Internet Engineering Task Force (IETF)
Internet-Draft
Obsoletes: 2195 (if approved)
Intended Status: Informational
Expires: December 31, 2017

Kurt D. Zeilenga
Isode Limited
L. Camara
Individual

June 29, 2017

CRAM-MD5 to Historic
draft-zeilenga-luis140219-crammd5-to-historic-00

[[RFC-Editor: non-ASCII (RFC 7997) characters WILL be added in AUTH48.]]

Abstract

This document recommends the retirement of the CRAM-MD5 authentication mechanism, and discusses the reasons for doing so. This document recommends RFC 2195 and its predecessor, RFC 2095, be moved to Historic status.

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 http://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 December 31, 2017.

1. CRAM-MD5

CRAM-MD5 [RFC2195] is a authentication mechanism. It was originally designed for use in Internet Messaging Access Protocol (IMAP) [RFC3501] and Post Office Protocol (POP) [RFC1939]. It is also

registered as a Simple Authentication and Security Layer (SASL) [RFC4422] mechanism [IANA-SASL], though it has not been formally specified as SASL mechanism.

CRAM-MD5 is a simple challenge/response protocol for establishing that both parties have knowledge of a shared secret derived from the user's password, presumedly a sequence of characters.

While CRAM-MD5 is widely implemented and deployed on the Internet, interoperability is only possible where the client and server have an a priori agreement on the character set and encoding of the password, and any normalization to be applied before input to the cryptographic functions applied by both client and server. Even where the client and server are implemented by the same developer, the client and server will not operate properly in absence of an a priori agreement (such as "passwords shall be a sequence of ASCII printable characters, encoded in a octet with zero parity, with no normalization").

CRAM-MD5 does not provide adequate security services for use on the Internet. CRAM-MD5 does not protect the user's authentication identifier from eavesdroppers. CRAM-MD5 challenge/response exchange is subject to a number of passive and active attacks.

CRAM-MD5 does not provide any data security services nor channel bindings [RFC5056] to data security services (e.g., TLS [RFC5246]) provided externally. Additionally, MD5 is fatally weak [RFC6151] and renders CRAM-MD5 completely insecure in today's environment.

RFC 2195 states no recommendation (or mandate) that implementors only offer CRAM-MD5 when external data security services are in place. RFC 2195 does not recommend (or mandate) that implementations supporting CRAM-MD5 implement any external data security service.

While it possible to revise RFC 2195 to address these and other deficiencies of the authentication mechanism, these changes would be disruptive to existing deployments. For instance, if a revision were to specify that a particular character set, encoding, and normalization of the password is to be used, this mandate would disruptive to deployers who use an incompatible character set, encoding, and/or normalization. Addition of additional security features, such as channel bindings, seems more appropriately done by introduced in a new mechanism.

2. Recommendations

It is recommended RFC 2195 and its predecessor, RFC 2095, be moved to Historic status.

It is recommended that application protocol designers and deployers

consider the SASL PLAIN [RFC4616] mechanism protected by TLS [RFC5246] and/or the SASL Salted Challenge Response Authentication Mechanism (SCRAM) [RFC5802] as alternatives to CRAM-MD5.

3. Security Considerations

The retirement of CRAM-MD5 may lead to use of stronger authentication mechanisms and, hence, may improve Internet security.

4. IANA Considerations

It is requested that IANA update the SASL CRAM-MD5 registration upon publication approval of this document.

Subject: Updated Registration of SASL CRAM-MD5 mechanism
SASL mechanism (or prefix for the family): CRAM-MD5
Security considerations: see RFC XXXX
Published specification (recommended): RFC XXXX, RFC 2195
Person & email address to contact for further information:
Kurt Zeilenga <kurt.zeilenga@isode.com>
Intended usage: LIMITED
Owner/Change controller: IESG

5. References

5.1. Normative References

[IANA-SASL] IANA, "SIMPLE AUTHENTICATION AND SECURITY LAYER (SASL) MECHANISMS", <http://www.iana.org/assignments/sasl-mechanisms>.

5.2. Informative References

[RFC1939] Myers, J. and M. Rose, "Post Office Protocol - Version 3", STD 53, RFC 1939, May 1996.

[RFC2095] Klensin, J., R. Catoe, and P. Krumviede, "IMAP/POP AUTHorize Extension for Simple Challenge/Response", RFC 2095, January 1997.

[RFC2195] Klensin, J., R. Catoe, and P. Krumviede, "IMAP/POP AUTHorize Extension for Simple Challenge/Response", RFC 2195, September 1997.

[RFC3501] Crispin, M., "INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1", RFC 3501, March 2003.

[RFC4422] Melnikov, A. (Editor), K. Zeilenga (Editor), "Simple Authentication and Security Layer (SASL)", RFC 4422, June 2006.

[RFC4616] Zeilenga, K., "The PLAIN Simple Authentication and Security Layer (SASL) Mechanism", RFC 4616, August 2006.

[RFC5056] Williams, N., "On the Use of Channel Bindings to Secure Channels", RFC 5056, November 2007.

[RFC5246] Dierks, T. and, E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams, "Salted Challenge Response Authentication (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, July 2010.

[RFC6151] Turner, S., and L. Chen, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms", RFC 6151, March 2011.

6. Authors' Addresses

Kurt D. Zeilenga
Isode Limited

Email: Kurt.Zeilenga@Isode.COM

Luis Camara (a.k.a. luis140219)
Praceta das Tilias 102 R/C A
2775-336 Parede
Portugal

EMail: luis.camara@live.com.pt

Appendix A: Notes about -01

[[Do not change the below note in any revision, but this appendix WILL be removed in AUTH48.]]

("-00 draft" refers to the 2008 version.)

The new -00 draft is a revision of the 2008-11-20 -00 draft, that I found expired and archived in the IETF Tools website.

The original draft was posted after November 10, 2008, so I have put the RFC 5378 notice at the top of the draft.

I've replaced references to Internet-Drafts with the RFCs they've turned onto (RFC 5802 and RFC 5056, respectively), as Kurt requested in the -00 draft.

I've modernised the header: added "Internet Engineering Task Force

(IETF)", replaced the incorrect phrase "Expires in six months" with "Expires December 31, 2017", added "(if approved)" to the Obsoletes header, replaced "Category" with "Status" and moved headers around to match the header order of a modern (2017-style) Internet-Draft.

The "Status of this Memo" section was renamed as a minor editorial change to "Status of This Memo" (note casing) and was replaced using the 2017-style boilerplate.

The abstract was moved to before the "Status of This Memo".

A sentence indicating MD5's fatal weaknesses was added to the end of the 5th paragraph of Section 1, and an informative reference to RFC 6151 was added.

RFC 2095 and RFC 2195 are normatively referenced in -00, but they shouldn't be. The 2 references were moved to the informative references section. The references were sorted by ASCII/UTF-8 order of their names.

The indenting was changed from 2 to 3 spaces, and I've added myself to the author's list.

There was also a reordering of the sections, correction of the numbering, and removal of the "Acknowledgements" section, that contained in -00 just "TBD" for almost 9 years.

The top line of every page except the first was changed to use "CRAM-MD5 to Historic" instead of "CRAM-MD5", as this document moves CRAM-MD5 to Historic instead of specifying CRAM-MD5.

Kurt, please update your email and affilliation if they've changed. I've revived the draft because it is crucial that RFC 2195 (CRAM-MD5) be moved to Historic.

The draft was taken off the SASL working group because it is concluded. The new name is "zeilenga-luis140219-crammd5-to-historic".

-- luis140219 2017-06-29