INTERNET-DRAFT
draft-ietf-cat-kerberos-extra-tgt-02.txt
Updates: RFC 1510
expires January 30, 2000

Jonathan Trostle
Cisco Systems
Michael M. Swift
University of WA

Extension to Kerberos V5 For Additional Initial Encryption

0. Status Of This Memo

1. Abstract

This document defines an extension to the Kerberos protocol specification (RFC 1510) [1] to enable a preauthentication field in the AS_REQ message to carry a ticket granting ticket. The session key from this ticket granting ticket will be used to cryptographically strengthen the initial exchange in either the conventional Kerberos V5 case or in the case the user stores their encrypted private key on the KDC [2].

2. Motivation

In Kerberos V5, the initial exchange with the KDC consists of the AS_REQ and AS_REP messages. For users, the encrypted part of the AS_REP message is encrypted in a key derived from a password. Although a password policy may be in place to prevent dictionary attacks, brute force attacks may still be a concern due to insufficient key length.

This draft specifies an extension to the Kerberos V5 protocol to allow a ticket granting ticket to be included in an AS_REQ message

preauthentication field. The session key from this ticket granting ticket will be used to cryptographically strengthen the initial

exchange in either the conventional Kerberos V5 case or in the case the user stores their encrypted private key on the KDC [2]. The session key from the ticket granting ticket is combined with the user password key (key K2 in the encrypted private key on KDC option) using HMAC to obtain a new triple des key that is used in place of the user key in the initial exchange. The ticket granting ticket could be obtained by the workstation using its host key.

3. The Extension

The following new preauthentication type is proposed:

PA-EXTRA-TGT	22

The preauthentication-data field contains a ticket granting ticket encoded as an ASN.1 octet string. The server realm of the ticket granting ticket must be equal to the realm in the KDC-REQ-BODY of the AS_REQ message. In the absence of a trust relationship, the local Kerberos client should send the AS_REQ message without this extension.

In the conventional (non-pkinit) case, we require the RFC 1510 PA-ENC-TIMESTAMP preauthentication field in the AS_REQ message. If neither it or the PA-PK-KEY-REQ preauthentication field is included in the AS_REQ message, the KDC will reply with a KDC_ERR_PREAUTH_FAILED error message.

We propose the following new etypes:

des3-cbc-md5-xor	16
des3-cbc-sha1-xor	17

The encryption key is obtained by:

(1) Obtaining an output M from the HMAC-SHA1 function [3] using the user password key (the key K2 in the encrypted private key on KDC option of pkinit) as the text and the triple des session key as the K input in HMAC:

    M = H(K XOR opad, H(K XOR ipad, text)) where H = SHA1.

    The session key from the accompanying ticket granting ticket must be a triple des key when one of the triple des xor encryption types is used.

(2) Concatenate the output M (20 bytes) with the first 8 non-parity bits of the triple-des ticket granting ticket session key to get 168 bits that will be used for the new triple-des encryption key.

(3) Set the parity bits of the resulting key.

The resulting triple des key is used to encrypt the timestamp for the PA-ENC-TIMESTAMP preauthentication value (or in the encrypted private key on KDC option of pkinit, it is used in place of the key K2 to both sign in the PA-PK-KEY-REQ and for encryption in the PA-PK-KEY-REP preauthentication types).

If the KDC decrypts the encrypted timestamp and it is not within the appropriate clock skew period, the KDC will reply with the KDC_ERR_PREAUTH_FAILED error. The same error will also be sent if the above ticket granting ticket fails to decrypt properly, or if it is not a valid ticket.

The KDC will create the shared triple des key from the ticket granting ticket session key and the user password key (the key K2 in the encrypted private key on KDC case) using HMAC as specified above and use it to validate the AS_REQ message and then to encrypt the encrypted part of the AS_REP message (use it in place of the key K2 for encryption in the PA-PK-KEY-REP preauthentication field).

Local workstation policy will determine the exact behaviour of the Kerberos client with respect to the extension protocol. For example, the client should consult policy to decide when to use use the extension. This policy could be dependent on the user identity, or whether the workstation is in the same realm as the user. One possibility is for the workstation logon to fail if the extension is not used. Another possibility is for the KDC to set a flag in tickets issued when this extension is used.

A similar idea was proposed in OSF DCE RFC 26.0 [4]; there a preauthentication field containing a ticket granting ticket, a randomly generated subkey encrypted in the session key from the ticket, and a timestamp structure encrypted in the user password and then the randomly generated subkey was proposed. Some advantages of the current proposal are that the KDC has two fewer decryptions to perform per request and the client does not have to generate a random key.

4. Bibliography

[1] J. Kohl, C. Neuman. The Kerberos Network Authentication Service (V5). Request for Comments 1510.

[2] B. Tung, C. Neuman, J. Wray, A. Medvinsky, M. Hur, J. Trostle. Public Key Cryptography for Initial Authentication in Kerberos. ftp://ds.internic.net/internet-drafts/draft-ietf-cat-kerberos-pkinit-08.txt

[3] H. Krawczyk, M. Bellare, R. Canetti. HMAC: Keyed-Hashing for Message Authentication. Request for Comments 2104.

[4] J. Pato. Using Pre-authentication to Avoid Password Guessing Attacks. OSF DCE SIG Request for Comments 26.0.

5. Acknowledgement: We thank Ken Hornstein for some helpful comments.

6. Expires January 30, 2000.

7. Authors' Addresses

Jonathan Trostle
170 W. Tasman Dr.
San Jose, CA 95134, U.S.A.

Email: jtrostle@cisco.com
Phone: (408) 527-6201

Michael Swift
Email: mikesw@cs.washington.edu