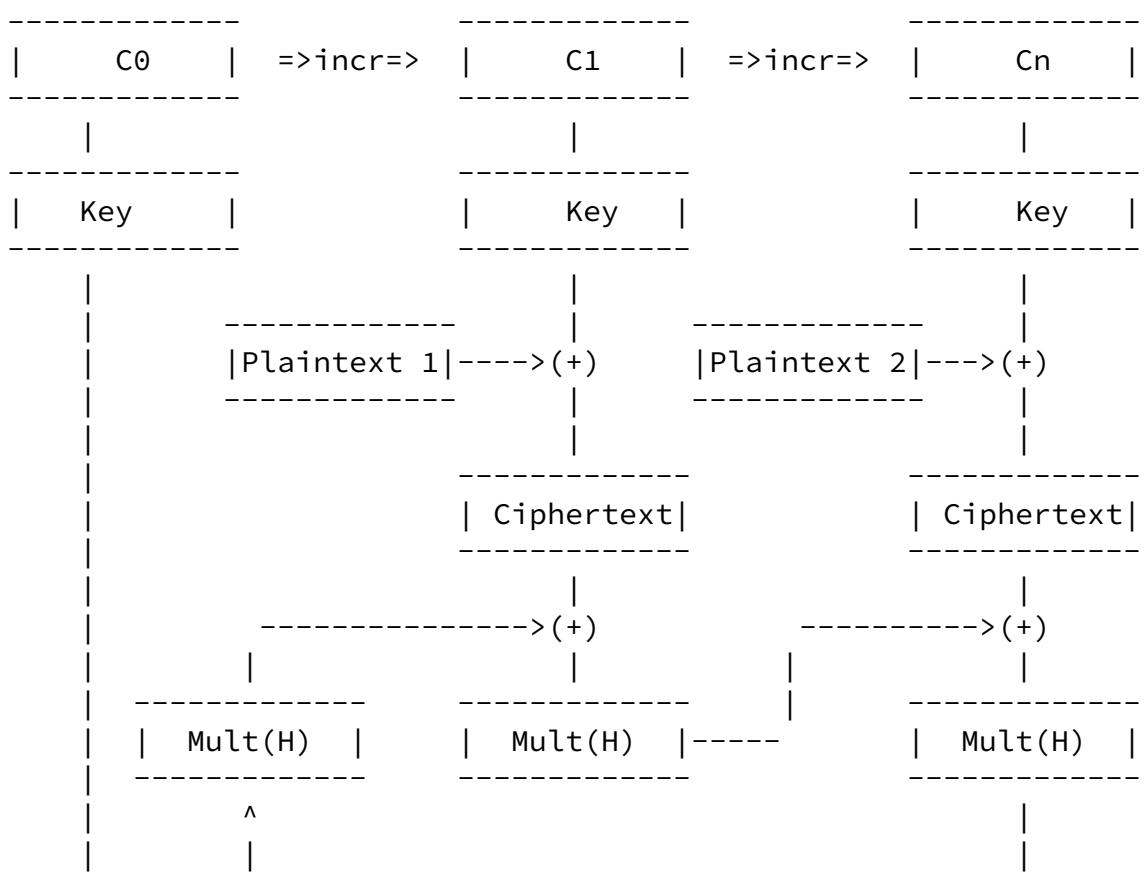
2. AES-GCM

AES-GCM is defined under NIST [GCM] as a combined mode algorithm providing data confidentiality and integrity. Furthermore, operation of this algorithm within network security protocols

such as IPsec and TLS can be found in RFC 4106 and RFC 5288 respectively.

2.1. AES-GCM using a single key

The high level operation of AES-GCM can be depicted as follows:



