Network Working Group
Internet Draft
Intended Status: Informational
Expires: April 22, 2013

K. Burgin
National Security Agency
M. Peck
The MITRE Corporation
October 19, 2012

AES Encryption with HMAC-SHA2 for Kerberos 5
draft-burgin-kerberos-aes-cbc-hmac-sha2-02

Abstract

This document specifies two encryption types and two corresponding checksum types for Kerberos 5. The new types use AES in CBC mode with ciphertext stealing for confidentiality and HMAC with a SHA-2 hash for integrity.

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 February 21, 2013.

Copyright and License Notice

Table of Contents

1. Introduction

This document defines two encryption types and two corresponding checksum types for Kerberos 5 using AES with 128-bit or 256-bit keys. The new types conform to the framework specified in [RFC3961], but do not use the simplified profile.

The new encryption types use AES in CBC mode with ciphertext stealing similar to [RFC3962] but with several variations.

The new types use the PBKDF2 algorithm for key generation from strings, with a modification to the use in [RFC3962] that the hash algorithm in the pseudorandom function used by PBKDF2 will be SHA-256 instead of SHA-1.

The new types use key derivation to produce keys for encryption, integrity protection, and checksum operations as in [RFC3962]. However, a key derivation function from [SP800-108] which uses the SHA-256 or SHA-384 hash algorithm is used in place of the DK key derivation function used in [RFC3961].

The new types use the HMAC algorithm with a hash from the SHA-2 family for integrity protection and checksum operations.

2. 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 RFC 2119 [RFC2119].

3. Protocol Key Representation

The AES key space is dense, so we can use random or pseudorandom octet strings directly as keys. The byte representation for the key is described in [FIPS197], where the first bit of the bit string is the high bit of the first byte of the byte string (octet string).

4. Key Generation from Pass Phrases

We use a variation on the key generation algorithm specified in Section 4 of [RFC3962] with the following changes:

* The pseudorandom function used by PBKDF2 will be the SHA-256 HMAC of the passphrase and salt, instead of the SHA-1 HMAC of the passphrase and salt. The salt SHOULD contain at least 128 random bits as recommended in [SP800-132]. It MAY also contain other information such as the principal's realm and name components.

* The final key derivation step uses the algorithm KDF-HMAC-SHA2 defined below in Section 5 instead of the DK function.

* If no string-to-key parameters are specified, the default number of iterations is raised to 32,768.

To ensure that different long-term keys are used with different enctypes, we prepend the enctype name to the salt string, separated by a null byte. The enctype name is "aes128-cts-hmac-sha256-128" or "aes256-cts-hmac-sha384-192" (without the quotes). The user's long-term key is derived as follows

```
saltp = enctype-name | 0x00 | salt
tkey = random-to-key(PBKDF2(passphrase, saltp,
                            iter_count, keylength))
key = KDF-HMAC-SHA2(tkey, "kerberos") where "kerberos" is the
      byte string {0x6b 0x65 0x72 0x62 0x65 0x72 0x6f 0x73}.
```

where the pseudorandom function used by PBKDF2 is the SHA-256 HMAC of the passphrase and salt, the value for keylength is the AES key length, and the algorithm KDF-HMAC-SHA2 is defined in Section 5.

5. Key Derivation Function

We use a key derivation function from Section 5.1 of [SP800-108] which uses the HMAC algorithm as the PRF. The counter i is expressed as four octets in big-endian order. The length of the output key in bits (denoted as k) is also represented as four octets in big-endian order. The "Label" input to the KDF is the usage constant supplied to the key derivation function, and the "Context" input is null.

When the encryption type is aes128-cts-hmac-sha256-128:

```
n = 1
K1 = HMAC-SHA-256(key, 00 00 00 01 | constant | 0x00 | 00 00 00 80)
DR(key, constant) = First 128 bits of K1
KDF-HMAC-SHA2(key, constant) = random-to-key(DR(key, constant))
```

When the encryption type is aes256-cts-hmac-sha384-192:

```
n = 1
K1 = HMAC-SHA-384(key, 00 00 00 01 | constant | 0x00 | 00 00 01 00)
DR(key, constant) = First 256 bits of K1
KDF-HMAC-SHA2(key, constant) = random-to-key(DR(key, constant))
```

6. Kerberos Algorithm Protocol Parameters

The following parameters apply to the encryption types aes128-cts-hmac-sha256-128 and aes256-cts-hmac-sha384-192.

The key-derivation function described in the previous section is used to produce the three intermediate keys. Typically, CBC mode [SP800-38A] requires the input be padded to a multiple of the encryption algorithm block size, which is 128 bits for AES. However, to avoid ciphertext expansion, we use the CBC-CS3 variant to CBC mode defined in [SP800-38A+].

Each encryption will use a freshly generated 16-octet nonce generated at random by the message originator. The initialization vector (IV) used by AES is obtained by xoring the random nonce with the cipherstate.

The ciphertext is the concatenation of the random nonce, the output of AES in CBC-CS3 mode, and the HMAC of the initialization vector concatenated with the AES output. The HMAC is computed using either SHA-256 or SHA-384. The output of SHA-256 is truncated to 128 bits and the output of SHA-384 is truncated to 192 bits. Sample test vectors are given in Appendix A.

Decryption is performed by removing the HMAC, verifying the HMAC against the remainder, and then decrypting the remainder if the HMAC is correct.

The encryption and checksum mechanisms below use the following notation from [RFC3961].

