Internet Engineering Task Force (IETF)
Request for Comments: 7630
Category: Standards Track
ISSN: 2070-1721

J. Merkle, Ed.
Secunet Security Networks
M. Lochter
BSI

October 2015

HMAC-SHA-2 Authentication Protocols in the User-based Security Model (USM) for SNMPv3

Abstract

This memo specifies new HMAC-SHA-2 authentication protocols for the User-based Security Model (USM) for SNMPv3 defined in RFC 3414.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7630.

Copyright Notice

Table of Contents

1. Introduction 2
2. The Internet-Standard Management Framework 3
3. Conventions 3
4. The HMAC-SHA-2 Authentication Protocols 3
4.1. Deviations from the HMAC-SHA-96 Authentication Protocol . 4
4.2. Processing 5
4.2.1. Processing an Outgoing Message 5
4.2.2. Processing an Incoming Message 6
5. Key Localization and Key Change 6
6. Structure of the MIB Module 6
7. Relationship to Other MIB Modules 7
7.1. Relationship to SNMP-USER-BASED-SM-MIB 7
7.2. Relationship to SNMP-FRAMEWORK-MIB 7
7.3. MIB Modules Required for IMPORTS 7
8. Definitions 7
9. Security Considerations 9
9.1. Use of the HMAC-SHA-2 Authentication Protocols in USM . . 9
9.2. Cryptographic Strength of the Authentication Protocols . 9
9.3. Derivation of Keys from Passwords 10
9.4. Access to the SNMP-USM-HMAC-SHA2-MIB 11
10. IANA Considerations 11
11. References 12
11.1. Normative References 12
11.2. Informative References 13
Authors' Addresses 14

1. Introduction

This memo defines a portion of the Management Information Base (MIB) for use with network management protocols. In particular, it defines additional authentication protocols for the User-based Security Model (USM) for the Simple Network Management Protocol version 3 (SNMPv3) specified in RFC 3414 [RFC3414].

In RFC 3414, two different authentication protocols, HMAC-MD5-96 and HMAC-SHA-96, are defined based on the hash functions MD5 and SHA-1, respectively. This memo specifies new HMAC-SHA-2 authentication protocols for USM using a Hashed Message Authentication Code (HMAC) based on the SHA-2 family of hash functions [SHA] and truncated to 128 bits for SHA-224, to 192 bits for SHA-256, to 256 bits for SHA-384, and to 384 bits for SHA-512. These protocols are straightforward adaptations of the authentication protocols HMAC-MD5-96 and HMAC-SHA-96 to the SHA-2-based HMAC.

2. The Internet-Standard Management Framework

For a detailed overview of the documents that describe the current Internet-Standard Management Framework, please refer to section 7 of RFC 3410 [RFC3410].

Managed objects are accessed via a virtual information store, termed the Management Information Base or MIB. MIB objects are generally accessed through the Simple Network Management Protocol (SNMP). Objects in the MIB are defined using the mechanisms defined in the Structure of Management Information (SMI). This memo specifies a MIB module that is compliant to the SMIv2, which is described in STD 58, RFC 2578 [RFC2578], STD 58, RFC 2579 [RFC2579] and STD 58, RFC 2580 [RFC2580].

3. Conventions

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 BCP 14, RFC 2119 [RFC2119].

4. The HMAC-SHA-2 Authentication Protocols

This section describes the HMAC-SHA-2 authentication protocols, which use the SHA-2 hash functions (described in FIPS PUB 180-4 [SHA] and RFC 6234 [RFC6234]) in the HMAC mode (described in RFC 2104 [RFC2104] and RFC 6234), truncating the output to 128 bits for SHA-224, 192 bits for SHA-256, 256 bits for SHA-384, and 384 bits for SHA-512. RFC 6234 also provides source code for all the SHA-2 algorithms and HMAC (without truncation). It also includes test harness and standard test vectors for all the defined hash functions and HMAC examples.

The following protocols are defined:

usmHMAC128SHA224AuthProtocol: uses SHA-224 and truncates the output to 128 bits (16 octets);

usmHMAC192SHA256AuthProtocol: uses SHA-256 and truncates the output to 192 bits (24 octets);

usmHMAC256SHA384AuthProtocol: uses SHA-384 and truncates the output to 256 bits (32 octets);

usmHMAC384SHA512AuthProtocol: uses SHA-512 and truncates the output to 384 bits (48 octets).

