Network Working Group
Internet Draft: The CRAM-MD5 SASL Mechanism
Document: draft-nerenberg-sasl-crammd5-03.txt

L. Nerenberg, Editor
Orthanc Systems

November 2002

The CRAM-MD5 SASL Mechanism

Status of this Memo

This document is an Internet Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

Internet Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet Drafts.

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."

The list of current Internet Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

A revised version of this draft document will be submitted to the RFC editor as a Proposed Standard for the Internet Community. Discussion and suggestions for improvement are requested. Distribution of this draft is unlimited.

Copyright Notice

How to Read This Document

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as defined in [KEYWORDS].

1. Introduction

This document defines a simple challenge-response [SASL]

authentication mechanism, using a [KEYED-MD5] digest.

2. CRAM-MD5 Authentication Mechanism

The mechanism name associated with CRAM-MD5 is 'CRAM-MD5'.

This mechanism does not provide a security layer.

The data encoded in the challenge contains a presumptively arbitrary string of random digits, a timestamp, and the fully-qualified primary host name of the server.

The client makes note of the data and then responds with a string consisting of the user name, a space, and a "digest." The latter is computed by applying the keyed MD5 algorithm from [KEYED-MD5] where the key is a shared secret and the digested text is the challenge (including angle-brackets). The client MUST NOT interpret or attempt to validate the contents of the challenge in any way.

This shared secret is a string known only to the client and server. The "digest" parameter itself is a 16-octet value which is sent in hexadecimal format, using lower-case US-ASCII characters.

When the server receives this client response, it verifies the digest provided. Since the user name may contain the space character, the server MUST scan the client response from right to left; the first space character encountered separates the digest from the user name. If the digest is correct, the server should consider the client authenticated and respond appropriately.

The user name and shared secret MUST be represented in the Unicode character set [UNICODE], and MUST be normalised using the Unicode Normalisation Form KC [NFKC]. The resulting values MUST be encoded as UTF-8 [UTF8].

2.1. Formal Syntax

The following syntax specification uses the augmented Backus-Naur

Form (ABNF) as specified in [ABNF], and incorporates by reference the Core Rules defined in that document.

```
challenge  = "<" 1*DIGIT "." 1*DIGIT "@" hostname ">"

digest     = 32(DIGIT / %x61-66)
               ; A hexadecimal string using only lower-case
               ; letters

hostname   = 1*(ALPHA / DIGIT) *("." / "-" / ALPHA / DIGIT)

response   = user SP digest

user       = 1*OCTET
```


2.2. Examples

The examples in this section do NOT form part of the specification. Where conflicts exist between the examples and the formal grammar or specification text, the latter are authoritative.

These examples show the use of the CRAM-MD5 mechanism with the IMAP4 AUTHENTICATE command [IMAP4]. The base64 encoding of the challenges and responses is part of the IMAP4 AUTHENTICATE command, not part of the CRAM-MD5 specification itself.

```
S: * OK IMAP4rev1 Server
C: A0001 AUTHENTICATE CRAM-MD5
S: + PDE4OTYuNjk3MTcwOTUyQHBvc3RvZmZpY2UucmVzdG9uLm1jaS5uZXQ+
C: dGltIGI5MTNhNjAyYzdlZGE3YTQ5NWI0ZTZlNzMzNGQzODkw
S: A0001 OK CRAM-MD5 authentication successful
```

In this example, the shared secret is the string

```
tanstaaftanstaaf
```

Hence, the Keyed MD5 digest is produced by calculating

```
MD5((tanstaaftanstaaf XOR opad),
```

MD5((tanstaaftanstaaf XOR ipad),
<1896.697170952@postoffice.reston.mci.net>))

where ipad and opad are as defined in [KEYED-MD5] and the string shown in the challenge is the base64 encoding of <1896.697170952@postoffice.reston.mci.net>. The shared secret is null-padded to a length of 64 bytes. If the shared secret is longer than 64 bytes, the MD5 digest of the shared secret is used as a 16 byte input to the keyed MD5 calculation.

This produces a digest value (in hexadecimal) of

b913a602c7eda7a495b4e6e7334d3890

The user name is then prepended to it, forming

tim b913a602c7eda7a495b4e6e7334d3890

Which is then base64 encoded to meet the requirements of the IMAP4 AUTHENTICATE command (or the similar POP3 AUTH command), yielding

dGltIGI5MTNhNjAyYzdlZGE3YTQ5NWI0ZTZlNzMzNGQzODkw

3. References

3.1. Normative References

[ABNF]
Crocker, D., P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC2234, Internet Mail Consortium and Demon Internet Ltd., November 1997.

