Internet Engineering Task Force (IETF)
Request for Comments: 7677
Updates: 5802
Category: Standards Track
ISSN: 2070-1721

T. Hansen
AT&T Laboratories

November 2015

SCRAM-SHA-256 and SCRAM-SHA-256-PLUS
Simple Authentication and Security Layer (SASL) Mechanisms

Abstract

This document registers the Simple Authentication and Security Layer (SASL) mechanisms SCRAM-SHA-256 and SCRAM-SHA-256-PLUS, provides guidance for secure implementation of the original SCRAM-SHA-1-PLUS mechanism, and updates the SCRAM registration procedures of RFC 5802.

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/rfc7677.

Copyright Notice

Table of Contents

1. Introduction

This document registers the SASL mechanisms SCRAM-SHA-256 and SCRAM-SHA-256-PLUS. SHA-256 has stronger security properties than SHA-1, and it is expected that SCRAM mechanisms based on it will have greater predicted longevity than the SCRAM mechanisms based on SHA-1.

The registration form for the SCRAM family of algorithms is also updated from [RFC5802].

After publication of [RFC5802], it was discovered that Transport Layer Security (TLS) [RFC5246] does not have the expected properties for the "tls-unique" channel binding to be secure [RFC7627]. Therefore, this document contains normative text that applies to both the original SCRAM-SHA-1-PLUS and the newly introduced SCRAM-SHA-256-PLUS mechanism.

2. Key Word Definitions

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. SCRAM-SHA-256 and SCRAM-SHA-256-PLUS

The SCRAM-SHA-256 and SCRAM-SHA-256-PLUS SASL mechanisms are defined in the same way that SCRAM-SHA-1 and SCRAM-SHA-1-PLUS are defined in [RFC5802], except that the hash function for HMAC() and H() uses SHA-256 instead of SHA-1 [RFC6234].

For the SCRAM-SHA-256 and SCRAM-SHA-256-PLUS SASL mechanisms, the hash iteration-count announced by a server SHOULD be at least 4096.

The GSS-API mechanism OID for SCRAM-SHA-256 is 1.3.6.1.5.5.18 (see Section 5).

This is a simple example of a SCRAM-SHA-256 authentication exchange when the client doesn't support channel bindings. The username 'user' and password 'pencil' are being used.

```
C: n,,n=user,r=rOprNGfwEbeRWgbNEkqO

S: r=rOprNGfwEbeRWgbNEkqO%hvYDpWUa2RaTCAfuxFIlj)hNlF$k0,
   s=W22ZaJ0SNY7soEsUEjb6gQ==,i=4096

C: c=biws,r=rOprNGfwEbeRWgbNEkqO%hvYDpWUa2RaTCAfuxFIlj)hNlF$k0,
   p=dHzbZapWIk4jUhN+Ute9ytag9zjfMHgsqmmiz7AndVQ=

S: v=6rriTRBi23WpRR/wtup+mMhUZUn/dB5nLTJRsjl95G4=
```

4. Security Considerations

The security considerations from [RFC5802] still apply.

To be secure, either SCRAM-SHA-256-PLUS and SCRAM-SHA-1-PLUS MUST be used over a TLS channel that has had the session hash extension [RFC7627] negotiated, or session resumption MUST NOT have been used.

See [RFC4270] and [RFC6194] for reasons to move from SHA-1 to a strong security mechanism like SHA-256.

The strength of this mechanism is dependent in part on the hash iteration-count, as denoted by "i" in [RFC5802]. As a rule of thumb, the hash iteration-count should be such that a modern machine will take 0.1 seconds to perform the complete algorithm; however, this is unlikely to be practical on mobile devices and other relatively low-performance systems. At the time this was written, the rule of thumb gives around 15,000 iterations required; however, a hash iteration-count of 4096 takes around 0.5 seconds on current mobile handsets. This computational cost can be avoided by caching the ClientKey (assuming the Salt and hash iteration-count is stable). Therefore, the recommendation of this specification is that the hash iteration-count SHOULD be at least 4096, but careful consideration ought to be given to using a significantly higher value, particularly where mobile use is less important.

5. IANA Considerations

5.1. Updates to SCRAM-* Registration

The IANA registry for SCRAM-* (the SCRAM family of SASL mechanisms) in the SASL mechanism registry ([RFC4422]) has been updated as follows. The email address for reviews has been updated, and the note at the end changed.

```
To: iana@iana.org
Subject: Registration of a new SASL family SCRAM

SASL mechanism name (or prefix for the family): SCRAM-*
Security considerations: Section 7 of [RFC5802]
Published specification (optional, recommended): RFC 7677
Person & email address to contact for further information:
   IETF KITTEN WG <kitten@ietf.org>
Intended usage: COMMON
Owner/Change controller: IESG <iesg@ietf.org>
Note: Members of this family MUST be explicitly registered using
   the "IETF Review" [RFC5226] registration procedure.  Reviews
   MUST be requested on the KITTEN mailing list kitten@ietf.org
   (or a successor designated by the responsible Security AD).

Note to future SCRAM-mechanism designers: each new SASL SCRAM
mechanism MUST be explicitly registered with IANA within the SASL
SCRAM Family Mechanisms registry.
```

5.2. SASL-SCRAM Family Mechanisms Registration Procedure

A new IANA registry has been added for members of the SCRAM family of SASL mechanisms, named "SASL SCRAM Family Mechanisms". It adds two new fields to the existing SCRAM mechanism registry: Minimum iteration-count and Associated OID. Below is the template for registration of a new SASL family SCRAM. (Note that the string "TBD-BY-IANA" should be left as is, so that it may be filled in at registration time by IANA.)

