NETWORK WORKING GROUP
Internet-Draft
Expires: December 30, 2004

N. Williams
Sun

July 2004

A PRF for the Kerberos V GSS-API Mechanism
draft-ietf-kitten-krb5-gssapi-prf-00.txt

Status of this Memo

Copyright Notice

Abstract

This document defines the Pseudo-Random Function (PRF) for the Kerberos V GSS-API mechanism, based on the PRF defined for the Kerberos V cryptographic framework, for keying application protocols given an established Kerberos V GSS-API security context.

Table of Contents

1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Introduction

The GSS-API PRF [GSS-PRF] function for the Kerberos V mechanism shall be the output of a PRF+ function based on the enctype's PRF function keyed with the negotiated session key of the security context (e.g., the acceptor's subkey) and key usage X (TBD).

The PRF+ function is a simple counter-based extension of the enctype's prf using an 16-bit network byte order unsigned binary counter: PRF+(k, input) = random-to-key(k-truncate(prf(k, 0 || input) || prf(k, 1 || input), .. prf(k, n || input))). The maximum output length for this PRF+ then is 65536 times the output length of the Kerberos V cryptographic framework PRF for the enctype of the input key.

If the desired_output_len input parameter exceeds the maximum output of this function then the maximum will be output instead.

3. Security Considerations

Kerberos V enctypes' PRF functions use a key derived from contexts' session keys and should preserve the forward security properties of the mechanisms' key exchanges.

See also [GSS-PRF] for generic security considerations of GSS_Pseudo_random().

4 Normative

[GSS-PRF] Williams, N., "A PRF API extension for the GSS-API".

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000.

[RFC2744] Wray, J., "Generic Security Service API Version 2 : C-bindings", RFC 2744, January 2000.

Author's Address

Nicolas Williams
Sun Microsystems
5300 Riata Trace Ct
Austin, TX 78727
US

EMail: Nicolas.Williams@sun.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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