LDAP schema for storing SCRAM secrets
draft-melnikov-sasl-scram-ldap-04

Abstract

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

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 sasl@ietf.org mailing list.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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.

This Internet-Draft will expire on May 12, 2010.

Copyright Notice
Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the BSD License.

Table of Contents

1. Conventions Used in This Document ................................ 3
2. Overview ........................................................................... 3
3. Security Considerations ...................................................... 4
4. IANA Considerations ............................................................ 5
5. Acknowledgements ............................................................... 5
6. Normative References ........................................................... 5
   Author’s Address ................................................................. 6
1. Conventions Used in This Document

   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 [RFC2119].

2. Overview

   This document describes how the authPassword LDAP attribute [AUTHPASS] can be used for storing secrets used by [SCRAM] Simple Authentication and Security Layer [RFC4422] Mechanisms.

   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 (iter-count in the ABNF below), 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]. Non terminal references in the following ABNF are defined in either [AUTHPASS], [RFC4422] or [RFC5234].
scram-mech = "SCRAM-SHA-1" / scram-mech-ext
; Complies with ABNF for <scheme>
; defined in [AUTHPASS].

scram-authInfo = iter-count "::" salt
; Complies with ABNF for <authInfo>
; defined in [AUTHPASS].

scram-authValue = stored-key "::" server-key
; Complies with ABNF for <authValue>
; defined in [AUTHPASS].

iter-count = %x31-39 *DIGIT
; SCRAM iteration count.
; A positive number without leading zeros

salt = <base-64 encoded value>

stored-key = <base-64 encoded value>
; See definition in [SCRAM]

server-key = <base-64 encoded value>
; See definition in [SCRAM]

scram-mech-ext = "SCRAM-" 1*9mech-char
; Other SCRAM mechanisms registered
; in the IANA registry for SASL
; mechanism names.

mech-char = <Defined in RFC 4422>

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

3. Security Considerations

This document defines how authPassword attribute can be used to store SCRAM secrets. So security considerations relevant to [SCRAM] and hash function used with it are also relevant to this document.

General security considerations related to authPassword attribute (as specified in [AUTHPASS]) also apply to use of authPassword as specified in this document. In particular values of authPassword SHOULD be protected as if they were clear text passwords. A read operation on this attribute which is not protected by a privacy layer
(such as IPSec or TLS) can expose this attribute to an attacker who
a) would be able to use the intercepted value to impersonate the
user to all servers providing SCRAM access using the same hash
function, password, iteration count and salt, or b) would be able to
perform an offline dictionary or brute-force attack in order to
recover the user’s password.

Servers MUST validate the 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 the 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.

4. IANA Considerations

No action is required from IANA.

5. Acknowledgements

The author gratefully acknowledges the feedback provided by Chris
Newman, Kurt Zeilenga, Chris Lonvick, Peter Saint-Andre, Barry Leiba
and Chris Ridd.

6. Normative References

[AUTHPASS] Zeilenga, K., "LDAP Authentication Password Schema",

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

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

[RFC4422] Melnikov, A. and K. Zeilenga, "Simple Authentication and


"Salted Challenge Response (SCRAM) SASL Mechanism",
draft-ietf-sasl-scram-07.txt (work in progress),
September 2009.

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/