Network Working Group
Internet-Draft
Intended status: Experimental
Expires: September 1, 2019

R. Van Rein
ARPA2.net

February 28, 2019

Diameter Messages in Kerberos5 AuthorizationData
draft-vanrein-krb5-authzdata-diameter-01

Abstract

The Kerberos5 infrastructure is concerned with authentication, but it can also carry AuthorizationData in a variety of formats. Diameter is an extensible standard for the expression of authorisation information. This specification defines an embedding of Diameter data in the AuthorizationData fields of Kerberos5.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on September 1, 2019.

Table of Contents

1. Introduction

Kerberos5 [RFC4120] is a single-signon system that provides the users of its realms with authentication tickets to individual services. Such tickets tend to be valid for the remaining user session, typically up to a day. Service tickets are provided by a central realm service known as the Key Distribution Center or KDC.

The KDC may not be able to supply tickets for all services. When it knows that a service belongs to another realm, and when it can locate a crossover key to the service's KDC, it will forward the user to a remote realm through a realm-crossing ticket. The user follows such tickets under current Kerberos semantics [RFC6806].

Though designed for authentication and not authorisation, the realm-centric position of a KDC makes it a suitable place to control both aspects of access control. The message formats can indeed carry AuthorizationData, consisting of a numerical tag and data to be interpreted according to that tag. This specification adds a tag value to describe AuthorizationData holding Diameter protocol messages.

AuthorizationData can be included in requests to the KDC, and the KDC can include AuthorizationData in a ticket. When requesting a service ticket from the KDC, a single-signon ticket with possible AuthorizationData is attached to that request by the Kerberos client. All this data is protected in transit; requests to the KDC are encrypted with the TGT secret or a sub-key; tickets carry it to a service using a key shared between the server and KDC. The KDC can prove to a ticket-receiving service that it originated certain parts of AuthorizationData by wrapping it in CAMMAC [RFC7751] structures.

Diameter frames [RFC6733] hold a list of Attribute-Value Pairs (AVP), with optional nesting into group AVPs. The format is easily parsed and applications exist (or can be defined) to capture a class of usage scenarios. Among the existing applications is an extensible network access application that lends itself for authorisation

applications. These Diameter frames are herein proposed as an AuthorizationData format in Kerberos.

The purpose of using Diameter in Kerberos is to employ the existing authentication infrastructure of Kerberos to also pass authorisation settings between hosts. The standardised format of Diameter simplifies access to services in foreign realms; this is useful to the InternetWide.org purpose to Bring Your Own IDentity (BYOID), which requires passing standardised authentication and authorisation information between collaborating but otherwise independent parties.

2. Embedding Diameter in Kerberos5

Diameter messages consist of a header choosing an application, followed by the AVPs that are meaningful within that application. The header guides the interpretation of the AVPs and is therefore a meaningful part in proper understanding of the exchange. This is why inclusion of Diameter as Kerberos AuthorizationData must not be limited to a set of AVPs but instead include a header. Formally, we define

```
AD-DIAMETER ::= -- A concatenation of byte strings:
                --  1. one Diameter Header, as defined
                --     in Section 3 of RFC 6733
                --  2. zero or more AVP Headers, with
                --     applicable AVP Data, as defined
                --     in Section 4 of RFC 6733
                -- The whole adhering to the Command
                -- Code Format Specification defined
                -- in Section 3.2 of RFC 6733 and its
                -- extensions.
```

and shall use it under this specification when the preceding ad-type field has value TBD assigned for this purpose. Note that AD-DIAMETER does not follow an ASN.1 encoding.

Diameter messages are always carried over a protected transport such as SCTP with DTLS or TCP with TLS, where the purpose is to mutually authenticate Diameter Peers in protection of in-transit data against rogue alterations and to conceal sensitive data from similarly undesirable parties. These security requirements are alternatively met by the Kerberos framework when AuthorizationData is used to carry the Diameter frames.

Diameter distinguishes between sessions and connections. Connections represent coherent message carriers such as TCP or SCTP connections, whereas a session specifies a conceptual relationship that may span multiple connections. Each connection may carry multiple sessions.

Requests over one connection may even be responded to over another. For the purposes of Diameter, passing messages via Kerberos can be viewed as an alternative form of connection; the collaboration between KDC and services can be considered a connection, consisting of a multitude of individual packages but together forming a coherent message carrier.

The average Diameter exchange is a request/response interaction between a resource requesting access and an oracle granting or withholding it. This model does not fit well on the Kerberos system, when the KDC is an intermediate. A modified form does hold; the client may request certain kinds of access in a Diameter frame, and the KDC may filter, modify and pass it on. It is also possible for the KDC to use just the client identity to state privileges that are granted to it.

