Network Working Group
Internet Draft
Intended Status: Informational
Expires: December 27, 2008

K.M. Igoe
National Security Agency
J.A. Solinas
National Security Agency
June 27, 2008

AES Galois Counter Mode for the Secure Shell Transport Layer Protocol
draft-igoe-secsh-aes-gcm-00

Status of this Memo

Copyright Notice

Abstract

Secure Shell (SSH) [RFC4251] is a secure remote-login protocol. SSH provides for algorithms that provide authentication , key agreement. confidentiality and data integrity services. This purpose of this document is to show how the AES Galois/Counter Mode can be used to provide both confidentiality and data integrity.

Table of Contents

1. Introduction.....1
2. Requirements Terminology.....1
3. Applicability Statement.....1
4. Two New AEAD Algorithms.....1
4.1. aead-aes-128-gcm-ssh.....2
4.2. aead-aes-256-gcm-ssh.....2
5. Size of the Message Authentication Code.....2
6. Maximum Payload Size.....3
7. Linkage of Confidentiality and Data Integrity.....3
8. Security Considerations.....3
9. IANA Considerations.....4
10. References.....4
10.1. Normative References.....4

1. Introduction

Galois/Counter Mode (GCM) is a block cipher mode of operation that provides both confidentiality and data integrity services. The purpose of this document is to show how AES-GCM can be intergrated into the Secure Shell Transport Layer Protocol.

2. Requirements Terminology

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].

3. Applicability Statement

Using AES-GCM to provide both confidentiality and data integrity is generally more efficient than using two separate algorithms to provide these security services.

4. Two New AEAD Algorithms

4.1. aead-aes-128-gcm-ssh

aead-aes-128-gcm-ssh is a variant of the algorithm AEAD_AES_128_GCM specified in section 5.1 of [RFC5116]. The only differences between the two algorithms are in the input and output lengths. Using the notation defined in [RFC5116], the input and output lengths for aead-aes-128-gcm-ssh are as follows:

PARAMETER	Meaning	Value
K_LEN	AES key length	16 octets
P_MAX	maximum plaintext length	2^32 octets
A_MAX	maximum additional authenticated data length	0 octets
N_MIN	minimum nonce (IV) length	12 octets
N_MAX	maximum nonce (IV) length	12 octets
C_MAX	maximum cipher length	2^32 octets

Test cases are provided in the appendix of [GCM].

The reader is reminded that due to the presence of length fields and padding in SSH packets, the plaintext length is not the same as the payload length. See section 6 below.

4.2. aead-aes-256-gcm-ssh

aead-aes-256-gcm-ssh is a variant of the algorithm AEAD_AES_256_GCM specified in section 5.2 of [RFC5116]. The only differences between the two algorithms are in the input and output lengths. Using the notation defined in [RFC5116], the input and output lengths for aead-aes-256-gcm-ssh are as follows:

PARAMETER	Meaning	Value
K_LEN	AES key length	32 octets
P_MAX	maximum plaintext length	2^32 octets
A_MAX	maximum additional authenticated data length	0 octets
N_MIN	minimum nonce (IV) length	12 octets
N_MAX	maximum nonce (IV) length	12 octets
C_MAX	maximum cipher length	2^32 octets

Test cases are provided in the appendix of [GCM].

The reader is reminded that due to the presence of length fields and padding in SSH packets, the plaintext length is not the same as the payload length. See section 6 below.

5. Size of the Message Authentication Code

Both aead-aes-128-gcm-ssh and aead-aes-256-gcm-ssh produce a 16-octet message authentication code. ([RFC5116] calls this an "authentication tag" rather than a "message authentication code".)

6. Maximum Payload Size

The value of P_MAX and C_MAX listed above are determined by constraints on the structure of an SSH packet. Referring to [RFC 4253], one finds that an SSH packet consists of five fields:

```
uint32    packet_length;  // 0 <= packet_length < 2^32
byte      padding_length; // 4 <= padding_length < 256
byte[n1]  payload;        // n1 = packet_length - padding_length - 1
byte[n2]  random_padding; // n2 = padding_length
byte[m]   mac;            // m  = mac_length
                             (= 16 for aes128/256_gcm)
```

All save the mac field are encrypted, and the total length of the data to be encrypted (plaintext length) must be a multiple of the block length. When using either aead-aes-128-gcm-ssh or aead-aes-256-gcm-ssh (or any other algorithm with either a 16 octet or 8 octet block size) the largest possible payload is achieved when

```
payload length   = 2^32-9 octets
padding length   = 4 octets
packet length    = 1 + (2^32-9) + 4 = 2^32 - 4 octets
plaintext length = 4 + 1 + (2^32 - 9) + 4 = 2^32 octets.
```

7. Linkage of Confidentiality and Data Integrity

When either aead-aes-128-gcm-ssh or aead-aes-256-gcm-ssh is being employed it SHOULD be used both as the confidentiality mechanism and as the data integrity mechanism.

8. Security Considerations

The security considerations in [RFC4251] apply.

9. IANA Considerations

IANA will add the following two entries to the AEAD Registry described in [RFC5116]:

Name	Reference	Proposed Numeric Identifier
aead-aes-128-gcm-ssh	Section 4.1	5
aead-aes-256-gcm-ssh	Section 4.2	6

IANA will add the following two entries to the Secure Shell Encryption Algorithm name Registry described in [RFC4250]:

Name	Reference
aead-aes-128-gcm-ssh	Section 4.1
aead-aes-256-gcm-ssh	Section 4.2

IANA will add the following two entries to the Secure Shell MAC Algorithm name Registry described in [RFC4250]:

Name	Reference
aead-aes-128-gcm-ssh	Section 4.1
aead-aes-256-gcm-ssh	Section 4.2

10. References

10.1. Normative References

[GCM] Dworkin, M, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC", NIST Special Publication 800-30D, November 2007.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4250] Lehtinen, S. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Assigned Numbers", RFC 4250, January 2006.

[RFC4251] Ylonen, T. and C. Lonvick, Ed., "The Secure Shell (SSH) Protocol Architecture", RFC 4251, January 2006.

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

Author's Addresses

Kevin M. Igoe
NSA/CSS Commercial Solutions Center
National Security Agency
EMail: kmigoe@nsa.gov

Jerome A. Solinas
National Information Assurance Research Laboratory
National Security Agency
EMail: jasolin@orion.ncsc.mil

Trademark Notice

"SSH" is a registered trademark in the United States.

Full Copyright Statement

Intellectual Property

Acknowledgement

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