Network Working Group
<draft-ietf-cat-kerb-des3-hmac-sha1-00.txt>
Internet-Draft

M. Horowitz
Cygnus Solutions

November, 1996

Triple DES with HMAC-SHA1 Kerberos Encryption Type

Status of this Memo

Abstract

This document defines a new encryption type and a new checksum type for use with Kerberos V5 [RFC1510]. This encryption type is based on the Triple DES cryptosystem and the HMAC-SHA1 [Krawczyk96] message authentication algorithm.

The des3-cbc-hmac-sha1 encryption type has been assigned the value 7. The hmac-sha1-des3 checksum type has been assigned the value 12.

Encryption Type des3-cbc-hmac-sha1

EncryptedData using this type must be generated as described in [Horowitz96]. The encryption algorithm is Triple DES in Outer-CBC mode. The keyed hash algorithm is HMAC-SHA1. Unless otherwise specified, a zero IV must be used. If the length of the input data is not a multiple of the block size, zero octets must be used to pad the plaintext to the next eight-octet boundary. The counfounder must be eight random octets (one block).

Checksum Type hmac-sha1-des3

Checksums using this type must be generated as described in [Horowitz96]. The keyed hash algorithm is HMAC-SHA1.

Common Requirements

Where the Triple DES key is represented as an EncryptionKey, it shall be represented as three DES keys, with parity bits, concatenated together. The key shall be represented with the most significant bit first.

When keys are generated by the derivation function, a key length of 168 bits shall be used. The output bit string will be converted to a valid Triple DES key by inserting DES parity bits after every seventh bit.

Any implementation which implements either of the encryption or checksum types in this document must support both.

Security Considerations

This entire document defines encryption and checksum types for use with Kerberos V5.

References

[Horowitz96] Horowitz, M., "Key Derivation for Kerberos V5", draft-horowitz-kerb-key-derivation-00.txt, November 1996.

[Krawczyk96] Krawczyk, H., Bellare, and M., Canetti, R., "HMAC: Keyed-Hashing for Message Authentication", draft-ietf-ipsec-hmac-md5-01.txt, August, 1996.

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

Author's Address

Marc Horowitz
Cygnus Solutions
955 Massachusetts Avenue
Cambridge, MA 02139

Phone: +1 617 354 7688
Email: marc@cygnus.com