Network Working Group
<draft-ietf-cat-kerb-chg-password-02.txt>
Internet-Draft

M. Horowitz
Stonecast, Inc.

August, 1998

Kerberos Change Password Protocol

Status of this Memo

Abstract

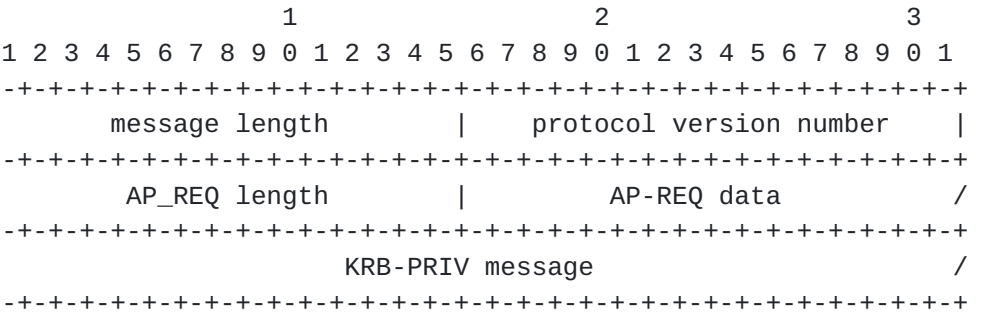
The Kerberos V5 protocol [RFC1510] does not describe any mechanism for users to change their own passwords. In order to promote interoperability between workstations, personal computers, terminal servers, routers, and KDC's from multiple vendors, a common password changing protocol is required.

Overview

When a user wishes to change his own password, or is required to by local policy, a simple request of a password changing service is necessary. This service must be implemented on at least one host for each Kerberos realm, probably on one of the kdc's for that realm. The service must accept requests on UDP port 464 (kpasswd), and may accept requests on TCP port 464 as well.

The protocol itself 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.

Request Message



message length (16 bits)
Contains the length of the message, including this field, in bytes (big-endian integer)

protocol version number (16 bits)
Contains the hex constant 0x0001 (big-endian integer)

AP-REQ length (16 bits)
length (big-endian integer) of AP-REQ data, in bytes.

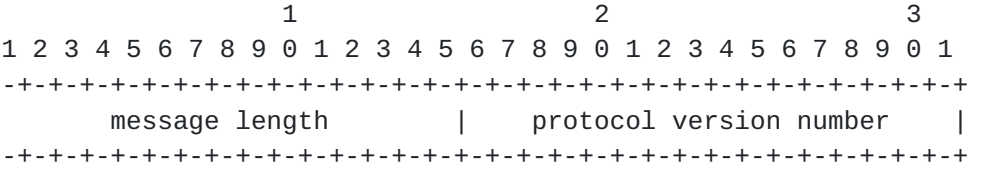
AP-REQ data, as described in RFC1510 (variable length)
This AP-REQ must be for the service principal kadmin/changepw@REALM, where REALM is the REALM of the user who wishes to change his password. The Ticket in the AP-REQ must be derived from an AS request (thus having the INITIAL flag set), and must include a subkey in the Authenticator.

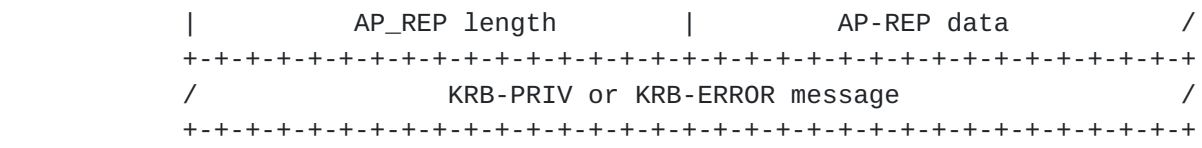
KRB-PRIV message, as described in RFC1510 (variable length)
This KRB-PRIV message must be generated using the subkey in the Authenticator in the AP-REQ data. The user-data component of the message must consist of the user's new password.

The server must verify the AP-REQ message, decrypt the new password, perform any local policy checks (such as password quality, history, authorization, etc.) required, then set the password to the new value specified.

The principal whose password is to be changed is the principal which authenticated to the password changing service. This protocol does not address administrators who want to change passwords of principal besides their own.

