KITTEN WG
Internet-Draft
Expires: August 28, 2008

N. Williams
Sun

February 25, 2008

Clarifications and Extensions to the GSS-API for the Use of Channel Bindings

draft-ietf-kitten-gssapi-channel-bindings-03.txt

Status of this Memo

Copyright Notice

Abstract

This document clarifies and generalizes the Generic Security Services Application Programming Interface (GSS-API) "channel bindings" facility, and imposes requirements on future GSS-API mechanisms and programming language bindings of the GSS-API.

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. New Requirements for GSS-API Mechanisms

Given the publication of RFC5056 we now assert that all new GSS-API mechanisms that support channel binding MUST conform to [RFC5056].

3. Generic Structure for GSS-API Channel Bindings

The base GSS-API v2, update 1 specification [RFC2743] provides a facility for channel binding. It models channel bindings as an OCTET STRING and leaves it to the GSS-API v2, update 1 C-Bindings specification to specify the structure of the contents of the channel bindings OCTET STRINGs. The C-Bindings specification [RFC2744]then defines, in terms of C, what should have been a generic structure for channel bindings. The Kerberos V GSS mechanism [RFC1964]then defines a method for encoding GSS channel bindings in a way that is independent of the C-Bindings -- otherwise the mechanism's channel binding facility would not be useable with other language bindings.

In other words, the structure of GSS channel bindings given in [RFC2744] is actually generic, rather than specific to the C programming language.

Here, then, is a generic re-statement of this structure, in pseudo-ASN.1:

```
GSS-CHANNEL-BINDINGS := SEQUENCE {
        initiator-address-type        INTEGER,
        initiator-address         OCTET STRING,
        acceptor-address-type    INTEGER,
        acceptor-address         OCTET STRING,
        application-data         OCTET STRING,
}
```

The values for the address fields are described in [RFC2744].

New language-specific bindings of the GSS-API SHOULD specify a language-specific formulation of this structure.

Where a language binding of the GSS-API models channel bindings as OCTET STRINGs (or the language's equivalent), then the implementation MUST assume that the given bindings correspond only to the application-data field of GSS-CHANNEL-BINDINGS as shown above, rather than some encoding of GSS-CHANNEL-BINDINGS.

GSS-API mechanisms MAY use the [RFC1964] encoding of channel bindings.

4. Security Considerations

For general security considerations relating to channel bindings see [RFC5056].

Language bindings that use OCTET STRING (or equivalent) for channel bindings will not support the use of network addresses as channel bindings. This should not cause any security problems, as the use of network addresses as channel bindings is not generally secure. However, it is important that "end-point channel bindings" not be modelled as network addresses, otherwise such channel bindings may not be useable with all language bindings of the GSS-API.

5. Normative References

[RFC1964] Linn, J., "The Kerberos Version 5 GSS-API Mechanism", RFC 1964, June 1996.

[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.

[RFC5056] Williams, N., "On the Use of Channel Bindings to Secure Channels", RFC 5056, November 2007.

Author's Address

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

Email: Nicolas.Williams@sun.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).