Network Working Group   A. Melnikov
Internet Draft   Isode Limited
Document: draft-melnikov-ldap-distr-auth-00.txt   Kurt D. Zeilenga
Expires in six months   OpenLDAP Foundation
                                                          July 2004

                 Distributed SASL authentication in LDAP

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. Internet Drafts may be updated, replaced, or obsoleted
   by other documents at any time. It is not appropriate 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 Draft Standard for the Internet Community. Discussion
   and suggestions for improvement are requested. Distribution of this
   draft is unlimited.

Abstract

   This document was prompted by a desire to allow deployments of
   distributed SASL implementations, so that all authentication can be
   performed in a one central place. It tries to fulfill the following
   requirements:

   1) The SASL framework is client/server authentication, but it doesn't
   preclude either the client or the server implementations from being
   distributed.

   2) It might be also desirable to proxy an authentication exchange
   whether it was initiated over LDAP or another SASL-supporting
   protocol.

   This document defines a Distributed Authentication LDAP extended
   operation, that enables applications (including LDAP proxies and
   gateways) that authenticate using SASL, to use LDAP for performing
   authentication, by forwarding the SASL authentication requests to an
   LDAP 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].

   All Basic Encoding Rules (BER)[BER] encodings follow the conventions
   found in Section 5.1 of [RFC2251].

2.   Distributed authentication Request and Response

2.1. Distributed authentication Request

   The Distributed authentication Request is sent as an LDAP extended
   operation. The requestName is 1.3.6.1.4.1.453.23.1. The requestValue
   is the BER [BER] encoding of the following ChainedAuthRequestValue
   ASN.1 definition.

   ChainedAuthRequestValue ::= SEQUENCE {
        bindRequest   BindRequest,
        chainingAuthArguments   ChainingAuthArguments }

   ChainingAuthArguments ::= SEQUENCE {

```
      serviceName              [0] LDAPString DEFAULT '6C646170'H,
                                   -- the default value is string "ldap"
      serviceProtocol          [1] ServiceProtocol DEFAULT (0),
      serverHostname           [2] HostName,
      clientEndpoint           [3] Endpoint OPTIONAL,
      serverEndpoint           [4] Endpoint OPTIONAL,
      controls                 [5] Controls OPTIONAL,
      ... }

Endpoint ::= CHOICE {
      ipv4                     [0] Ipv4Endpoint,
      ipv6                     [1] Ipv6Endpoint,
      ... }

Ipv4Endpoint ::= SEQUENCE {
      ipAddress                [0] Ipv4Address,
      port                     [1] INTEGER (1 .. 65535) }

Ipv6Endpoint ::= SEQUENCE {
      ipAddress                [0] Ipv6Address,
      port                     [1] INTEGER (1 .. 65535) }

ServiceProtocol ::= ENUMERATED {
      tcp                      (0),
      udp                      (1),
      ... }

Ipv4Address ::= OCTET STRING -- UTF-8 encoded
              -- Constrained to <IPv4address> [RFC2373]

Ipv6Address ::= OCTET STRING -- UTF-8 encoded
              -- Constrained to <IPv6reference> [RFC2373]

HostName ::= OCTET STRING -- UTF-8 encoded
              -- Constrained to <hostname> [RFC2396]
```

BindRequest and Controls are defined in [RFC2251].

<<serviceName, serviceProtocol, serverHostname, clientEndpoint and
serverEndpoint MUST NOT change between any 2 steps of the same
authentication exchange.>>

2.2. Distributed authentication Response

The Distributed authentication Response is sent as an LDAP extended
operation. The requestName is omitted. The requestValue is the BER
[BER] encoding of the following ChainedAuthResponse ASN.1 definition.

```
ChainedAuthResponse ::= SEQUENCE {
    bindResponse            BindResponse,
    controls                [0] Controls OPTIONAL,
    ... }
```

<<Do we need to pass back any additional data? Like some sort of ID
associated with the enclosed bind exchange?>>

<<Do we need new error codes?>>

BindResponse and Controls are defined in [RFC2251].

2.3. Semantics of Distributed authentication Request and Response

In order to avoid confusion, this section will use the following 3
terms to define parties involved in a Distributed Authentication
exchange. The term "server" refers to an LDAP server which is the
recipient of Distribution Authentication Request. The term "client"
refers to an LDAP client which sends the Distribution Authentication
Request. The "client" also acts as a SASL server (in a normal sense
of this word) for another authentication exchange, which is happening
between an "application" and the "client". The authentication
exchange may be carried by any SASL-supporting protocol, which is not
necessarily LDAP.

