INTERNET-DRAFT
Intended Category: Standards Track
Expires in six months
Updates: RFC 2595

Editor: Kurt D. Zeilenga
OpenLDAP Foundation

4 November 2002

Plain SASL Mechanism
<draft-zeilenga-sasl-plain-01.txt>

Status of Memo

Abstract

This document defines a simple clear-text user/password Simple Authentication and Security Layer (SASL) mechanism called the PLAIN mechanism. The PLAIN mechanism intended to be used, in combination with data confidentiality services provided by a lower layer, in

protocols which lack a simple password authentication command.

Conventions

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 [KEYWORDS].

1. Background and Intended Usage

Clear-text passwords are simple, interoperate with almost all existing operating system authentication databases, and are useful for a smooth transition to a more secure password-based authentication mechanism. The drawback is that they are unacceptable for use over an unencrypted network connection.

This document defines the PLAIN Simple Authentication and Security Layer ([SASL]) mechanism for use in protocols with no clear-text login command (e.g., ACAP).

The name associated with this mechanism is "PLAIN".

The PLAIN SASL mechanism does not provide a security layer. This mechanism MUST NOT be used without adequate security protection as the mechanism affords no integrity nor confidentiality protection itself. The PLAIN SASL mechanism MUST NOT be advertised unless a strong encryption layer, such as provided by Transport Layer Security ([TLS]), is active.

This document updates RFC 2595, replacing Section 6. Changes since RFC 2595 are detailed in Appendix A.

2. PLAIN SASL mechanism

The mechanism consists of a single message from the client to the server. The client sends the authorization identity (identity to login as), followed by a NUL character, followed by the authentication identity (identity whose password will be used), followed by a NUL character, followed by the clear-text password. The client may leave the authorization identity empty if wishes the server to derive the authorization identity from the provided the authentication identity.

The authorization identity (authzid), authentication identity (authcid) and password (passwd) SHALL be transferred as [UTF-8] encoded strings of printable [Unicode] characters in Unicode

Normalisation Form KC [NFKC] delimitated by the NUL (U+0000) character.

The following characters are considered non-printable:
- control characters: U+0000..U+001F, U+007F..U+009F;
- replacement character: U+FFFD; and
- special characters and noncharacter: U+FEFF, U+FFFE, U+FFFF.

The server will verify the authentication identity (authcid) and password (passwd) with the system authentication database and verify that the authentication credentials permit the client to login as the authorization identity (authzid). If both steps succeed, the user is logged in.

The server MAY also use the password to initialize any new authentication database, such as one suitable for [CRAM-MD5] or [DIGEST-MD5].

The formal grammar for the client message using Augmented BNF [ABNF] follows.

```
message   = [authzid] NUL authcid NUL passwd
authcid   = 1*SAFE ; MUST accept up to 255 octets
authzid   = 1*SAFE ; MUST accept up to 255 octets
passwd    = 1*SAFE ; MUST accept up to 255 octets
NUL       = %x00

SAFE      = UTF1 / UTF2 / UTF3 / UTF4 / UTF5 / UTF6 / UTF7
            ;; any UTF-8 encoded Unicode printable character

UTF1   = %x01-7F
UTF2      = %xC0-DF 1(UTF0)
UTF3      = %xE0-EF 2(UTF0)
UTF4      = %xF0-F7 3(UTF0)
UTF5      = %xF8-FB 4(UTF0)
UTF6      = %xFC-FD 5(UTF0)
UTF0      = %x80-BF
```

4. Example

Here is an example of how this might be used to initialize a CRAM-MD5 authentication database for ACAP. "C:" and "S:" indicate lines sent by the client and server respectively.

```
S: * ACAP (SASL "CRAM-MD5") (STARTTLS)
C: a001 AUTHENTICATE "CRAM-MD5"
```

```
S: + "<1896.697170952@postoffice.reston.mci.net>"
C: "tim b913a602c7eda7a495b4e6e7334d3890"
S: a001 NO (TRANSITION-NEEDED)
   "Please change your password, or use TLS to login"
C: a002 STARTTLS
S: a002 OK "Begin TLS negotiation now"
<TLS negotiation, further commands are under TLS layer>
S: * ACAP (SASL "CRAM-MD5" "PLAIN" "EXTERNAL")
C: a003 AUTHENTICATE "PLAIN" {21+}
C: <NUL>tim<NUL>tanstaaftanstaaf
S: a003 OK CRAM-MD5 password initialized
```

In this example, <NUL> represents a single NUL (U+0000) character.

5. Security Considerations

The PLAIN mechanism relies on the TLS encryption layer for security. When used without TLS, it is vulnerable to a common network eavesdropping attack. Therefore PLAIN MUST NOT be advertised or used unless a suitable TLS encryption layer is active or backwards compatibility dictates otherwise.

When the PLAIN mechanism is used, the server gains the ability to impersonate the user to all services with the same password regardless of any encryption provided by TLS or other network privacy mechanisms. While many other authentication mechanisms have similar weaknesses, stronger SASL mechanisms such as the Kerberos-based GSSAPI mechanism address this issue. Clients are encouraged to have an operational mode where all mechanisms which are likely to reveal the user's password to the server are disabled.

Clients are encouraged to have an operational mode where all mechanisms which are likely to reveal the user's password to the server are disabled. It is RECOMMENDED that this mode be the default.

General SASL security considerations apply to this mechanism.

6. IANA Considerations

It is requested that the SASL Mechanism registry [IANA-SASL] entry for the PLAIN mechanism be updated to reflect that this document now provides its technical specification.

```
To: iana@iana.org
Subject: Updated Registration of SASL mechanism PLAIN
```

```
SASL mechanism name: PLAIN
Security considerations: See RFC XXXX.
Published specification (optional, recommended): RFC XXXX
Person & email address to contact for further information:
     Kurt Zeilenga <kurt@openldap.org>
     Chris Neuman <chris.newman@innosoft.com>
Intended usage: COMMON
Author/Change controller: IESG <iesg@ietf.org>
Note: Updates existing entry for PLAIN
```

7. Acknowledgement

This document is a revision of RFC 2595 by Chris Newman.

8. Normative References

[ABNF] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

[KEYWORDS] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", BCP 14 (also RFC 2119), March 1997.

[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/tr15-22.html).

[SASL] Myers, J., "Simple Authentication and Security Layer (SASL)", RFC 2222bis (a work in progress).

[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 #28: Unicode 3.2 (http://www.unicode.org/reports/tr28/tr28-3.html).

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

[TLS] T. Dierks, C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

9. Informative References

[CRAM-MD5] J. Klensin, R. Catoe, and P. Krumviede, "IMAP/POP

AUTHorize Extension for Simple Challenge/Response", RFC 2195, September 1997.

[DIGEST-MD5] P. Leach, C. Newman, "Using Digest Authentication as a SASL Mechanism", RFC 2831, May 2000.

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

10. Editor's Address

Kurt Zeilenga
OpenLDAP Foundation

Email: kurt@OpenLDAP.org

Appendix A. Changes since RFC 2595

This appendix is non-normative.

This document replaces Section 6 of RFC 2595.

The specification clarifies the normalized form to be used and details which characters are considered to be printable. The ABNF grammar was updated.

Additionally, a number of editorial changes were made.

Full Copyright Statement