NETWORK WORKING GROUP N. Williams
Internet-Draft Sun
Expires: December 30, 2004 July 2004

A PRF API extension for the GSS-API
draft-ietf-kitten-gssapi-prf-01.txt

Status of this Memo

Copyright Notice

Abstract

This document defines a Pseudo-Random Function (PRF) extension to the Generic Security Service Applicatoin Programming Interface (GSS-API) for keying application protocols given an established GSS-API security context. The primary intended use of this function is to key secure session layers that don't or cannot use GSS-API per-message MIC (message integrity check) and wrap tokens for session protection.

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

A need has arisen for users of the GSS-API to key applications' cryptographic protocols using established GSS-API security contexts. Such applications can use the GSS-API for authentication, but not for transport security (for whatever reasons), and since the GSS-API does not provide a method for obtaining keying material from established security contexts such applications cannot make effective use of the GSS-API.

To address this need we define a pseudo-random function (PRF) extension to the GSS-API.

3. GSS_Pseudo_random()

Inputs:

- context CONTEXT handle,
- prf_in OCTET STRING,
- desired_output_len INTEGER

Outputs:

- major_status INTEGER,
- minor_status INTEGER,
- prf_out OCTET STRING

Return major_status codes:

- GSS_S_COMPLETE indicates no error.
- GSS_S_NO_CONTEXT indicates that a null context has been provided as input.
- GSS_S_CONTEXT_EXPIRED indicates that an expired context has been provided as input.
- GSS_S_UNAVAILABLE indicates that the mechanism lacks support for this function.
- GSS_S_FAILURE indicates failure or lack of support; the minor status code may provide additional information.

This function applies the established context's mechanism's keyed PRF function to the input data (prf_in), keyed with key material associated with the given security context and outputs the resulting octet string (prf_out) of desired_output_len length.

The output string of this function MUST be a pseudo-random function [GGM1][GGM2] of the input keyed with key material from the established security context -- the chances of getting the same output given different input parameters should be exponentially small.

This function, applied to the same inputs by an initiator and acceptor using the same established context, MUST produce the *same results* for both, the initiator and acceptor, even if called multiple times for the same context.

Mechanisms MAY limit the output of the PRF according, possibly in ways related to the types of cryptographic keys available for the PRF function, thus the prf_out output of GSS_Pseudo_random() MAY be smaller than requested.

3.1 C-Bindings

```
OM_uint32 gss_pseudo_random(
  OM_uint32                  *minor_status,
  gss_ctx_id_t                        context,
  const gss_buffer_t         prf_in,
  ssize_t            desired_output_len,
  gss_buffer_t               prf_out
);
```

4. Security Considerations

Care should be taken in properly designing a mechanism's PRF function.

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

5. References

5.1 Normative References

[GGM1] Goldreich, O., Goldwasser, S. and S. Micali, "How to Construct Random Functions", October 1986.

[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.

5.2 Informative References

[GGM2] Goldreich, O., Goldwasser, S. and S. Micali, "On the Cryptographic Applications of Random Functions", 1985.

[RFC1750] Eastlake, D., Crocker, S. and J. Schiller, "Randomness Recommendations for Security", RFC 1750, December 1994.

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.