Implementations conforming to this specification MUST support usmHMAC192SHA256AuthProtocol and SHOULD support usmHMAC384SHA512AuthProtocol. The protocols usmHMAC128SHA224AuthProtocol and usmHMAC256SHA384AuthProtocol are OPTIONAL.

4.1. Deviations from the HMAC-SHA-96 Authentication Protocol

All the HMAC-SHA-2 authentication protocols are straightforward adaptations of the HMAC-MD5-96 and HMAC-SHA-96 authentication protocols. Specifically, they differ from the HMAC-MD5-96 and HMAC-SHA-96 authentication protocols in the following aspects:

- o The SHA-2 hash function is used to compute the message digest in the HMAC computation according to RFC 2104 and RFC 6234, as opposed to the MD5 hash function [RFC1321] and SHA-1 hash function [SHA] used in HMAC-MD5-96 and HMAC-SHA-96, respectively. Consequently, the length of the message digest prior to truncation is 224 bits for the SHA-224-based protocol, 256 bits for the SHA-256-based protocol, 384 bits for the SHA-384-based protocol, and 512 bits for the SHA-512-based protocol.

- o The resulting message digest (output of HMAC) is truncated to

  * 16 octets for usmHMAC128SHA224AuthProtocol

  * 24 octets for usmHMAC192SHA256AuthProtocol

  * 32 octets for usmHMAC256SHA384AuthProtocol

  * 48 octets for usmHMAC384SHA512AuthProtocol

  as opposed to the truncation to 12 octets in HMAC-MD5-96 and HMAC-SHA-96.

- o The user’s secret key to be used when calculating a digest MUST be

  * 28 octets long and derived with SHA-224 for the SHA-224-based protocol usmHMAC128SHA224AuthProtocol

  * 32 octets long and derived with SHA-256 for the SHA-256-based protocol usmHMAC192SHA256AuthProtocol

  * 48 octets long and derived with SHA-384 for the SHA-384-based protocol usmHMAC256SHA384AuthProtocol

  * 64 octets long and derived with SHA-512 for the SHA-512-based protocol usmHMAC384SHA512AuthProtocol

as opposed to the keys being 16 and 20 octets long in HMAC-MD5-96 and HMAC-SHA-96, respectively.

4.2. Processing

This section describes the procedures for the HMAC-SHA-2 authentication protocols. The descriptions are based on the definition of services and data elements defined for HMAC-SHA-96 in RFC 3414 with the deviations listed in Section 4.1.

Values of constants M (the length of the secret key in octets) and N (the length of the Message Authentication Code (MAC) output in octets), and the hash function H used below are:

usmHMAC128SHA224AuthProtocol: M=28, N=16, H=SHA-224;

usmHMAC192SHA256AuthProtocol: M=32, N=24, H=SHA-256;

usmHMAC256SHA384AuthProtocol: M=48, N=32, H=SHA-384;

usmHMAC384SHA512AuthProtocol: M=64, N=48, H=SHA-512.

4.2.1. Processing an Outgoing Message

This section describes the procedure followed by an SNMP engine whenever it must authenticate an outgoing message using one of the authentication protocols defined above. Values of the constants M and N, and the hash function H are as defined in Section 4.2 and are selected based on which authentication protocol is configured for the given USM usmUser Table entry.

1. The msgAuthenticationParameters field is set to the serialization of an OCTET STRING containing N zero octets; it is serialized according to the rules in RFC 3417 [RFC3417].

2. Using the secret authKey of M octets, the HMAC is calculated over the wholeMsg according to RFC 6234 with hash function H.

3. The N first octets of the above HMAC are taken as the computed MAC value.

4. The msgAuthenticationParameters field is replaced with the MAC obtained in the previous step.

5. The authenticatedWholeMsg is then returned to the caller together with the statusInformation indicating success.

4.2.2. Processing an Incoming Message

This section describes the procedure followed by an SNMP engine whenever it must authenticate an incoming message using one of the HMAC-SHA-2 authentication protocols. Values of the constants M and N, and the hash function H are as defined in Section 4.2 and are selected based on which authentication protocol is configured for the given USM usmUser Table entry.

1. If the digest received in the msgAuthenticationParameters field is not N octets long, then a failure and an errorIndication (authenticationError) are returned to the calling module.

2. The MAC received in the msgAuthenticationParameters field is saved.

3. The digest in the msgAuthenticationParameters field is replaced by the N zero octets.

4. Using the secret authKey of M octets, the HMAC is calculated over the wholeMsg according to RFC 6234 with hash function H.

