Internet Engineering Task Force
Internet-Draft
Updates: 4120 (if approved)
Intended status: Standards Track
Expires: August 5, 2013

S. Sorce, Ed.
Red Hat
T. Yu, Ed.
T. Hardjono, Ed.
MIT Kerberos Consortium

Feb 2013

Kerberos Authorization Data Container Authenticated by Multiple MACs
draft-ietf-krb-wg-cammac-04

Abstract

Abstract: This document specifies a Kerberos Authorization Data container that supersedes AD-KDC-ISSUED. It allows for multiple Message Authentication Codes (MACs) or signatures to authenticate the contained Authorization Data elements.

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 http://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 August 5, 2013.

Copyright Notice

Table of Contents

1. Introduction 3
2. Requirements Language 3
3. Validation 3
4. Encoding 4
4.1. AD-CAMMAC 5
5. Assigned numbers 6
6. IANA Considerations 6
7. Security Considerations 6
8. Acknowledgements 7
9. References 7
9.1. Normative References 7
9.2. Informative References 8
Appendix A. Additional Stuff 8
Authors' Addresses 8

1. Introduction

This document specifies a new Authorization Data container for Kerberos, called AD-CAMMAC (Container Authenticated by Multiple MACs), that supersedes AD-KDC-ISSUED. The container allows both the receiving application service and the Key Distribution Center (KDC) itself to verify the authenticity of the contained authorization data. The AD-CAMMAC container can also include additional verifiers that "trusted services" can use to verify the contained authorization data.

2. Requirements Language

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 [RFC2119].

3. Validation

Kerberos ticket authorization data are highly sensitive and must be validated to insure that no tampering has occurred. Although authorization data are in the encrypted part of a Kerberos ticket and therefore have their integrity protected by the ticket encryption, clients can request that KDCs insert potentially arbitrary authorization data into tickets on their behalf. The Kerberos protocol specifications allow this client behavior because the originally envisioned usage of authorization data was to serve as restrictions on the client's privileges. Services that need to interpret specific authorization data as granting increased privileges need some way to ensure that the KDC originated those authorization data.

In order to validate any information, the receiving application service needs to be able to cryptographically verify the data. This is done by introducing a new AuthorizationData element called AD-CAMMAC that contains enough information to bind the contents to a principal in a way that a receiving application service can verify autonomously without further contact with the KDC.

The following information is needed:

- The KDC MAC
- The Service MAC

o Optional Trusted Service MAC

The KDC MAC is required to allow the KDC to validate the data without needing to recompute the contents at every Ticket Granting Service (TGS) request.

The Service MAC is required so that the Service can verify that the authorization data has been validated by the KDC.

The Trusted Service MAC is useful to verify the authenticity of the contents on the same host, when the data is received by a less trusted service and passed to a more trusted service on the same host without the need for additional round trips to the KDC.

The ad-type for AD-CAMMAC is (TBD).

4. Encoding

The Kerberos protocol is defined in [RFC4120] using Abstract Syntax Notation One (ASN.1) [X.680][X.690]. As such, this specification also uses the ASN.1 syntax for specifying both the abstract layout of the AD-CAMMAC attributes, as well as its encoding.

4.1. AD-CAMMAC

```
KerberosV5CAMMAC DEFINITIONS EXPLICIT TAGS ::= BEGIN

AD-CAMMAC                   ::= SEQUENCE {
      elements              [0] AuthorizationData,
      kdc-verifier          [1] Verifier-MAC,
      svc-verifier          [2] Verifier-MAC OPTIONAL,
      other-verifiers       [3] SEQUENCE OF Verifier
}

Verifier              ::= CHOICE {
      mac             Verifier-MAC,
      ...
}

Verifier-MAC          ::= SEQUENCE {
      identifier      [0] PrincipalName OPTIONAL,
      kvno            [1] UInt32,
      enctype         [2] Int32,
      mac             [3] Checksum
}

AD-CAMMAC-BINDING     ::= SEQUENCE {
     cname            [0] PrincipalName,
     authtime         [1] KerberosTime,
     endtime          [2] KerberosTime
}

END
```

elements:
   A sequence of authorization data elements issued by the KDC.
   These elements are the authorization data that the verifier fields
   authenticate.

