Network Working Group M. Swift
Request for Comments: 3244 University of Washington
Category: Informational J. Trostle
Cisco Systems
J. Brezak
Microsoft
February 2002

Microsoft Windows 2000 Kerberos Change Password and Set Password Protocols

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This memo specifies Microsoft's Windows 2000 Kerberos change password and set password protocols. The Windows 2000 Kerberos change password protocol interoperates with the original Kerberos change password protocol. Change password is a request reply protocol that includes a KRB_PRIV message that contains the new password for the user.

1. Introduction

Microsoft's Windows 2000 Kerberos change password protocol interoperates with the original Kerberos change password protocol. Change password is a request reply protocol that includes a KRB_PRIV message that contains the new password for the user. The original change password protocol does not allow an administrator to set a password for a new user. This functionality is useful in some environments, and this proposal extends the change password protocol to allow password setting. The changes are: adding new fields to the request message to indicate the principal which is having its password set, not requiring the initial flag in the service ticket, using a new protocol version number, and adding three new result codes.

2. The Protocol

The service accepts requests on UDP port 464 and TCP port 464 as well. The protocol consists of a single request message followed by a single reply message. For UDP transport, each message must be fully contained in a single UDP packet.

For TCP transport, there is a 4 octet header in network byte order that precedes the message and specifies the length of the message.

Request Message

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         message length        |    protocol version number    |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          AP_REQ length        |         AP_REQ data           /
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    /                        KRB-PRIV message                       /
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

All 16 bit fields are in big-endian order.

message length field: contains the number of bytes in the message including this field.

protocol version number: contains the hex constant 0xff80 (big-endian integer).

AP-REQ length: length of AP-REQ data, in bytes. If the length is zero, then the last field contains a KRB-ERROR message instead of a KRB-PRIV message.

AP-REQ data: (see [1]) The AP-REQ message must be for the service principal kadmin/changepw@REALM, where REALM is the REALM of the user who wishes to change/set his password. The authenticator in the AP-REQ must include a subsession key. (NOTE: The subsession key must be pseudo-randomly generated and must never be reused for multiple authenticators.) To enable setting of passwords, it is not required that the initial flag be set in the Kerberos service ticket.

KRB-PRIV message (see [1]) This user-data field in the KRB-PRIV message is encrypted using the subkey from the authenticator in the AP-REQ data. The usec and seq-number fields of the KRB_PRIV message are present and have the same value as the seq-number field in the authenticator from the AP_REQ message (the seq-number in the authenticator will be present). The server ignores the optional r-address field in the KRB_PRIV message, if it is present.

The user-data component of the message consists of the following ASN.1 structure encoded as an OCTET STRING:

```
   ChangePasswdData ::=  SEQUENCE {
                       newpasswd[0]   OCTET STRING,
                       targname[1]    PrincipalName OPTIONAL,
                       targrealm[2]   Realm OPTIONAL
                       }
```

The server must verify the AP-REQ message, check whether the client principal in the ticket is authorized to set/change the password (either for that principal, or for the principal in the targname field if present), and decrypt the new password. The server also checks whether the initial flag is required for this request, replying with status 0x0007 if it is not set and should be. An authorization failure is cause to respond with status 0x0005. For forward compatibility, the server should be prepared to ignore fields after targrealm in the structure that it does not understand.

The newpasswd field contains the cleartext password, and the server will apply any local policy checks including password policy checks. The server then generates the appropriate keytypes from the password and stores them in the KDC database. If all goes well, status 0x0000 is returned to the client in the reply message (see below).

Reply Message

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |         message length        |    protocol version number    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          AP_REP length        |         AP-REP data           /
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 /                        KRB-PRIV message                       /
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

All 16 bit fields are in big-endian order.

message length field: contains the number of bytes in the message including this field.

protocol version number: contains the hex constant 0x0001 (big-endian integer). (The reply message has the same format as the original change password protocol.)

AP-REP length: length of AP-REP data, in bytes. If the length is zero, then the last field contains a KRB-ERROR message instead of a KRB-PRIV message.

AP-REP data: the AP-REP is the response to the AP-REQ in the request packet.

KRB-PRIV message: This KRB-PRIV message must be encrypted with the subsession key from the authenticator in the AP-REQ data.

The server will respond with a KRB-PRIV message unless it cannot decode the client AP-REQ or KRB-PRIV message, in which case it will respond with a KRB-ERROR message. NOTE: Unlike change password version 1, the KRB-ERROR message will be sent back without any encapsulation.

The user-data component of the KRB-PRIV message, or e-data component of the KRB-ERROR message, consists of the following data.

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |          result code          |        result string         /
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

result code (16 bits) (result codes 0-4 are from the original change password protocol):

The result code must have one of the following values (big-endian integer):

KRB5_KPASSWD_SUCCESS	0	request succeeds (This value is not allowed in a KRB-ERROR message)
KRB5_KPASSWD_MALFORMED	1	request fails due to being malformed
KRB5_KPASSWD_HARDERROR	2	request fails due to "hard" error in processing the request (for example, there is a resource or other problem causing the request to fail)

KRB5_KPASSWD_AUTHERROR	3	request fails due to an error in authentication processing
KRB5_KPASSWD_SOFTERROR	4	request fails due to a "soft" error in processing the request
KRB5_KPASSWD_ACCESSDENIED	5	requestor not authorized
KRB5_KPASSWD_BAD_VERSION	6	protocol version unsupported
KRB5_KPASSWD_INITIAL_FLAG_NEEDED	7	initial flag required

0xFFFF is returned if the request fails for some other reason. Although only a few non-zero result codes are specified here, the client should accept any non-zero result code as indicating failure.

result string:

This field contains information which might be useful to the user, such as feedback about policy failures. The string is encoded in UTF-8. It may be omitted if the server does not wish to include it. If it is present, the client will display the string to the user.

3. Security Considerations

Password policies should be enforced to make sure that users do not pick passwords (for change password) that are vulnerable to brute force password guessing attacks. An administrator who is authorized to set other principal’s passwords is highly trusted and must also carefully protect his/her own credentials.

4. References

[1] Kohl, J. and C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

5. Authors' Addresses

Mike Swift
University of Washington
Seattle, WA

EMail: mikesw@cs.washington.edu

Jonathan Trostle
Cisco Systems
170 W. Tasman Dr.
San Jose, CA 95134

EMail: john3725@world.std.com

John Brezak
Microsoft
1 Microsoft Way
Redmond, WA 98052

EMail: jbrezak@microsoft.com

6. Full Copyright Statement

Acknowledgement

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