5. The N first octets of the above HMAC are taken as the computed MAC value.

6. The msgAuthenticationParameters field is replaced with the MAC value that was saved in step 2.

7. The newly calculated MAC is compared with the MAC saved in step 2. If they do not match, then a failure and an errorIndication (authenticationFailure) are returned to the calling module.

8. The authenticatedWholeMsg and statusInformation indicating success are then returned to the caller.

5. Key Localization and Key Change

For any of the protocols defined in Section 4, key localization and key change SHALL be performed according to RFC 3414 [RFC3414] using the same SHA-2 hash function as in the HMAC-SHA-2 authentication protocol.

6. Structure of the MIB Module

The MIB module specified in this memo does not define any managed objects, subtrees, notifications, or tables; rather, it only defines object identities (for authentication protocols) under a subtree of an existing MIB.

7. Relationship to Other MIB Modules

7.1. Relationship to SNMP-USER-BASED-SM-MIB

RFC 3414 specifies the MIB module for USM for SNMPv3 (SNMP-USER-BASED-SM-MIB), which defines authentication protocols for USM based on the hash functions MD5 and SHA-1, respectively. The following MIB module defines new HMAC-SHA2 authentication protocols for USM based on the SHA-2 hash functions [SHA]. The use of the HMAC-SHA2 authentication protocols requires the usage of the objects defined in the SNMP-USER-BASED-SM-MIB.

7.2. Relationship to SNMP-FRAMEWORK-MIB

RFC 3411 [RFC3411] specifies the SNMP-FRAMEWORK-MIB, which defines a subtree snmpAuthProtocols for SNMP authentication protocols. The following MIB module defines new authentication protocols in the snmpAuthProtocols subtree.

7.3. MIB Modules Required for IMPORTS

The following MIB module IMPORTS definitions from SNMPv2-SMI [RFC2578] and SNMP-FRAMEWORK-MIB [RFC3411].

8. Definitions

```
SNMP-USM-HMAC-SHA2-MIB DEFINITIONS ::= BEGIN
    IMPORTS
        MODULE-IDENTITY, OBJECT-IDENTITY,
    snmpModules             FROM SNMPv2-SMI          -- [RFC2578]
    snmpAuthProtocols       FROM SNMP-FRAMEWORK-MIB; -- [RFC3411]

snmpUsmHmacSha2MIB MODULE-IDENTITY
    LAST-UPDATED    "201508130000Z"      -- 13 August 2015, midnight
    ORGANIZATION    "SNMPv3 Working Group"
    CONTACT-INFO    "WG email: OPSAWG@ietf.org
                    Subscribe:
                        https://www.ietf.org/mailman/listinfo/opsawg
                    Editor:     Johannes Merkle
                                secunet Security Networks
                    Postal:     Mergenthaler Allee 77
                                D-65760 Eschborn
                                Germany
                    Phone:      +49 20154543091
                    Email:      johannes.merkle@secunet.com
```

```
                      Co-Editor: Manfred Lochter
                                 Bundesamt fuer Sicherheit in der
                                 Informationstechnik (BSI)
                      Postal:    Postfach 200363
                                 D-53133 Bonn
                                 Germany
                      Phone:     +49 228 9582 5643
                      Email:     manfred.lochter@bsi.bund.de"

    DESCRIPTION       "Definitions of Object Identities needed
                      for the use of HMAC-SHA2 by SNMP's User-based
                      Security Model.

          Copyright (c) 2015 IETF Trust and the persons identified
          as authors of the code.  All rights reserved.

          Redistribution and use in source and binary forms, with
          or without modification, is permitted pursuant to, and
          subject to the license terms contained in, the Simplified
          BSD License set forth in Section 4.c of the IETF Trust's
          Legal Provisions Relating to IETF Documents
          (http://trustee.ietf.org/license-info)."

    REVISION    "201508130000Z"       -- 13 August 2015, midnight
    DESCRIPTION "Initial version, published as RFC 7630"
::= { snmpModules 235 }

usmHMAC128SHA224AuthProtocol OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "The Authentication Protocol
                usmHMAC128SHA224AuthProtocol uses HMAC-SHA-224 and
                truncates output to 128 bits."
    REFERENCE   "- Krawczyk, H., Bellare, M., and R. Canetti, HMAC:
                Keyed-Hashing for Message Authentication, RFC 2104.
                - National Institute of Standards and Technology,
                Secure Hash Standard (SHS), FIPS PUB 180-4, 2012."
    ::= { snmpAuthProtocols 4 }

usmHMAC192SHA256AuthProtocol OBJECT-IDENTITY
    STATUS      current
    DESCRIPTION "The Authentication Protocol
                usmHMAC192SHA256AuthProtocol uses HMAC-SHA-256 and
                truncates output to 192 bits."
    REFERENCE   "- Krawczyk, H., Bellare, M., and R. Canetti, HMAC:
                Keyed-Hashing for Message Authentication, RFC 2104.
                - National Institute of Standards and Technology,
                Secure Hash Standard (SHS), FIPS PUB 180-4, 2012."
    ::= { snmpAuthProtocols 5 }
```

```
   usmHMAC256SHA384AuthProtocol OBJECT-IDENTITY
       STATUS      current
       DESCRIPTION "The Authentication Protocol
                   usmHMAC256SHA384AuthProtocol uses HMAC-SHA-384 and
                   truncates output to 256 bits."
       REFERENCE   "- Krawczyk, H., Bellare, M., and R. Canetti, HMAC:
                   Keyed-Hashing for Message Authentication, RFC 2104.
                   - National Institute of Standards and Technology,
                   Secure Hash Standard (SHS), FIPS PUB 180-4, 2012."
       ::= { snmpAuthProtocols 6 }

   usmHMAC384SHA512AuthProtocol OBJECT-IDENTITY
       STATUS      current
       DESCRIPTION "The Authentication Protocol
                   usmHMAC384SHA512AuthProtocol uses HMAC-SHA-512 and
                   truncates output to 384 bits."
       REFERENCE   "- Krawczyk, H., Bellare, M., and R. Canetti, HMAC:
                   Keyed-Hashing for Message Authentication, RFC 2104.
                   - National Institute of Standards and Technology,
                   Secure Hash Standard (SHS), FIPS PUB 180-4, 2012."
       ::= { snmpAuthProtocols 7 }

   END
```

