Network Working Group
Internet Draft
Document: draft-melnikov-sasl-auxprop-attrs-00.txt

A. Melnikov
Isode Limited

April 2004
Expires in six months

An LDAP Schema for CMU SASL auxiliary properties plugins

Status of this Memo

Abstract

The CMU SASL implementation of the RFC 2222 defines an API for auxiliary properties (auxprop) plugins. Auxprop plugins can store properties. A property can be a user password in cleartext or in a hashed form used by a particular SASL mechanism, or any other information associated with the user. This document describes a schema for the storage of auxprop properties in an LDAP directory server.

1. Conventions used in this document

The key words "MUST", "MUST NOT", "SHOULD", "SHOULD NOT", and "MAY" in this document are to be interpreted as defined in "Key words for use in RFCs to Indicate Requirement Levels" [KEYWORDS].

<<1.3.6.1.4.1.3.8 - "ldapResources" under CMU node.

1.3.6.1.4.1.3.8.1 - cmuSaslAuxprop

1.3.6.1.4.1.3.8.1.0 - Syntaxes

1.3.6.1.4.1.3.8.1.1 - Attributes types

1.3.6.1.4.1.3.8.1.2 - Object classes >>

2. SASL related Attribute Types

This document defines the attribute types cmusaslsecretCRAM-MD5, cmusaslsecretDIGEST-MD5, cmusaslsecretOTP and cmusaslsecretSRP. Their definition is provided below.

```
( 1.3.6.1.4.1.3.8.1.1.1
        NAME 'cmusaslsecretCRAM-MD5'
        DESC 'Prehashed password as described in CRAM-MD5'
     EQUALITY octetStringMatch
        SINGLE-VALUE
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{32} )
```

cmusaslsecretCRAM-MD5 attribute contains the binary representation of the following C structure:

```
typedef struct HMAC_MD5_STATE_s {
    UINT4 ipad_state[4];
    UINT4 opad_state[4];
```

```
} HMAC_MD5_STATE;
```

i.e. 16 bytes (4 element array of 32bit integers, each element in network byte order) of ipad is followed by 16 bytes (4 element array of 32bit integers, each element in network byte order) of opad. ipad and opad are calculated as defined in [SASL-CRAM].

```
( 1.3.6.1.4.1.3.8.1.1.2
        NAME 'cmusaslsecretDIGEST-MD5'
        DESC 'Shared secret for DIGEST-MD5'
     EQUALITY octetStringMatch
        SINGLE-VALUE
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.40{16} )
```

The cmusaslsecretDIGEST-MD5 attribute contains the binary representation of SS (16-octets) as defined in section 2.1.2.1 of [SASL-DIGEST]:

```
SS = H( { unq(username-value), ":", unq(realm-value), ":", passwd } )
```

```
( 1.3.6.1.4.1.3.8.1.1.3
        NAME 'cmusaslsecretOTP'
        DESC 'OTP secret'
     EQUALITY octetStringMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

The cmusaslsecretOTP attribute is a tab separated octet string that contains information relevant for OTP [SASL-OTP] authentication. The syntax of the string is as follows:

```
  <alg> \t <seq> \t <seed> \t <otp> \t <timeout>
```

where \t is the horizontal tab character (%x09),

<alg> - name of the hashing algorithm as described in [SASL-OTP];

<otp> - 16 hex digits (in lowercase) of the 8-byte OTP hash;

<seq> - 4 digit unsigned integer that specifies how many times the user is allowed to log in using the password before it has to change it. This value is decremented each time the user has successfully authenticated;

<seed> - random string that doesn't contain \t (<<and no NULs?>>)

<timeout> 20 digit unsigned integer, the time since the Epoch (00:00:00 UTC, January 1, 1970), measured in seconds. It defines the time when the record lock expires. This value is used to lock

the record, as OTP doesn't allow for simultaneous authentication by the same user.

This attribute is multivalued. For example, it may contain multiple OTP hashes for different hashing algorithms.

```
( 1.3.6.1.4.1.3.8.1.1.4
        NAME 'cmusaslsecretSRP'
        DESC 'base64 encoded SRP secret'
     EQUALITY octetStringMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.40 )
```

This is the base64 encoding of the following data described in [SASL-SRP]:

{ utf8(mda) mpi(v) os(salt) }

where

mda - message digest algorithm name as defined in [SASL-SRP]

v - password verifier (<<See: RFC 2945>>)

salt - a random string, 1 to 255 octets in length

This attribute is multivalued. For example, it may contain data for multiple message digest algorithms.

<<cmusaslsecretPLAIN is deprecated in favor of userPassword>>

3. Object Classes

This document defines the following object class:

```
( 1.3.6.1.4.1.3.8.1.2.1
     NAME 'cmuSaslUser'
     SUP top
     AUXILIARY
     MAY ( userPassword $ cmusaslsecretCRAM-MD5 $ cmusaslsecretDIGEST-MD5 $
           cmusaslsecretOTP $ cmusaslsecretSRP) )
```

The cmusaslsecretCRAM-MD5, cmusaslsecretDIGEST-MD5, cmusaslsecretOTP and cmusaslsecretSRP attribute types are described in section 2 of this document. The userPassword attribute type is defined in [RFC2256].

4. Security considerations

<<Rant about userPassword>>

5. References

5.1. Normative References

[KEYWORDS] Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, March 1997

[RFC2256] Wahl, A., "A Summary of the X.500(96) User Schema for use with LDAPv3", RFC 2256, December 1997

[SASL-CRAM] Nerenberg, L. (Editor), "The CRAM-MD5 SASL Mechanism", work in progress, draft-ietf-sasl-crammd5-XX.txt, replaces RFC 2195

[KEYED-MD5] Krawczyk, Bellare, Canetti, "HMAC: Keyed-Hashing for Message Authentication", RFC 2104, IBM and UCSD, February 1997.

[SASL-DIGEST] Leach, P., Newman, C., Melnikov, A., "Using Digest Authentication as a SASL Mechanism", work in progress, draft-ietf-sasl-rfc2831bis-XX.txt, replaces RFC 2831

[SASL-OTP] Newman, C., "The One-Time-Password SASL Mechanism", RFC 2444, October 1998

[SASL-SRP] Burdis, K.R., Naffah, R., "Secure Remote Password SASL Mechanism", work in progress, draft-burdis-cat-srp-sasl-XX.txt

5.2. Informative References

6. Author's Address

Alexey Melnikov
Isode Limited
5 Castle Business Village
36 Station Road
Hampton, Middlesex
TW12 2BX, United Kingdom

Email: Alexey.Melnikov@isode.com
URI: http://www.melnikov.ca/

7. Acknowledgments

The author of the document would like to thank Howard Chu for reminding that this document has to be written; to Chris Ridd, Damy Mahl and Rob Siemborski for comments and suggestions to this document; to Ken Murchison for designing the OTP and SRP secret formats.

8. Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

9. Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights 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; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat 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 implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.