HMAC output size, h
message block size, m
encryption/decryption functions, E and D
cipher block size, c

Encryption Mechanism for AES-CBC-HMAC-SHA2

protocol key format	128- or 256-bit string
specific key structure	Three protocol-format keys: { Kc, Ke, Ki }.
required checksum mechanism	As defined below.
key-generation seed length	key size (128 or 256 bits)

cipher state	Random nonce of length c (128 bits)
initial cipher state	All bits zero

encryption function	N = random nonce of length c (128 bits)
	IV = N + cipherState (+ denotes XOR)
	C = E(Ke, plaintext, IV)
	  using CBC-CS3-Encrypt defined
	  in [SP800-38A+]
	H = HMAC(Ki, N | C)
	ciphertext = N | C | H[1..h]
	cipherState = N

decryption function	(N, C, H) = ciphertext
	if (H != HMAC(Ki, N | C)[1..h])
	  stop, report error
	IV = N + cipherState (+ denotes XOR)
	P = D(Ke, C, IV)
	  using CBC-CS3-Decrypt defined
	  in [SP800-38A+]
	cipherState = N

pseudo-random function	Kp = KDF-HMAC-SHA2(protocol-key, "prf") PRF = HMAC(Kp, octet-string)
key generation functions:	

string-to-key function	tkey = random-to-key(PBKDF2(passphrase, saltp,
	  iter_count,
	  keylength))
	base-key = KDF-HMAC-SHA2(tkey, "kerberos")
	
	where the pseudorandom function used by PBKDF2
	is the SHA-256 HMAC of the passphrase and salt

default string-to-key parameters	00 00 80 00
random-to-key function	identity function
key-derivation function	KDF-HMAC-SHA2 as defined in Section 5. The key usage number is expressed as four octets in big-endian order. Kc = KDF-HMAC-SHA2(base-key, usage | 0x99) Ke = KDF-HMAC-SHA2(base-key, usage | 0xAA) Ki = KDF-HMAC-SHA2(base-key, usage | 0x55);

Checksum Mechanism for AES-CTS-HMAC-SHA2	
associated cryptosystem	AES-128-CBC or AES-256-CBC as appropriate
get_mic	HMAC(Kc, message)[1..h]
verify_mic	get_mic and compare

Using this profile with each key size gives us two each of encryption and checksum algorithm definitions.

encryption types		
type name	etype value	key size
aes128-cts-hmac-sha256-128	TBD1	128
aes256-cts-hmac-sha384-192	TBD2	256

checksum types		
type name	sumtype value	length
hmac-sha256-128-aes128	TBD3	128
hmac-sha384-192-aes256	TBD4	192

These checksum types will be used with the corresponding encryption types defined above.

7. IANA Considerations

IANA is requested to assign:

1. Encryption type numbers for aes128-cts-hmac-sha256-128 and aes256-cts-hmac-sha384-192 in the Kerberos Encryption Type Numbers registry.

Etype	encryption type	Reference
TBD1	aes128-cts-hmac-sha256-128	[I.D.burgin-kerberos-aes-cbc-hmac-sha2]
TBD2	aes256-cts-hmac-sha384-192	[I.D.burgin-kerberos-aes-cbc-hmac-sha2]

2. Checksum type numbers for hmac-sha256-128-aes128 and hmac-sha384-

192-aes256 in the Kerberos Checksum Type Numbers registry.

Sumtype	Checksum type	Size	Reference
TBD3	hmac-sha256-128-aes128	16	[I.D.burgin-kerberos-aes-cbc-hmac-sha2]
TBD4	hmac-sha384-192-aes256	24	[I.D.burgin-kerberos-aes-cbc-hmac-sha2]

8. Security Considerations

This specification requires implementations to generate random values. The use of inadequate pseudo-random number generators (PRNGs) can result in little or no security. The generation of quality random numbers is difficult. NIST Special Publication 800-90 [SP800-90] and [RFC4086] offer random number generation guidance.

This document specifies a mechanism for generating keys from pass phrases or passwords. The salt and iteration count resist brute force and dictionary attacks, however, it is still important to choose or generate strong passphrases.

9. References

9.1. Normative References

[SP800-38A+] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode", Addendum to NIST Special Publication 800-38A, October 2010.

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

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, February 2005.

[RFC3962] Raeburn, K., "Advanced Encryption Standard (AES) Encryption for Kerberos 5", RFC 3962, February 2005.

[RFC4086] Eastlake 3rd, D., Schiller, J., and S. Crocker, "Randomness Requirements for Security", BCP 106, RFC 4086, June 2005.

[FIPS197] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)", FIPS PUB 197, November 2001.

9.2. Informative References

[SP800-38A] National Institute of Standards and Technology, "Recommendation for Block Cipher Modes of Operation - Methods and Techniques", NIST Special Publication 800-38A, February 2001.

[SP800-90] National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), NIST Special Publication 800-90, March 2007.

[SP800-108] National Institute of Standards and Technology, "Recommendation for Key Derivation Using Pseudorandom Functions", NIST Special Publication 800-108, October 2009.

[SP800-132] National Institute of Standards and Technology, "Recommendation for Password-Based Key Derivation, Part 1: Storage Applications", NIST Special Publication 800-132, June 2010.

Appendix A. AES-CBC Test Vectors

TBD

Authors' Addresses

Kelley W. Burgin
National Security Agency

EMail: kwburgi@tycho.ncsc.mil

Michael A. Peck
The MITRE Corporation

EMail: mpeck@mitre.org