A Distributed authentication Request consist of a bind Request
information, together with some additional information that would
enable the server to perform authentication on client's behalf. The
additional information is described by chainingAuthArguments.

In a case when the client is an application level gateway between
another SASL-supporting protocol and LDAP, the
chainingAuthArguments.serviceName must be set to the service name
[GSSAPI] of the protocol used to carry out authentication exchange
between the application and the client. For example, if the client
is an SMTP server [SMTP] this value would be set to "smtp".

The chainingAuthArguments.serviceProtocol is set to 0 (i.e. TCP) by
default. This field is reserved for future extensibility when the
authentication exchange between the application and the client
doesn't happen over TCP.

The chainingAuthArguments.serverHostname is the fully qualified
hostname that was used by the client when it has accepted the
original authentication request from the application. This field is
required, because the client may, for example, listen on multiple
interfaces that may have different hostnames associated with them.

The chainingAuthArguments.clientEndpoint and
chainingAuthArguments.serverEndpoint define connection endpoint
information for the authentication exchange carried out between the
application and the client respectively.

The chainingAuthArguments.controls member contains controls that are
associated with the bindResponse. The controls serve the same purpose
as controls attached to a bind request.

<<Describe how to handle a negotiated SASL security layer>>

3.   Security considerations

Distributed authentication extended operation assumes that both
endpoints are secure. A compromise of one endpoint may make it
possible to use the operation to mount a MITM attack. <<More details
here?>>

An LDAP server should (<<SHOULD?>>) only accept Distributed
authentication Requests from trusted peers and only over properly
protected channel. It is recommended that before issuing the
Distributed authentication operation the protocol peers:

  - establish each other identities through appropriate authentication
    mechanism,
  - establish appropriate data integrity, data confidentiality, and
    other protections,
  - establish an LDAP association between the initiating peer and the
    responding peer.

Servers may place access control or other restrictions upon the use
of this operation.

As with any other extended operations, general LDAP security
considerations [RFC3377] apply.

4.   IANA Considerations

This OID 1.3.6.1.4.1.453.23.1 to identify the LDAP Distributed
authentication extended operation. This OID was assigned by Isode
Limited, under its IANA-assigned private enterprise allocation
[PRIVATE], for use in this specification.

Registration of this protocol mechansism is requested [RFC3383].

Subject: Request for LDAP Protocol Mechanism Registration

Object Identifier: 1.3.6.1.4.1.453.23.1

Description: Distributed bind operation

Person & email address to contact for further information:
     Alexey Melnikov <Alexey.Melnikov@isode.com>

Usage: Extended Operation

Specification: RFCxxxx

Author/Change Controller: IESG

Comments: none

5. References

5.1. Normative References

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

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

[RFC2251] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory
Access Protocol (v3)", RFC 2251, December 1997.

[RFC3377] Hodges, J. and R. Morgan, "Lightweight Directory Access
Protocol (v3): Technical Specification", RFC 3377, September 2002.

[SASL] Melnikov, A. (editor), "Simple Authentication and Security
Layer (SASL)", draft-ietf-sasl-rfc2222bis-xx.txt, a work in progress.

[RFC2373] Hinden, R., Deering, S., "IP Version 6 Addressing
Architecture", RFC 2373, July 1998.

[RFC 2396] Berners-Lee, T., Fielding, R., Masinter, L., "Uniform
Resource Identifiers (URI): Generic Syntax", RFC 2396, August 1998.

[GSSAPI] Linn, J., "Generic Security Service Application Program
Interface, Version 2, Update 1", RFC 2743, January 2000.

5.2. Informative References

[RFC3383] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", RFC 3383, September 2002.

[PRIVATE] IANA, "Private Enterprise Numbers", http://www.iana.org/assignments/enterprise-numbers.

[SMTP] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

<<[LDAP-AUTHMECH] Harrison, R. (Editor), "LDAP: Authentication Methods and Connection Level Security Mechanisms", work in progress, draft-ietf-ldapbis-authmeth-xx.txt>>

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/

Kurt D. Zeilenga
OpenLDAP Foundation

Email: Kurt@OpenLDAP.org

7. Acknowledgments

Thanks to Steve Kille and Chris Ridd for providing useful feedback and suggestions.

8. IPR Disclosure Acknowledgement

By submitting this Internet-Draft, I certify that any applicable patent or other IPR claims of which I am aware have been disclosed, and any of which I become aware will be disclosed, in accordance with

RFC 3668.

9.   Full Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject
to the rights, licenses and restrictions contained in BCP 78, and
except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an
"AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS
OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET
ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR 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.

Acknowledgement

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

10.   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.