Network Working Group
Internet-Draft
Updates: 4120 (if approved)
Expires: November 11, 2006

S. Josefsson
SJD

May 10, 2006

Extended Kerberos Version 5 Key Distribution Center (KDC) Exchanges Over TCP

draft-ietf-krb-wg-tcp-expansion-00

Status of this Memo

Copyright Notice

Abstract

This document describes an extensibility mechanism for the Kerberos v5 protocol when used over TCP transports.

Table of Contents

1. Introduction

The Kerberos 5 [3] specification, in section 7.2.2, reserve the high order bit in the initial length field for TCP transport for future expansion. This document update [3] to describe the behaviour when that bit is set. This mechanism is intended for extensions that are specific for the TCP transport.

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 RFC 2119 [1].

3. Extension Mechanism for TCP transport

The reserved high bit of the request length field is used to signal the use of this extension mechanism. When the reserved high bit is set, the remaining 31 bits of the initial 4 octets are interpreted as a bitmap. Each bit in the bitmask can be used to request a particular extension. The 31 bits form the "extension bitmask". It is expected that other documents will describe the details associated with particular bits.

A 4-octet value with only the high bit set, and thus the extension bitmask all zeros, is called a PROBE. A client may send a probe to find out which extensions a KDC support. A client may also set particular bits in the extension bitmask directly, if it does not need to query the KDC for available extensions before deciding which extension to request.

If a KDC receive a PROBE, or if a KDC does not support all extensions corresponding to set bits in the extension bitmask, the KDC MUST return 4 octets with the high bit set, and with the remaining bitmask

indicate which extensions it supports. The KDC SHOULD NOT close the connection, and SHOULD wait for the client to then send a second 4-octet value, with the high bit set and the remaining bits as the bitmask, to request a particular extension. If the second 4-octet value is a PROBE or an unsupported extension, the KDC MUST close the connection. This is used by the client to shutdown a session when the KDC did not support a, by the client, required extension.

Resource avaibility considerations may influence whether, and for how long, the KDC will wait for the client to send requests.

The behaviour when more than one non-high bit is set depends on the

particular extension mechanisms. If a requested extension (bit X) does not specify how it interact with another requested extensions (bit Y), the KDC MUST treat the request as a PROBE or unsupported extension, and proceed as above.

Each extension MUST describe the structure of protocol data beyond the length field, and the behaviour of the client and KDC. If an extension mechanism reserve multiple bits, it MUST describe how they interact.

4. Interoperability Consideration

Implementations with support for TCP that do not claim to conform to RFC 4120 may not handle the high bit correctly. Behaviour may include closing the TCP connection without any response, and logging an error message in the KDC log. When this was written, this problem existed in modern versions of popular implementations. Implementations experiencing trouble getting the expected responses from a server SHOULD assume that it does not support this extension mechanism. Clients MAY remember this semi-permanently, to avoid excessive logging in the server. Care should be taken to avoid unexpected behaviour for the user when the KDC is eventually upgraded. Implementations MAY also provide a way to enable and disable this extension on a per-realm basis. How to handle these backwards compatibility quirks are in general left unspecified.

5. Security Considerations

Because the initial length field is not protected, it is possible for an active attacker (i.e., one that is able to modify traffic between the client and the KDC) to make it appear to the client that the server does not support this extension mechanism. Client and KDC policies can be used to reject connections that does not use any expansion.

6. IANA Considerations

IANA needs to create a new registry for "Kerberos 5 TCP Extensions". The initial contents of this registry should be:

[[RFC Editor: Replace xxxx below with the number of this RFC.]]

Bit #	Meaning	Reference
0..29	AVAILABLE for registration.	

30	RESERVED.	RFC XXXX

IANA will register values 0 to 29 after IESG Approval, as defined in BCP 64 [2]. Assigning value 30 requires a Standards Action that update or obsolete this document.

7. Acknowledgements

Thanks to Andrew Bartlett who pointed out that some implementations (MIT Kerberos and Heimdal) did not follow RFC 4120 properly with regards to the high bit, which resulted in an Interoperability Consideration.

Nicolas Williams and Jeffrey Hutzelman provided comments that improved the document.

8. Normative References

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

[2] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

[3] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

Appendix A. Copying conditions

Author's Address

Simon Josefsson
SJD

Email: simon@josefsson.org

Intellectual Property Statement

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.

Disclaimer of Validity

Copyright Statement

Acknowledgment

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