Verifier:
   A CHOICE type that currently contains only one alternative:
   Verifier-MAC. Future extensions might add support for public-key
   signatures.

Verifier-MAC:
   Contains a MAC computed over the encoding of the AuthorizationData
   value in the elements field of the AD-CAMMAC. The identifier,
   kvno, and enctype fields help the recipient locate the key

required for verifying the MAC.

AD-CAMMAC-BINDING:
An AuthorizationData element that binds the CAMMAC contents to the enclosing ticket. This AuthorizationData element has ad-type number TBD, and MUST be absent from the transmitted elements field of the AD-CAMMAC. It MUST be included in the computation of the Verifiers as if it were the first element.

kdc-verifier:
A Verifier-MAC where the key is the TGS key. The checksum type is the mandatory checksum type for the TGS key.

svc-verifier:
A Verifier-MAC where the key is the long-term key of the service for which the ticket is issued. The checksum type is the mandatory checksum type for the long-term key of the service. This field MUST be present if the service principal of the ticket is not the local TGS, including when the ticket is a cross-realm TGT.

other-verifiers:
A sequence of additional verifiers. In each additional Verifier-MAC, the key is the long-term key of the principal name specified in the identifier field. The PrincipalName MUST be present and be a valid principal in the realm. KDCs MAY add one or more 'trusted service' verifiers. Unless otherwise administratively configured, the 'trusted service' SHOULD be found by replacing the service identifier component of the principal name of the svc-verifier with 'host'. The checksum type is the mandatory checksum type for the long-term key (which one?) of the principal. The key usage is TBD.

5. Assigned numbers

TBD

6. IANA Considerations

TBD.

7. Security Considerations

Although authorization data are generally conveyed within the encrypted part of a ticket and are thereby protected by the existing

encryption methods on the ticket, some authorization data requires the additional protection provided by the CAMMAC.

Extracting a CAMMAC from a ticket for use as a credential removes it from the context of the ticket. In the general case, this could turn it into a bearer token, with all of the associated security implications. Also, the CAMMAC does not itself necessarily contain sufficient information to identify the client principal (if the encoding of AD-CAMMAC-BINDING is omitted from the transmitted CAMMAC). Therefore, application protocols that rely on extracted CAMMACs might need to duplicate a substantial portion of the ticket contents and include that duplicated information in the authorization data contained within the CAMMAC.

A KDC that needs to verify the contents of a CAMMAC in a non-TGS service ticket MUST ensure that the CAMMAC in the ticket is the same one that it inserted into the ticket. A malicious service could substitute legitimate CAMMACs from other tickets that it has received (but not fabricate completely new CAMMACs) into a service ticket. A CAMMAC by itself does not contain sufficient information to accomplish this.

8. Acknowledgements

TBD.

9. References

9.1. Normative References

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, February 2005.

[RFC3962] Raeburn, K., "Advanced Encryption Standard (AES) Encryption for Kerberos 5", RFC 3962, February 2005.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[X.680] ISO, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation -- ITU-T Recommendation X.680 (ISO/IEC International Standard 8824-1:2008)", 2008.

[X.690] ISO, "Information technology -- ASN.1 encoding rules:

Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) -- ITU-T Recommendation X.690 (ISO/IEC International Standard 8825-1:2008)", 1997.

9.2. Informative References

[MIT-Athena] Steiner, J., Neuman, B., and J. Schiller, "Kerberos: An Authentication Service for Open Network Systems. In Proceedings of the Winter 1988 Usenix Conference. February.", 1988.

[RFC1510] Kohl, J. and B. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

Appendix A. Additional Stuff

This becomes an Appendix.

Authors' Addresses

Simo Sorce (editor)
Red Hat

Email: ssorce@redhat.com

Tom Yu (editor)
MIT Kerberos Consortium

Email: tlyu@mit.edu

Thomas Hardjono (editor)
MIT Kerberos Consortium

Email: hardjono@mit.edu