To: iana@iana.org
Subject: Registration of a new SASL SCRAM family mechanism

SASL mechanism name (or prefix for the family): SCRAM-<NAME>
Security considerations: Section 7 of [RFC5802]
Published specification (optional, recommended): RFC 7677
Minimum iteration-count: The minimum hash iteration-count that servers SHOULD announce
Associated OID: TBD-BY-IANA
Person & email address to contact for further information:
IETF KITTEN WG <kitten@ietf.org>
Intended usage: COMMON
Owner/Change controller: IESG <iesg@ietf.org>

Note: Members of this family MUST be explicitly registered using the "IETF Review" [RFC5226] registration procedure. Reviews MUST be requested on the KITTEN mailing list kitten@ietf.org (or a successor designated by the responsible Security Area Director).

Note: At publication of a new SASL SCRAM Family Mechanism, IANA SHOULD assign a GSS-API mechanism OID for this mechanism from the iso.org.dod.internet.security.mechanisms prefix (see the "SMI Security for Mechanism Codes" registry) and fill in the value for "TBD-BY-IANA" above. Only one OID needs to be assigned for a SCRAM-<NAME> and SCRAM-<NAME>-PLUS pair. The same OID should be assigned to both entries in the registry.

Note to future SASL SCRAM mechanism designers: each new SASL SCRAM mechanism MUST be explicitly registered with IANA and MUST comply with the SCRAM-mechanism naming convention defined in Section 4 of [RFC5802].

The existing entries for SASL SCRAM-SHA-1 and SCRAM-SHA-1-PLUS have been moved from the existing SASL mechanism registry to the "SASL SCRAM Family Mechanisms" registry. At that time, the following values were added:

Minimum iteration-count: 4096
OID: 1.3.6.1.5.5.14 (from [RFC5802])

The following new SASL SCRAM mechanisms have been added to the "SASL SCRAM Family Mechanisms" registry:

```
   To: iana@iana.org
   Subject: Registration of a new SASL SCRAM Family mechanism
      SCRAM-SHA-256

   SASL mechanism name (or prefix for the family): SCRAM-SHA-256
   Security considerations: Section 4 of RFC 7677
   Published specification (optional, recommended): RFC 7677
   Minimum iteration-count: 4096
   OID: 1.3.6.1.5.5.18
   Person & email address to contact for further information:
      IETF KITTEN WG <kitten@ietf.org>
   Intended usage: COMMON
   Owner/Change controller: IESG <iesg@ietf.org>
   Note:

   To: iana@iana.org
   Subject: Registration of a new SASL SCRAM Family mechanism
      SCRAM-SHA-256-PLUS

   SASL mechanism name (or prefix for the family): SCRAM-SHA-256-PLUS
   Security considerations: Section 4 of RFC 7677
   Published specification (optional, recommended): RFC 7677
   Minimum iteration-count: 4096
   OID: 1.3.6.1.5.5.18
   Person & email address to contact for further information:
      IETF KITTEN WG <kitten@ietf.org>
   Intended usage: COMMON
   Owner/Change controller: IESG <iesg@ietf.org>
   Note:
```

6. References

6.1. Normative References

[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>.

[RFC4422] Melnikov, A., Ed. and K. Zeilenga, Ed., "Simple Authentication and Security Layer (SASL)", RFC 4422, DOI 10.17487/RFC4422, June 2006, <http://www.rfc-editor.org/info/rfc4422>.

[RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams, "Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, DOI 10.17487/RFC5802, July 2010, <http://www.rfc-editor.org/info/rfc5802>.

[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>.

[RFC7627] Bhargavan, K., Ed., Delignat-Lavaud, A., Pironti, A., Langley, A., and M. Ray, "Transport Layer Security (TLS) Session Hash and Extended Master Secret Extension", RFC 7627, DOI 10.17487/RFC7627, September 2015, <http://www.rfc-editor.org/info/rfc7627>.

6.2. Informative References

[RFC4270] Hoffman, P. and B. Schneier, "Attacks on Cryptographic Hashes in Internet Protocols", RFC 4270, DOI 10.17487/RFC4270, November 2005, <http://www.rfc-editor.org/info/rfc4270>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, DOI 10.17487/RFC5226, May 2008, <http://www.rfc-editor.org/info/rfc5226>.

[RFC6194] Polk, T., Chen, L., Turner, S., and P. Hoffman, "Security Considerations for the SHA-0 and SHA-1 Message-Digest Algorithms", RFC 6194, DOI 10.17487/RFC6194, March 2011, <http://www.rfc-editor.org/info/rfc6194>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <http://www.rfc-editor.org/info/rfc5246>.

Acknowledgements

This document benefited from discussions on the KITTEN WG mailing list. The author would like to specially thank Russ Allbery, Dave Cridland, Shawn Emery, Stephen Farrell, Simon Josefsson, Pearl Liang, Alexey Melnikov, Peter Saint-Andre, Robert Sparks, Martin Thompson, and Nico Williams for their comments on this topic.

Author's Address

Tony Hansen
AT&T Laboratories
200 Laurel Ave. South
Middletown, NJ 07748
United States

Email: tony+scramsha256@maillennium.att.com