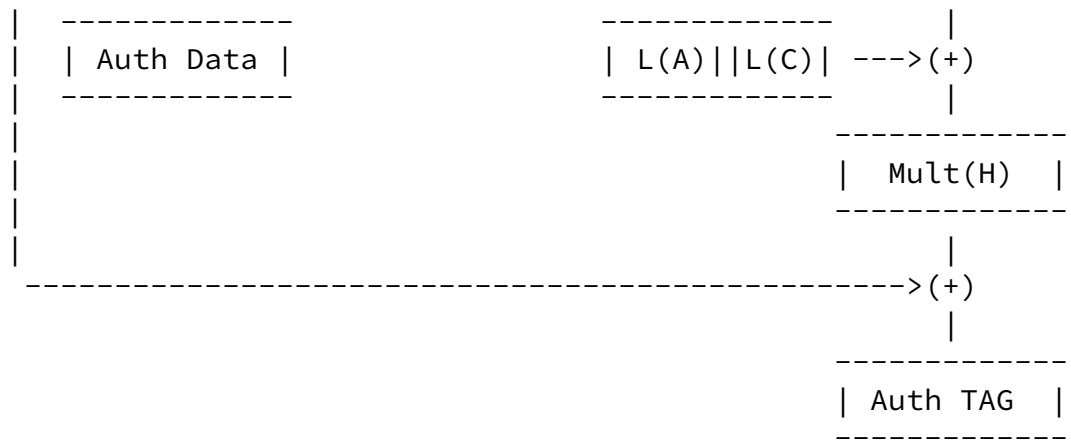


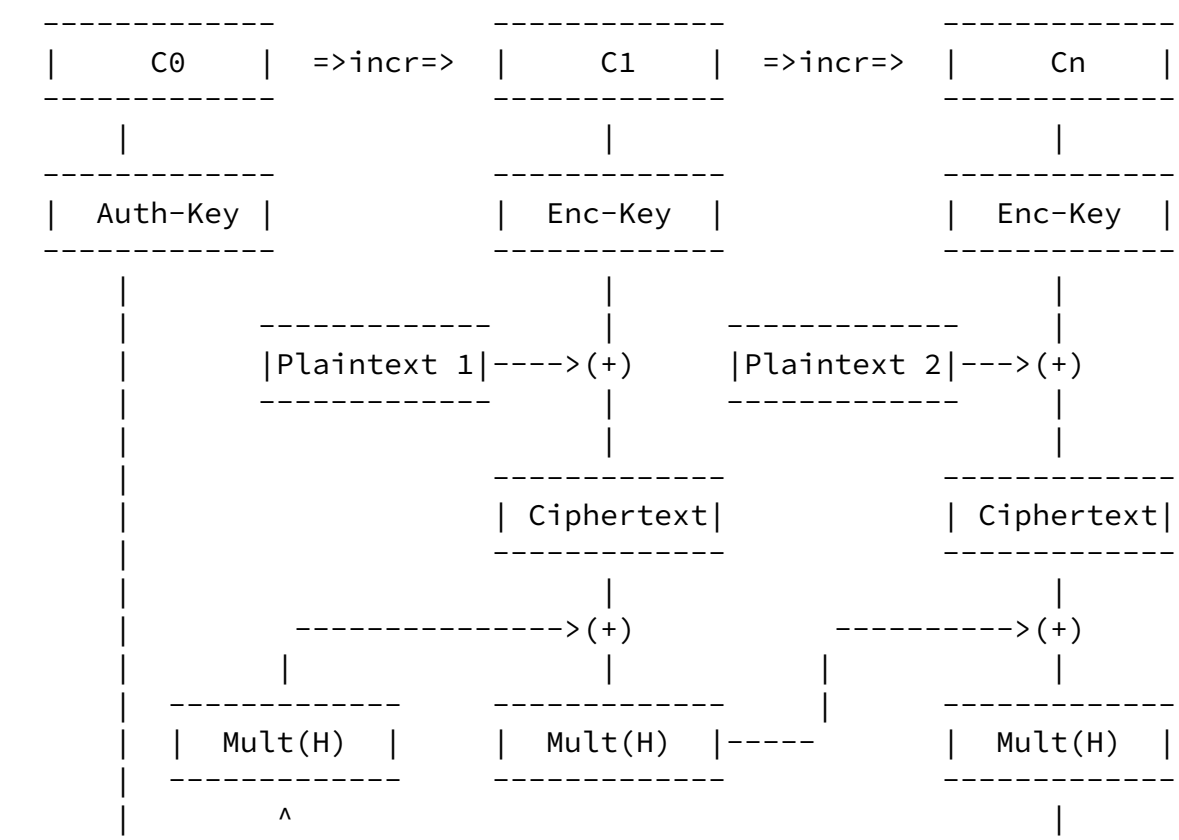
Figure 1 AES-GCM Operation Today

In this diagram, a high level view of the counter mode of AES with GCM is described, where each incremental counter value is encrypted

using the AES-GCM key and subsequently XOR'ed with the plain text to compute the cipher text. Mult(H) is the multiplication in the finite field of GF(2^128), where H is the secret value that is derived by AES(Key, 0..0). Each subsequent Mult(H) value is computed from the previous blocks Mult(H) value XORed with the ciphertext. This is repeated for all data blocks in the input data stream until a Mult(H) value for the last data block is computed. This value is then XOR'ed with the length fields of the input data, as well as the length of any additional authentication data (AAD), which does not require confidentiality protection, but does require data authenticity. Additionally, the value is again XOR'ed with the encrypted counter 0 value to produce the authentication tag for the packet. For additional details on these operations, refer to the NIST specification on AES-GCM.

2.2. AES-GCM using Bifurcated Keys

Bifurcated key means that two discrete keys are used for data confidentiality and integrity, instead of a single key as defined in AES-GCM. The algorithm diagram for AES-GCM using bifurcated keys can be depicted as follows:


C0
=>incr=>
C1
=>incr=>
Cn
Auth-Key
Enc-Key
Enc-Key
Plaintext 1
Plaintext 2
Ciphertext
Ciphertext
Mult(H)
Mult(H)
Mult(H)

