KITTEN WG
Internet-Draft
Intended status: Standards Track
Expires: September 14, 2008

N. Williams
Sun

March 13, 2008

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

draft-ietf-kitten-gssapi-channel-bindings-04.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 14, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

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 3
2. Introduction 4
3. New Requirements for GSS-API Mechanisms 5
4. Generic Structure for GSS-API Channel Bindings 6
5. IANA Considerations 7
6. Security Considerations 8
7. Normative References 9
Author's Address 10
Intellectual Property and Copyright Statements 11

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 base GSS-API v2, update 1 specification [RFC2743] provides a facility for channel binding (see also [RFC5056]), but its treatment was incomplete. The C-bindings of the GSS-API [RFC2744] expanded a little on this facility in what should have been a generic way, but was a C-specific way, and still, the treatment of this facility was incomplete.

This document clarifies the GSS-API's channel binding facility and generalizes the parts of it that are specified in the C-bindings document but which should have been generic from the first.

3. 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].

4. 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.

5. IANA Considerations

There are no IANA considerations in this document.

6. 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.

7. 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

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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