Reply Message





message length (16 bits)

Contains the length of the message, including this field, in bytes (big-endian integer),

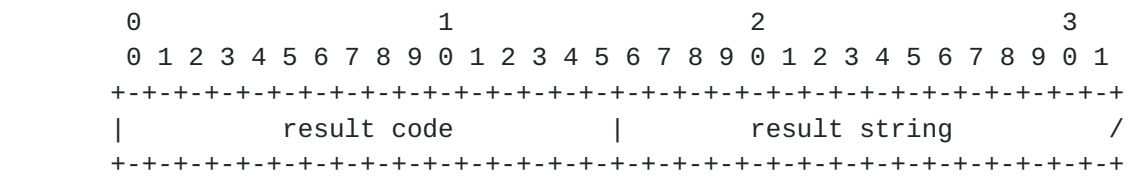
protocol version number (16 bits)
Contains the hex constant 0x0001 (big-endian integer)

AP-REP length (16 bits)
length of AP-REP data, in bytes. If the the length is zero, then the last field will contain a KRB-ERROR message instead of a KRB-PRIV message.

AP-REP data, as described in RFC1510 (variable length)
The AP-REP corresponding to the AP-REQ in the request packet.

KRB-PRIV or KRB-ERROR message, as described in RFC1510 (variable length)
If the AP-REP length is zero, then this field contains a KRB-ERROR message. Otherwise, it contains a KRB-PRIV message. This KRB-PRIV message must be generated using the subkey in the Authenticator in the AP-REQ data.

The user-data component of the KRB-PRIV message, or e-data component of the KRB-ERROR message, must consist of the following data:



result code (16 bits)
The result code must have one of the following values (big-endian integer):
0x0000 if the request succeeds. (This value is not permitted in a KRB-ERROR message.)
0x0001 if the request fails due to being malformed
0x0002 if the request fails due to a "hard" error processing the request (for example, there is a resource or other problem causing the request to fail)
0x0003 if the request fails due to an error in authentication processing
0x0004 if the request fails due to a "soft" error processing the request (for example, some policy or other similar consideration is causing the request to be rejected).
0xFFFF 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 (variable length)
This field should contain information which the server thinks might be useful to the user, such as feedback about policy

failures. The string must be encoded in UTF-8. It may be omitted if the server does not wish to include it. If it is present, the client should display the string to the user. This field is analogous to the string which follows the numeric code in SMTP, FTP, and similar protocols.

Dropped and Modified Messages

An attacker (or simply a lossy network) could cause either the request or reply to be dropped, or modified by substituting a KRB-ERROR message in the reply.

If a request is dropped, no modification of the password/key database will take place. If a reply is dropped, the server will (assuming a valid request) make the password change. However, the client cannot distinguish between these two cases.

In this situation, the client should construct a new authenticator, re-encrypt the request, and retransmit. If the original request was lost, the server will treat this as a valid request, and the password will be changed normally. If the reply was lost, then the server should take care to notice that the request was a duplicate of the prior request, because the "new" password is the current password, and the password change time is within some implementation-defined replay time window. The server should then return a success reply (an AP-REP message with result code == 0x0000) without actually changing the password or any other information (such as modification timestamps).

If a success reply was replaced with an error reply, then the application performing the request would return an error to the user. In this state, the user's password has been changed, but the user believes that it has not. If the user attempts to change the password again, this will probably fail, because the user cannot successfully provide the old password to get an INITIAL ticket to make the request. This situation requires administrative intervention as if a password was lost. This situation is, unfortunately, impossible to prevent.

Security Considerations

This document deals with changing passwords for Kerberos. Because Kerberos is used for authentication and key distribution, it is important that this protocol use the highest level of security services available to a particular installation. Mutual authentication is performed, so that the server knows the request is valid, and the client knows that the request has been received and processed by the server.

There are also security issues relating to dropped or modified messages which are addressed explicitly.

References

[RFC1510] Kohl, J. and Neuman, C., "The Kerberos Network
Authentication Service (V5)", RFC 1510, September 1993.

Author's Address

Marc Horowitz
Stonecast, Inc.
108 Stow Road
Harvard, MA 01451

Phone: +1 978 456 9103
Email: marc@stonecast.net