SASL Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 31, 2010

A. Melnikov
Isode Limited

July 30, 2009

LDAP schema for storing SCRAM secrets
draft-melnikov-sasl-scram-ldap-02

Status of this Memo

Copyright Notice

Abstract

This memo describes how authPassword LDAP attribute can be used for storing secrets used by Salted Challenge Response (SCRAM) Simple Authentication and Security Layer (SASL) Mechanism.

Note

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, and should be sent to ietf-sasl@imc.org.

Table of Contents

1. Overview

This memo defines a family of schema for authPassword attribute defined in [AUTHPASS]. Non terminal references in the following ABNF are defined in either [AUTHPASS] or [RFC5234].

The "scheme" part of the authPassword attribute is the SCRAM mechanism name (always without the "-PLUS" suffix), e.g. "SCRAM-SHA-1". See [SCRAM] for the exact syntax of SCRAM mechanism names.

The "authInfo" part of the authPassword attribute is the iteration count, followed by ":" and base-64 [BASE64] encoded salt.

The "authValue" part of the authPassword attribute is the base-64 [BASE64] encoded StoredKey [SCRAM], followed by ":" and base-64 [BASE64] encoded ServerKey [SCRAM].

Syntax of the attribute can be expressed using ABNF [RFC5234]:

```
scram-mech     = "SCRAM-SHA-1"
                 ;; Complies with ABNF for <scheme>

scram-authInfo = iter-count ":" salt
                 ;; Complies with ABNF for <authInfo>

scram-authValue = stored-key ":" server-key
                 ;; Complies with ABNF for <authValue>

iter-count   = %x31-39 *DIGIT
                ; a positive number without leading zeros

salt         = <<base-64 encoded value>>

stored-key   = <<base-64 encoded value>>

server-key   = <<base-64 encoded value>>
```

[[anchor2: Add an example.]]

Note that the authPassword attribute is multivalued. For example, it may contain multiple SCRAM hashes for different hashing algorithms.

2. Security Considerations

Servers MUST validate format of the authPassword attribute before using it for performing a SCRAM authentication exchange. It is

possible that an attacker compromised the LDAP server or got access to the entry containing the attribute in order to exploit a vulnerability in the subsystem performing SCRAM authentication exchange. Big iteration counts and invalid base-64 encoding are two possible (but not the only) exploits in the format specified in the document.

3. IANA Considerations

No action is required from IANA.

4. Acknowledgements

The author gratefully acknowledges the feedback provided by Chris Newman and Kurt Zeilenga.

5. References

5.1. Normative References

[AUTHPASS] Zeilenga, K., "LDAP Authentication Password Schema", RFC 3112, May 2001.

[BASE64] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, October 2006.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[SCRAM] Menon-Sen, A. and C. Newman, "Salted Challenge Response (SCRAM) SASL Mechanism", draft-newman-auth-scram-07.txt (work in progress), July 2008.

5.2. Informative References

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

Author's Address

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

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