Network Working Group
Request for Comments: 5554
Updates: 2743
Category: Standards Track

N. Williams
Sun

May 2009

Clarifications and Extensions to the Generic Security Service Application Program Interface (GSS-API) for the Use of Channel Bindings

Status of This Memo

Copyright Notice

Abstract

This document clarifies and generalizes the Generic Security Service 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. Introduction

The base GSS-API version 2, update 1 specification [RFC2743] provides a facility for channel binding (see also [RFC5056]), but its treatment is incomplete. The GSS-API C-bindings specification [RFC2744] expands somewhat on this facility in what should be a generic way, but is instead a C-specific way, thus leaving the treatment of this facility 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 that should have been generic from the start.

2. 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].

3. New Requirements for GSS-API Mechanisms

Given the publication of RFC 5056, 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 version 2, 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 version 2, 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 [RFC4121] also 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 in spite of being specified in terms of C concepts and syntax.

We generalize it as shown below, using the same pseudo-ASN.1 as is used in RFC 2743. Although the figure below is, indeed, a valid ASN.1 [CCITT.X680] type, we do not provide a full ASN.1 module as none is needed because no standard encoding of this structure is needed -- the definition below is part of an abstract API, not part

of a protocol defining bits on the wire. GSS-API mechanisms do need to encode the contents of this structure, but that encoding will be mechanism specific (see below).

```
GSS-CHANNEL-BINDINGS ::= SEQUENCE {
        initiator-address-type  INTEGER,      -- See RFC2744
        initiator-address       OCTET STRING, -- See RFC2744
        acceptor-address-type   INTEGER,      -- See RFC2744
        acceptor-address        OCTET STRING, -- See RFC2744
        application-data        OCTET STRING  -- See RFC5056
}
```

Abstract GSS-API Channel Bindings Structure

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.

As mentioned above, [RFC4121] describes an encoding of the above GSS-CHANNEL-BINDINGS structure and then hashes that encoding. Other GSS-API mechanisms are free to use that encoding.

5. 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 modeled as network addresses; otherwise, such channel bindings may not be useable with all language bindings of the GSS-API.

6. References

6.1. Normative References

[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.

[RFC4121] Zhu, L., Jaganathan, K., and S. Hartman, "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API) Mechanism: Version 2", RFC 4121, July 2005.

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

6.2. Informative References

[CCITT.X680] International Telephone and Telegraph Consultative Committee, "Abstract Syntax Notation One (ASN.1): Specification of basic notation", CCITT Recommendation X.680, July 2002.

Author's Address

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

EMail: Nicolas.Williams@sun.com