INTERNET DRAFT
Kerberos Working Group
Document: draft-ietf-krb-wg-sha1-00.txt

K. Raeburn
MIT

October 18, 2004
expires April 18, 2005

Unkeyed SHA-1 Checksum Specification for Kerberos 5

Status of this Memo

Copyright Notice

Abstract

The Kerberos cryptosystem specification requires a profile detailing several operations for a new checksum type for ensuring the integrity of data in Kerberos and related protocol exchanges. This document specifies the use of a simple unkeyed checksum type based on SHA-1.

1. Introduction

The Kerberos cryptosystem specification requires a profile detailing several operations for a new checksum type for ensuring the integrity of data in Kerberos and related protocol exchanges. This document specifies the use of a simple unkeyed checksum type based on SHA-1.

(...to be expanded on a bit, describe PKINIT use...)

2. Checksum Definition

The SHA-1 Kerberos checksum type calculates a checksum using the SHA-1 hash algorithm. This algorithm takes as input a message of arbitrary length, and produces as output a 160-bit (20 octet) hash value.

Any general specification of a Kerberos checksum value to be computed must include the encryption key and a key usage value [KCRYPTO]. Both of these values are ignored for the SHA-1 checksum type, thus this checksum algorithm may be used with any encryption key type.

The parameters for the Kerberos checksum profile for this type are thus:

	sha1
associated cryptosystem	any
get_mic	sha1(msg)
verify_mic	get_mic and compare

The sha1 checksum algorithm is assigned a checksum type number of 14.

3. Security Considerations

Unkeyed checksum types should be used with caution, in limited circumstances where the lack of a key does not provide an avenue for an attacker to compromise the integrity of the data being conveyed. Even when encrypted, the use of unkeyed checksums may allow some forms of attack; this is discussed in the Security Considerations section of [KCRYPTO].

The use of unkeyed checksums for integrity protection should be done with great care.

4. IANA Considerations

The Kerberos checksum type values 10 and 14 have both been reserved for "sha1 (unkeyed)" per [KCRYPTO], the latter with intent to use it with this specification, and the former on the basis of speculation that some implementation might have used that value for the same purpose.

XXX...mention PKINIT above as the intended use?

IANA is directed to assign the Kerberos checksum type value 14 to "sha1" with a reference to this document.

As no supporting information has been found regarding any existing experimental use of or specification for Kerberos checksum type 10, IANA is directed to delete that registry entry, leaving the value available for future assignment.

Normative References

[KCRYPTO]
Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", draft-ietf-krb-wg-crypto-07.txt, February 2004.

[SHA1]
NIST, "Secure Hash Standard", FIPS PUB 180-1, April 1995.

Informative References

[KRB]
Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", draft-ietf-krb-wg-kerberos-clarifications-07.txt, September 2004.

[PKINIT]
Tung, B., Neuman, C., Hur, M., Medvinsky, A., Medvinsky, S., Wray, J., and J. Trostle, "Public Key Cryptography for Initial Authentication in Kerberos", draft-ietf-cat-kerberos-pk-init-20.txt, July 2004.

Author's Address

Kenneth Raeburn
Massachusetts Institute of Technology
77 Massachusetts Avenue
Cambridge, MA 02139
raeburn@mit.edu

Full Copyright Statement

Disclaimer