SCRAM-SHA-512 and SCRAM-SHA-512-PLUS Simple Authentication and Security Layer (SASL) Mechanisms

Abstract

This document registers the Simple Authentication and Security Layer (SASL) mechanisms SCRAM-SHA-512 and SCRAM-SHA-512-PLUS.

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 https://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 22 April 2022.

Copyright Notice

Table of Contents

1. Introduction

   This document registers the SASL [RFC4422] mechanisms SCRAM-SHA-512
   and SCRAM-SHA-512-PLUS. SHA-512 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.

2. Key Word Definitions

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
   "OPTIONAL" in this document are to be interpreted as described in
   BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all

3. SCRAM-SHA-512 and SCRAM-SHA-512-PLUS

   The SCRAM-SHA-512 and SCRAM-SHA-512-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-512 instead of SHA-1 [RFC6234].

   For the SCRAM-SHA-512 and SCRAM-SHA-512-PLUS SASL mechanisms, the
   hash iteration-count announced by a server SHOULD be at least 10000.

   The GSS-API mechanism OID for SCRAM-SHA-512 is 1.3.6.1.5.5.<TBD>
   (see Section 5).

   This is a simple example of a SCRAM-SHA-512 authentication exchange
   when the client doesn't support channel bindings. The username
   'user' and password 'pencil' are being used.

   [[TBD: Add an example]]

4. Security Considerations

   The security considerations from [RFC5802] still apply.

To be secure, SCRAM-SHA-512-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. When using SCRAM over
TLS 1.2 [RFC5246], the "tls-unique" channel binding is still the
default channel binding to use (see Section 6.1 of [RFC5802]),
assuming the above conditions are satisfied. As "tls-unique" channel
binding is not defined for TLS 1.3 [RFC8446], when using SCRAM over
TLS 1.3, the "tls-exporter" channel binding [tls-1.3-channel-
binding] MUST be the default channel binding (in the sense specified
in Section 6.1 of [RFC5802]) to use.

See [RFC4270] and [RFC6194] for reasons to move from SHA-1 to a
strong security mechanism like SHA-512.

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 10000 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 10000, but careful consideration ought to
be given to using a significantly higher value, particularly where
mobile use is less important.

5. IANA Considerations

IANA is requested to add the following new SASL SCRAM mechanisms to
the "SASL SCRAM Family Mechanisms" registry:

To: iana@iana.org

Subject: Registration of a new SASL SCRAM Family mechanism
   SCRAM-SHA-512

SASL mechanism name (or prefix for the family): SCRAM-SHA-512

Security considerations: [Section 4](#) of RFC XXXX

Published specification (optional, recommended): RFC XXXX

Minimum iteration-count: 10000

OID: 1.3.6.1.5.5.<TBD>

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: iana@iana.org
To:
Subject: Registration of a new SASL SCRAM Family mechanism
            SCRAM-SHA-512-PLUS

SASL mechanism name (or prefix for the family): SCRAM-SHA-512-
   PLUS

Security considerations: [Section 4](#) of RFC XXXX

Published specification (optional, recommended): RFC XXXX

Minimum iteration-count: 10000

OID: 1.3.6.1.5.5.<TBD>

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, <https://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, <https://www.rfc-editor.org/
            info/rfc4422>.

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

[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, <https://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, <https://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, <https://
            www.rfc-editor.org/info/rfc7627>.

[RFC8174]   Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
            2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
            May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8446]   Rescorla, E., "The Transport Layer Security (TLS)
            Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446,
            August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[tls-1.3-channel-binding]
            Whited, S., "Channel Bindings for TLS 1.3", Work in
            Progress, Internet-Draft, draft-ietf-kitten-tls-channel-
            bindings-for-tls13-11, 18 October 2021, <https://
            www.ietf.org/archive/id/draft-ietf-kitten-tls-channel-
            bindings-for-tls13-11.txt>.

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, <https://www.rfc-editor.org/info/
           rfc4270>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an
           IANA Considerations Section in RFCs", RFC 5226, DOI
           10.17487/RFC5226, May 2008, <https://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,
           <https://www.rfc-editor.org/info/rfc6194>.

Acknowledgements

Author's Address

Alexey Melnikov (editor)
Isode Ltd
14 Castle Mews
Hampton
TW12 2NP
United Kingdom

Email: alexey.melnikov@isode.com