9. Security Considerations

9.1. Use of the HMAC-SHA-2 Authentication Protocols in USM

The security considerations of RFC 3414 [RFC3414] also apply to the HMAC-SHA-2 authentication protocols defined in this document.

9.2. Cryptographic Strength of the Authentication Protocols

At the time of publication of this document, all of the HMAC-SHA-2 authentication protocols provide a very high level of security. The security of each HMAC-SHA-2 authentication protocol depends on the parameters used in the corresponding HMAC computation, which are the length of the key (if the key has maximum entropy), the size of the hash function’s internal state, and the length of the truncated MAC. For the HMAC-SHA-2 authentication protocols, these values are as follows (values are given in bits).

Protocol	Key length	Size of internal state	MAC length
usmHMAC128SHA224AuthProtocol	224	256	128
usmHMAC192SHA256AuthProtocol	256	256	192
usmHMAC256SHA384AuthProtocol	384	512	256
usmHMAC384SHA512AuthProtocol	512	512	384

Table 1: HMAC Parameters of the HMAC-SHA-2 Authentication Protocols

The security of the HMAC scales with both the key length and the size of the internal state: longer keys render key guessing attacks more difficult, and a larger internal state decreases the success probability of MAC forgeries based on internal collisions of the hash function.

The role of the truncated output length is more complicated: according to [BCK], there is a trade-off in that

> by outputting less bits the attacker has less bits to predict in a MAC forgery but, on the other hand, the attacker also learns less about the output of the compression function from seeing the authentication tags computed by legitimate parties.

Thus, truncation weakens the HMAC against forgery by guessing but, at the same time, strengthens it against chosen message attacks aiming at MAC forgery based on internal collisions or at key guessing. RFC 2104 and [BCK] allow truncation to any length that is not less than half the size of the internal state.

Further discussion of the security of the HMAC construction is given in RFC 2104.

9.3. Derivation of Keys from Passwords

If secret keys to be used for HMAC-SHA-2 authentication protocols are derived from passwords, the derivation SHOULD be performed using the password-to-key algorithm from Appendix A.1 of RFC 3414 with MD5 being replaced by the SHA-2 hash function H used in the HMAC-SHA-2 authentication protocol. Specifically, the password is converted into the required secret key by the following steps:

o forming a string of length 1,048,576 octets by repeating the value of the password as often as necessary, truncating accordingly, and using the resulting string as the input to the hash function H. The resulting digest, termed "digest1", is used in the next step.