An AuthorizationData field with a Diameter message reaching the service from an known-aware KDC can be treated as a pro-active hint, to prepare an answer that might come up when interpreting a service request. This is possible because the KDC is always aware of the service being targeted by a requested ticket. The hint provided would stand for the entire duration of the service ticket, effectively turning such tickets into client-held caches of their authorisations.

Diameter connections must start interactions with a Capabilities Exchange. This specification answers that with a default setup with the Network Access Application [RFC7155] and possible overrides to take place during administrative setup, such as during the creation of service keys or the establishment of realm crossover. This loosely addresses the requirement for Capabilities Exchange.

This looseness is warranted because the customary need for a Capabilities Exchange is not fully applicable to the use of Diameter messages in AuthorizationData, not even when crossing realms. First, this can be used as a pro-active mechanism and it is generally safe to ignore any misunderstood Diameter messages. Second, tickets tend to be cached for a day, which makes their generation less resource-demanding. Third, the purpose can help avoid traditional Diameter traffic, thus limiting the danger of a lot of spurious network traffic.

Peers that process Kerberos messages should not be considered Diameter processing nodes, as they may be just passing traffic, except for the end points that produce and consume Diameter messages in AuthorizationData. By default, a KDC will pass AuthorizationData that the client supplies as-is, though it reserves the right to make modifications. This means that clients under a KDC unaware of

Diameter-formatted AuthorizationData might send any claims they like to a foreign realm, and that the KDC cannot be considered a Diameter end point unless it adds a proof of origination.

3. Use with Realm Crossover

When crossing over between realms under independent administrative control, matters of trust and security arise. This has implications for the interpretation of the AuthorizationData fields, including the form described herein.

To overcome this problem, the client KDC must use CAMMAC [RFC7751] to protectively wrap the AuthorizationData for AD-DIAMETER. Trusting services should validate the origin to be the intended KDC. This usually means that the KDC of the service realm validates the AD-DIAMETER data as having originated from the client realm.

With the possible exception for manual overrides, it is not safe to rely on any other delivery form of AD-DIAMETER data from another realm.

4. Security Considerations

This specification suggests some leniency in terms of attempting to access Diameter services that may extend beyond available capabilities. To mitigate any risk, unrecognised messages could be silently ignored. In other uses of Diameter, this would instead cause an explicit error message. As long as no actions are taken on unrecognised content, this should not impact security.

Diameter messaging parties must take responsibility for what they send. Kerberos KDCs may pass AuthorizationData without looking, so any such fields with AD-DIAMETER data must be sent under CAMMAC protection to prove the agreement of the originating KDC.

During realm crossing, privileges may be passed in from a KDC of another realm. It is important for any service realm to be mindful of this. Whether this concern is implemented in individual services or generally dealt with in the realm's KDC is a local operational choice of the service realm; the KDC for the service realm always participates in realm crossover, because it needs to supply the service ticket to the client that crosses over.

During realm crossing, the client's KDC releases a crossover ticket to reach a remote realm. The information contained in this ticket's AuthorizationData may be visible to all services in the remote realm, and is therefore a privacy concern. It may be necessary to either

supply only generic or selected information (such as descriptive attributes) or use only one or a few foreign services per realm.

5. IANA Considerations

When IANA takes on the registration of AuthorizationData tags, it will take the following allocation into account:

TODO

6. Normative References

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, DOI 10.17487/RFC4120, July 2005, <https://www.rfc-editor.org/info/rfc4120>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <https://www.rfc-editor.org/info/rfc6733>.

[RFC6806] Hartman, S., Ed., Raeburn, K., and L. Zhu, "Kerberos Principal Name Canonicalization and Cross-Realm Referrals", RFC 6806, DOI 10.17487/RFC6806, November 2012, <https://www.rfc-editor.org/info/rfc6806>.

[RFC7155] Zorn, G., Ed., "Diameter Network Access Server Application", RFC 7155, DOI 10.17487/RFC7155, April 2014, <https://www.rfc-editor.org/info/rfc7155>.

[RFC7751] Sorce, S. and T. Yu, "Kerberos Authorization Data Container Authenticated by Multiple Message Authentication Codes (MACs)", RFC 7751, DOI 10.17487/RFC7751, March 2016, <https://www.rfc-editor.org/info/rfc7751>.

Appendix A. Acknowledgements

Thanks to the Kerberos list at MIT and especially Greg Hudson, for a lot of information about Kerberos and GSSAPI.

This work was conducted as part of the InternetWide.org project, and aims to support authorisation data that crosses over between platforms and realms. Implementation projects under this architecture are named ARPA2 projects.

We thank NLnet foundation and SURFnet for funding (parts of) this work.

Author's Address

Rick van Rein
ARPA2.net
Haarlebrink 5
Enschede, Overijssel 7544 WP
The Netherlands

Email: rick@openfortress.nl