[KEYED-MD5]
Krawczyk, Bellare, Canetti, "HMAC: Keyed-Hashing for Message

Authentication", RFC 2104, IBM and UCSD, February 1997.

[KEYWORDS]
Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC2119, Harvard University, March 1997.

[MD5]
Rivest, R., "The MD5 Message Digest Algorithm", RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, Inc., April 1992.

[NFKC]
Davis, M., M. Durst, "Unicode Standard Annex #15: Unicode Normalisation Forms", An integral part of The Unicode Standard, Version 3.2.0 (http://www.unicode.org/reports/tr15/).

[SASL]
Myers, J., "Simple Authentication and Security Layer (SASL)," RFC 2222, Netscape Communications, October 1997.

[UNICODE]
The Unicode Consortium, The Unicode Standard, Version 3.2.0, defined by: The Unicode Standard, Version 3.0 (Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), as amended by the Unicode Standard Annex #27: Unicode 3.1 (http://www.unicode.org/reports/tr27/) and the Unicode Standard Annex #28: Unicode 3.2 (http://www.unicode.org/reports/tr28/)

[UTF8]
Yergeau, F., "UTF-8, a transformation format of ISO 10646", RFC 2279, Alis Technologies, January 1998.

3.2. Informative References

[IMAP4]
Crispin, M., "Internet Message Access Protocol - Version 4rev1," Work in progress (son of RFC2060)

4. Security Considerations

It is conjectured that use of the CRAM-MD5 authentication mechanism provides replay protection for a session.

This mechanism does not obscure the user name in any way. Accordingly, a server that implements both a cleartext password command and this authentication type should not allow both methods of access for a given user name.

Keyed MD5 is chosen for this application because of the greater security imparted to authentication of short messages. In addition, the use of the techniques described in [KEYED-MD5] for precomputation of intermediate results make it possible to avoid explicit cleartext storage of the shared secret on the server system by instead storing the intermediate results which are known as "contexts."

While the saving, on the server, of the MD5 "context" is marginally better than saving the shared secrets in cleartext, it is not sufficient to protect the secrets if the server itself is compromised. Consequently, servers that store the secrets or contexts must both be protected to a level appropriate to the potential information value in the data and services protected by this mechanism. In other words, techniques like this one involve a tradeoff between vulnerability to network sniffing and I/O buffer snooping and vulnerability of the server host's databases. If one believes that the host and its databases are subject to compromise, and the network is not, this technique (and all others like it) is unattractive. It is perhaps even less attractive than cleartext passwords, which are typically stored on hosts in one-way hash form. On the other hand, if the server databases are perceived as reasonably secure, and one is concerned about client-side or network interception of the passwords (secrets), then this (and similar) techniques are preferable to clear-text passwords by a wide margin.

As the length of the shared secret increases, so does the difficulty of deriving it.

While there are now suggestions in the literature that the use of MD5 and keyed MD5 in authentication procedures probably has a limited effective lifetime, the technique is now widely deployed and widely understood. It is believed that this general understanding may assist with the rapid replacement, by CRAM-MD5, of the current uses of permanent cleartext passwords in many protocols. This document has been deliberately written to permit easy upgrading to use SHA (or whatever alternatives emerge) when they are considered to be widely available and adequately safe.

Even with the use of CRAM-MD5, users are still vulnerable to active attacks. An example of an increasingly common active attack is 'TCP Session Hijacking' as described in CERT Advisory CA-95:01.

5. Contributors

The CRAM-MD5 mechanism was originally specified in RFC 2095, IMAP/POP AUTHorize Extension for Simple Challenge/Response. The authors of that document -- John C. Klensin, Paul Krumviede, and Randy Catoe -- are to be credited with the design and specification of CRAM-MD5. This memo serves only to re-state CRAM-MD5 within the formal context of SASL, which specification it preceeded by several months.

6. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

7. Authors' Address

Lyndon Nerenberg
Orthanc Systems
508 - 11025 Jasper Avenue
Edmonton, Alberta
Canada T5K 0K7
Email: lyndon@orthanc.ab.ca

8. Full Copyright Statement

IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.