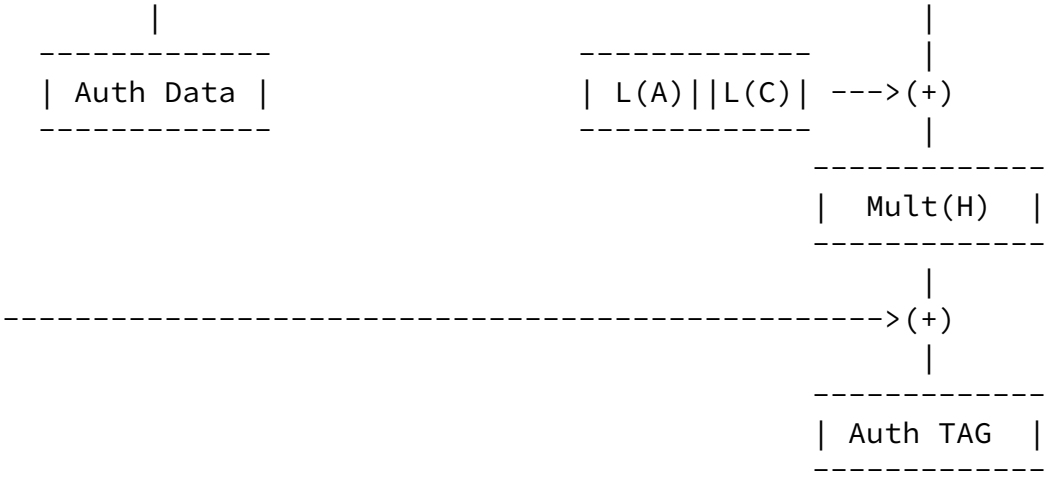


Figure 2 Bifurcated Key AES-GCM Operation

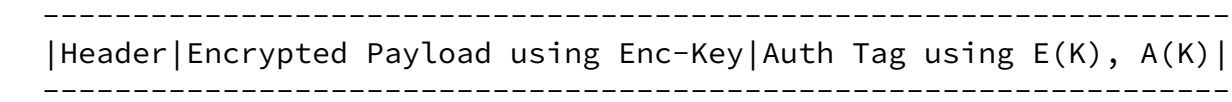
The notable difference between this approach and the standard definition of AES-GCM is the use of two independent keys (one for data encryption and the other for data authenticity). In the most part, the encryption key is unchanged and can be viewed as equivalent to the single key as used in standard AES-GCM. In this context we label the original AES-GCM 'Key' as the encryption key, Enc-Key, and introduce a separate key for data authenticity, denoted as Auth-Key. The encryption key is used for all counter values C1 to Cn, where C1 is encrypted with the encryption key and the resultant data XORed with the first plaintext block and Cn counter value is encrypted with the

encryption key and XORed with the last plaintext block in order to produce the cipher text for a given block of plaintext.

The authentication key is used to encrypt the first counter value C0 and the resultant data is XORed with the last block in generation of the final authentication tag.

Mult(H) is the multiplication in the finite field of GF(2^128), where H is the secret value that is derived by AES(Auth-Key, 0..0). Note that the Auth-Key is used in the generation of H. This composition ensures that the AES encryption computation can be performed independently with the finite field multiplication for the authentication tag.

Packet Applicability: Using the bifurcated key approach, a generic packet requiring data confidentiality and integrity can be depicted as follows:



2.3. Using AES-GCM bifurcated keys in security protocols

AES-GCM using a bifurcated key can be employed within the existing network security protocols such as IPsec and TLS with small modifications. These modifications pertain to the algorithm value that is negotiated via the control channel handshake of a protocol and defines the data path usage of the bifurcated key based AES-GCM. The modifications needed for a control channel handshake to generate independent keys for data confidentiality and data authenticity are outside the scope of this document and can be defined in protocol specific documents.

3. Security Considerations

The security analysis of the AES-GCM algorithm is part of the original AES-GCM NIST specification. The key generation process needs to employ well reviewed cryptographic techniques to provide two independent keys for AES-GCM. The key generation process is outside the scope of this specification. We believe the partitioning of the two key constructs has preserved the security property as the security is analyzed on the encryption and authentication path, respectively.

4. IANA Considerations

There are no IANA considerations, as allocation of an algorithm ID for this bifurcated key approach can be defined in a separate draft, together with the application of this algorithm within a given network security protocol.

5. Acknowledgments

The authors would like to acknowledge the following people for their feedback on updating the definitions in this document.

David McGrew, Jesse Walker, David Durham.

This document was prepared using 2-Word-v2.0.template.doc.

6. References

6.1. Normative References

[GCM] McGrew, D. and J. Viega, "The Galois/Counter Mode of Operation (GCM)", Submission to NIST. http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/gcm/gcm-spec.pdf, January 2004.

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

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

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

[RFC5288] McGrew, D. and Viega J., "The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH", RFC 4543, May 2006.

[RFC5226] Narten, T., Alverstrand, H., "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, May 2008.

6.2. Informative References

Author's Addresses

Ken Grewal
Intel Corporation
2111 NE 25th Avenue, JF3-232
Hillsboro, OR 97124
USA

Phone:
Email: ken.grewal@intel.com

Men long
Intel Corporation
2111 NE 25th Avenue, JF3-232
Hillsboro, OR 97124
USA

Phone:
Email: men.long@intel.com