Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms

draft-melnikov-scram-bis-01

Abstract

This document updates requirements on implementations of various Salted Challenge Response Authentication Mechanism (SCRAM) Simple Authentication and Security Layer (SASL) mechanisms based on more modern security practices.

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 12 January 2023.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.
1. Introduction

The intent of this document is to serve as an implementor's roadmap for implementing various Salted Challenge Response Authentication Mechanism (SCRAM) [RFC5802] SASL [RFC4422] mechanisms.

[RFC5802] defined the generic SCRAM framework and described instantiation of a SCRAM mechanism using SHA-1 hash function: SCRAM-SHA-1 (and SCRAM-SHA-1-PLUS). [RFC7677] described another instantiation using SHA-256 hash function (SCRAM-SHA-256 and SCRAM-SHA-256-PLUS) and also clarified conditions for using the mandatory-to-implement "tls-unique" channel binding with TLS 1.2. [tls-1.3-channel-binding] defines the "tls-exporter" channel binding that is to be used when a SCRAM mechanism is used over TLS 1.3 [RFC8446] or later.

[I-D.melnikov-scram-sha-512] and [I-D.melnikov-scram-sha3-512] define further instantiations of SCRAM using SHA-512 and SHA3-512 hash functions respectively.

[I-D.melnikov-scram-2fa] defines an extension to SCRAM for two factor authentication. It is applicable to all instantiations of SCRAM.

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. Implementation Recommendations

[tls-1.3-channel-binding] document updated [RFC5802] and [RFC7677] to use the "tls-exporter" channel binding as the mandatory to implement (instead of "tls-unique") when a SCRAM mechanism is used over TLS 1.3 [RFC8446] or later.

[[Discuss if rough consensus can be reached on this in the KITTEN WG.]] All SCRAM implementations SHOULD support [I-D.melnikov-scram-2fa] to allow for two factor authentication with SCRAM.

[[Possibly narrow down choices to only one of these. Discuss in the KITTEN WG.]] Unless required for backward compatibility, server and client implementations MUST support SCRAM-SHA-512-PLUS/SCRAM-SHA-512 [I-D.melnikov-scram-sha-512] and/or SCRAM-SHA3-512-PLUS/SCRAM-SHA3-512 [I-D.melnikov-scram-sha3-512] instead of SCRAM-SHA-1-PLUS/SCRAM-SHA-1 [RFC5802].

[RFC5803] describes how SCRAM hashes can be stored in LDAP. It is compatible with all versions of SCRAM described in this document, including SCRAM-SHA-256, SCRAM-SHA-512 and SCRAM-SHA3-512.

4. Security Considerations

The security considerations from [RFC5802] still apply.

To be secure, SCRAM-*-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. When using SCRAM over TLS 1.3 [RFC8446], the "tls-exporter" channel binding [tls-1.3-channel-binding] is the default (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 RFC XXXX as an extra reference for the following SASL SCRAM mechanisms listed in the "SASL SCRAM Family Mechanisms" registry: SCRAM-SHA-1, SCRAM-SHA-1-PLUS, SCRAM-SHA-256 and SCRAM-SHA-256-PLUS.

6. References

6.1. Normative References


6.2. Informative References


Acknowledgements

This document is based on RFC 7677 by Tony Hansen.

Thank you to Ludovic Bocquet for comments and corrections.

Author's Address

Alexey Melnikov (editor)
Isode Ltd
14 Castle Mews
Hampton
TW12 2NP
United Kingdom
Email: alexey.melnikov@isode.com