Internet Engineering Task Force
Internet-Draft
Updates: 4120 (if approved)
Intended status: Standards Track
Expires: April 24, 2014

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

October 21, 2013

Kerberos Authorization Data Container Authenticated by Multiple MACs
draft-ietf-krb-wg-cammac-06

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 April 24, 2014.

described in the Simplified BSD License.

Table of Contents

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. This new 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. Motivations

The new AD-CAMMAC authorization data container specified in this document is an improvement upon AD-KDC-ISSUED because it provides assurance to the KDC that the service named in the ticket did not tamper with the contained authorization data. By adding MACs verifiable by the KDC and trusted services, AD-CAMMAC enables several new use cases for the Kerberos protocol that AD-KDC-ISSUED does not accommodate.

The existing AD-KDC-ISSUED authorization data container allows a service to verify that the KDC has issued the contained authorization data. However, because the symmetric key for the MAC is known to both the KDC and the service, the KDC cannot generally detect whether the service has forged the contents of an AD-KDC-ISSUED container in an existing ticket. The new kdc-verifier MAC in the AD-CAMMAC container, because it uses a key known only to the KDC, allows the

KDC to verify the integrity of the contents of that container.

For example, the new AD-CAMMAC container can protect authorization data when using the Constrained Delegation (S4U2Proxy [MS-SFU]) protocol extension. This extension allows a service to use a ticket to itself as evidence that it received a user request and consequently ask the KDC to issue a new ticket on behalf of the user to perform operations against another service.

If the KDC had issued a AD-KDC-ISSUED container in the S4U2Proxy evidence ticket instead of AD-CAMMAC, it would have no way to subsequently verify whether the service had tampered with the

contents of that container. The service would know the key for the MAC for the AD-KDC-ISSUED container in the evidence ticket, and could therefore forge its contents.

The kdc-verifier MAC in the AD-CAMMAC container allows a KDC to verify the integrity of the contained authorization data without having to compute all of the authorization data, an operation that might not always be possible when the data contains ephemeral information such as the strength or type of authentication method used to obtain the original ticket.

A lesser-privileged service on a host may receive an authentication from a client, and might then ask a higher-privileged service ("trusted service") on the same host to act on behalf of the client. To demonstrate that the client has authenticated to it, the lesser-privileged service can extract the AD-CAMMAC container from the ticket and submit it to the trusted service. The trusted service can either ask a specialized service (not yet specified) on the KDC to validate the AD-CAMMAC container, or use verify the optional additional verifiers (the other-verifiers field) that are part of the AD-CAMMAC.

4. Encoding

The Kerberos protocol is defined in [RFC4120] using Abstract Syntax Notation One (ASN.1) [X.680][X.690]. For consistency, this specification also uses the ASN.1 syntax for specifying the layout of AD-CAMMAC. The ad-data of the AD-CAMMAC authorization data element

is the ASN.1 DER encoding of the AD-CAMMAC ASN.1 type specified below.

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    ::= OCTET STRING

    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 optional AuthorizationData element that binds the CAMMAC contents to the enclosing ticket. This AuthorizationData element has ad-type number TBD, and if it appears in the AD-CAMMAC, it MUST be the first member of the elements field of the AD-CAMMAC. The contents of the AD-CAMMAC-BINDING element are a local matter for the KDC implementation. A KDC can use this element to checksum portions of the ticket outside of the CAMMAC, to ensure that a service has not tampered with them. This can be useful if the KDC implements a capability resembling the Windows Constrained Delegation (S4U2Proxy) [MS-SFU] extension.

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.

Some protocol extensions such as S4U2Proxy allow the KDC to issue a

new ticket based on an evidence ticket provided by the service. If the evidence ticket contains authorization data that needs to be preserved in the new ticket, then the KDC MUST revalidate it.

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. 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 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, but including an AD-CAMMAC-BINDING element could be sufficient.

8. Open Issues

Consider making other-verifiers "[3] SEQUENCE (SIZE (1..MAX)) OF VERIFIER OPTIONAL" to make the common case encoding smaller.

Enclose in AD-IF-RELEVANT?

9. Acknowledgements

TBD.

10. References

10.1. 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.

10.2. 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.

[MS-SFU] Microsoft, "[MS-SFU]: Kerberos Protocol Extensions: Service for User and Constrained Delegation Protocol", January 2013, <http://msdn.microsoft.com/en-us/library/cc246071.aspx>.

[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