- forming a second string by concatenating digest1, the SNMP engine's snmpEngineID value, and digest1. This string is used as input to the hash function H.

9.4. Access to the SNMP-USM-HMAC-SHA2-MIB

The SNMP-USM-HMAC-SHA2-MIB module defines OBJECT IDENTIFIER values for use in other MIB modules. It does not define any objects that can be accessed. As such, the SNMP-USM-HMAC-SHA2-MIB does not, by itself, have any effect on the security of the Internet.

The values defined in this module are expected to be used with the usmUserTable defined in the SNMP-USER-BASED-SM-MIB [RFC3414]. The considerations in Section 11.5 of RFC 3414 should be taken into account.

10. IANA Considerations

IANA has assigned an OID for the MIB as follows.

Descriptor	OBJECT IDENTIFIER value
snmpUsmHmacSha2MIB	{ snmpModules 235 }

Table 2: OID of MIB

Furthermore, IANA has assigned a value in the SnmpAuthProtocols registry for each of the following protocols.

Description	Value	Reference
usmHMAC128SHA224AuthProtocol	4	RFC 7630
usmHMAC192SHA256AuthProtocol	5	RFC 7630
usmHMAC256SHA384AuthProtocol	6	RFC 7630
usmHMAC384SHA512AuthProtocol	7	RFC 7630

Table 3: Code Points Assigned to HMAC-SHA-2 Authentication Protocols

11. References

11.1. Normative References

[RFC2104] Krawczyk, H., Bellare, M., and R. Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, DOI 10.17487/RFC2104, February 1997, <http://www.rfc-editor.org/info/rfc2104>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC2578] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Structure of Management Information Version 2 (SMIv2)", STD 58, RFC 2578, DOI 10.17487/RFC2578, April 1999, <http://www.rfc-editor.org/info/rfc2578>.

[RFC2579] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Textual Conventions for SMIv2", STD 58, RFC 2579, DOI 10.17487/RFC2579, April 1999, <http://www.rfc-editor.org/info/rfc2579>.

[RFC2580] McCloghrie, K., Ed., Perkins, D., Ed., and J. Schoenwaelder, Ed., "Conformance Statements for SMIv2", STD 58, RFC 2580, DOI 10.17487/RFC2580, April 1999, <http://www.rfc-editor.org/info/rfc2580>.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)", STD 62, RFC 3414, DOI 10.17487/RFC3414, December 2002, <http://www.rfc-editor.org/info/rfc3414>.

[RFC6234] Eastlake 3rd, D. and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)", RFC 6234, DOI 10.17487/RFC6234, May 2011, <http://www.rfc-editor.org/info/rfc6234>.

[SHA] National Institute of Standards and Technology, "Secure Hash Standard (SHS)", FIPS PUB 180-4, DOI 10.6028/NIST.FIPS.180-4, March 2012, <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>.

11.2. Informative References

[RFC1321] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, DOI 10.17487/RFC1321, April 1992, <http://www.rfc-editor.org/info/rfc1321>.

[RFC3410] Case, J., Mundy, R., Partain, D., and B. Stewart, "Introduction and Applicability Statements for Internet-Standard Management Framework", RFC 3410, DOI 10.17487/RFC3410, December 2002, <http://www.rfc-editor.org/info/rfc3410>.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, DOI 10.17487/RFC3411, December 2002, <http://www.rfc-editor.org/info/rfc3411>.

[RFC3417] Presuhn, R., Ed., "Transport Mappings for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3417, DOI 10.17487/RFC3417, December 2002, <http://www.rfc-editor.org/info/rfc3417>.

[BCK] Bellare, M., Canetti, R., and H. Krawczyk, "Keyed Hash Functions for Message Authentication", Advances in Cryptology - CRYPTO 96, Lecture Notes in Computer Science 1109, Springer-Verlag Berlin Heidelberg, DOI 10.1007/3-540-68697-5_1, 1996.

Authors' Addresses

Johannes Merkle (editor)
Secunet Security Networks
Mergenthaler Allee 77
65760 Eschborn
Germany

Phone: +49 201 5454 3091
Email: johannes.merkle@secunet.com

Manfred Lochter
BSI
Postfach 200363
53133 Bonn
Germany

Phone: +49 228 9582 5643
Email: manfred.lochter@bsi.bund.de