Network Working Group   Rob Weltman
INTERNET-DRAFT   Netscape Communications Corp.
                                                                Tim Howes
                                             Netscape Communications Corp.
                                                        November 20, 1997

LDAP Proxied Authentication Control
draft-weltman-ldapv3-proxy-00.txt

Status of this Memo

Abstract

This document defines support for the Proxied Authentication Control. Controls are an LDAP protocol version 3 extension, to allow passing arbitrary control information along with a standard request to a server, and to receive arbitrary information back with a standard result. The Proxied Authentication Control allows a connection with sufficient privileges to assume the identity of another entry for the duration of an LDAP request.

1. Introduction

Version 3 of the LDAP protocol provides a means of supplying arbitrary additional information along with a request to an LDAP server, and receiving arbitrary additional response information. The Control protocol extension is described in [1], section 4.1.12. This document defines support for proxied authentication using the Control mechanism.

The key words "MUST", "SHOULD", and "MAY" used in this document are to be interpreted as described in [2].

2. Publishing support for the Proxied Authentication Control

Support for the virtual list view extended operation is indicated by the presence of the OID "2.16.840.1.113730.3.4.12" in the supportedExtensions attribute of a server's root DSE.

3. Proxied Authentication Control

This control may be included in any search, modify, delete, or modrdn request message as part of the controls field of the LDAPMessage, as defined in [1].

```
proxyAuthControl ::= SEQUENCE {
        controlType     2.16.840.1.113730.3.4.12,
        criticality     BOOLEAN DEFAULT FALSE,
        controlValue    proxyAuthValue
}
```

The criticality SHOULD be included and SHOULD be TRUE. If it is not TRUE, and the requester is not authorized to use proxied authentication within the target Directory tree, the requester s own authentication will be used to execute the request. The controlValue is an OCTET STRING, whose value is the BER encoding of a value of the following:

```
proxyAuthValue ::= LDAPDN
```

4. Permission to execute as proxy

An LDAP server supporting the proxied authentication control may choose to honor or not honor a particular request. If the control is supported but a particular request is denied, the server MUST return the error code insufficientAccessRights. A typical implementation will evaluate if the requester has proxy access rights at the base DN of the request. If the requester has proxy access rights, and if the proxy DN corresponds to a valid entry in the directory managed by the server, the request will be honored. If the request is honored, it will be executed as if submitted by the proxy identity.

5. Security Considerations

The proxied authentication control method is subject to standard LDAP security considerations. The control may be passed over a secure as well as over an insecure channel. No additional confidential information is passed in the control.

Note that the server is responsible for determining if a proxied authentication request is to be honored.

6. Copyright

7. Bibliography

[1] M. Wahl, T. Howes, S. Kille, "Lightweight Directory Access Protocol (v3)", Internet Draft draft-ietf-asid-ldapv3-protocol-06.txt, July 1997.

[2] Bradner, Scott, "Key Words for use in RFCs to Indicate Requirement Levels", draft-bradner-key-words-03.txt, January, 1997.

8. Author s Addresses

Rob Weltman
Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043
USA
+1 650 937-3301
rweltman@netscape.com

Tim Howes
Netscape Communications Corp.
501 E. Middlefield Rd.
Mountain View, CA 94043
USA
+1 650 937-3419
howes@netscape.com