Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 14, 2021

A. Melnikov
Isode Ltd

July 13, 2020

Extensions to Salted Challenge Response (SCRAM) for 2 factor authentication
draft-melnikov-scram-2fa-01

Abstract

This specification describes an extension to family of Simple Authentication and Security Layer (SASL; RFC 4422) authentication mechanisms called the Salted Challenge Response Authentication Mechanism (SCRAM), which provides support for 2 factor authentication.

This specification also gives an example how TOTP (RFC 6238) can be used as the second factor.

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 January 14, 2021.

Copyright Notice

Copyright (c) 2020 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 Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Conventions Used in This Document 2
2.1. Terminology 3
2.2. Notation 3
3. SCRAM Extension for 2FA 3
4. Formal Syntax 4
5. Use of TOTP with SCRAM 4
6. Examples 5
7. Open Issues 5
8. Security Considerations 5
9. IANA Considerations 5
10. Acknowledgements 5
11. Normative References 6
Author's Address 6

1. Introduction

SCRAM [RFC5802] is a password based SASL [RFC4422] authentication mechanism that provides (among other things) mutual authentication and binding to an external security layer such as TLS.

Two-factor authentication (2FA) is a way to add additional security to an authentication exchange. The first "factor" is a password. The second "factor" is a verification code retrieved from an application on a mobile device or computer. 2FA is conceptually similar to a security token device that banks in some countries require for online banking. Other names for 2FA systems include OTP (one-time password) and TOTP (Time-based One-time Password algorithm, such as [RFC6238]).

This specification describes an extension to SCRAM to provide 2 factor authentication. SCRAM already relies on passwords for authentication. This document specifies how second "factors" can be incorporated into SCRAM authentication.

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 [RFC2119].

Formal syntax is defined by [RFC5234] including the core rules defined in Appendix B of [RFC5234].

Example lines prefaced by "C:" are sent by the client and ones prefaced by "S:" by the server. If a single "C:" or "S:" label applies to multiple lines, then the line breaks between those lines are for editorial clarity only, and are not part of the actual protocol exchange.

2.1. Terminology

This document uses several terms defined in [RFC4949] ("Internet Security Glossary") including the following: authentication, authentication exchange, authentication information, brute force, challenge-response, cryptographic hash function, dictionary attack, eavesdropping, hash result, keyed hash, man-in-the-middle, nonce, one-way encryption function, password, replay attack and salt. Readers not familiar with these terms should use that glossary as a reference. Other terms defined in [RFC5802] are also used in this document.

2.2. Notation

This document reuses notation defined in SCRAM.

3. SCRAM Extension for 2FA

This extension doesn't add any extra roundtrips to SCRAM authentication. SCRAM was designed to be extensible, so it allows for optional and mandatory attributes, which covered by MAC codes. Second "factors" are conveyed in the second message sent from the client to the server.

This extension doesn't change how the client authenticates the server.

The server authenticates the client after receiving the second message as described in Section 3 of [RFC5802] If the client included "type" and "second-factor" attributes (see Section 4) and the server supports the specified second factor type, the server verifies content of the "second-factor" according to the "type". If the second factor verification fails, the server MUST fail authentication and SHOULD return "second-factor-failed" error in the "e" attribute. [[It would be possible to make the extra attributes mandatory by using SCRAM's "m=", but the text above doesn't do that.]]

4. Formal Syntax

This document defines the following SCRAM attributes:

- t: This attribute specifies the type of second factor. (Create IANA registry for these?) This document defines one type: "otp". If this attribute is specified, the "f" attribute MUST also be specified.

- f: This attribute specifies the value of the second factor. For "t=otp" it is 6 digit decimal number. This attribute MUST be ignored unless the "t" attribute is also specified.

The following syntax specification uses the Augmented Backus-Naur Form (ABNF) notation as specified in [RFC5234].

```
type            = "t=" type-value
                ; Complies with "attr-val" syntax.
type-value      = "otp" / value
                ; Type of second factor.
                ; Should be registered with IANA.
second-factor   = "f=" second-factor-value
                ; Complies with "attr-val" syntax.
second-factor-value = 6DIGIT / value

server-error-value-ext =
        "second-factor-failed" /
        "second-factor-value-missing"

value = <as defined in RFC 5802>
```

5. Use of TOTP with SCRAM

This document defines the following SCRAM attributes:

- t: This attribute specifies the type of second factor. (Create IANA registry for these?) This document defines one type: "otp". If this attribute is specified, the "f" attribute MUST also be specified.

- f: This attribute specifies the value of the second factor. For "t=otp" it is 6 digit decimal number. This attribute MUST be ignored unless the "t" attribute is also specified.

A TOTP URI is specified with the following ABNF:

```
totp-uri = "otpauth" "://" "totp/" label "?secret=" secret "&issuer=" issuer
label = issuer (":" / "%3A") identity
identity = 1*CHAR ; URI-encoded SASL identity
secret = 40 * HEXCHAR ; Base32 (hex) encoded secret with no padding.
issuer = 1*CHAR ; Issuer name.
```

6. Examples

The following example extends the example from Section 5 of [RFC5802]:

```
C: n,,n=user,r=fyko+d2lbbFgONRv9qkxdawL
S: r=fyko+d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j,s=QSXCR+Q6sek8bf92,
   i=4096
C: c=biws,r=fyko+d2lbbFgONRv9qkxdawL3rfcNHYJY1ZVvWVs7j,
   t=totp,f=776804,
       p=v0X8v3Bz2T0CJGbJQyF0X+HI4Ts=
S: v=lz59pqV8S7suAoZWja4dJRkFsKQ=
```

7. Open Issues

Simon Josefsson: should this be a new SASL mechanism name, e.g. SCRAM-SHA-1-TOTP?

Simon Josefsson: cookie option for fast reauthentication? Alexey: can do or just used CLIENT-KEY (draft-cridland-kitten-clientkey)?

8. Security Considerations

TBD

9. IANA Considerations

TBD. Possibly create a new registry of second factor types.

10. Acknowledgements

Thank you to Stephen Farrell for motivating creation of this document and to Dave Cridland for describing how TOTP can be used with XMPP in XEP-400.

11. 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>.

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <https://www.rfc-editor.org/info/rfc4949>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/info/rfc5234>.

[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>.

[RFC6238] M'Raihi, D., Machani, S., Pei, M., and J. Rydell, "TOTP: Time-Based One-Time Password Algorithm", RFC 6238, DOI 10.17487/RFC6238, May 2011, <https://www.rfc-editor.org/info/rfc6238>.

Author's Address

Alexey Melnikov
Isode Ltd

Email: Alexey.Melnikov@isode.com