Internet Engineering Task Force   A. Jain
Internet-Draft   Georgia Tech
Updates: 4120 (if approved)   N. Kinder
Intended status: Standards Track   N. McCallum
Expires: November 17, 2016   Red Hat, Inc.
                                                          May 16, 2016

                Authentication Indicator in Kerberos Tickets
                 draft-ietf-kitten-krb-auth-indicator-01

Abstract

   This document proposes an extension in the Kerberos protocol
   [RFC4120]. It defines a new Authorization Data Type AD-
   AUTHENTICATION-INDICATOR. The purpose of introducing this data type
   is to include an indicator of the strength of a client's
   authentication in the service tickets so that the application
   services can use it as an input into policy decisions.

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 November 17, 2016.

Copyright Notice

Table of Contents

1. Introduction

   Kerberos [RFC4120] allows secure interaction among users and services
   over a network. It supports a variety of authentication mechanisms
   using its Pre-Authentication framework [RFC6113]. The Kerberos
   Authentication Service has been architected to support password based
   authentication as well as multi-factor authentication using One Time
   Password devices or Public Key Cryptography. Implementations that
   have Pre-Authentication mechanisms offering significantly different
   strengths of client authentication may choose to keep track of the
   strength of the authentication used as an input into policy
   decisions.

   This document proposes a new Authorization Data Type to be used to
   convey the authentication strength to the application services. The
   KDC can provide the DER encoding of the ASN.1 type defined in this
   document into the ad-data field of the AD-CAMMAC [RFC7751] container.
   This ASN.1 type contains information about the type of authentication
   mechanism used by the Kerberos client to authenticate itself to the
   KDC.

2. Document Conventions

   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. AD Type Specification

The KDC MAY include the following Authorization Data element, wrapped
in AD-CAMMAC, in the initial credentials and copy it from a ticket-
granting ticket into service tickets:

AD-AUTHENTICATION-INDICATOR 97

The corresponding ad-data field contains the DER encoding of the
ASN.1 type which is defined as

AD-AUTHENTICATION-INDICATOR ::= SEQUENCE OF UTF8String

Each UTF8String value is a short string that indicates that a
particular set of requirements was met during the initial
authentication. These strings are intended to be compared against
known values. They are not intended to store structured data. These
strings MAY be site-defined strings that do not contain a colon such
as the name of the Pre-Authentication mechanism used, or
alternatively URIs that reference a Level of Assurance Profile
[RFC6711].

The AD-AUTHENTICATION-INDICATOR MUST be included in the AD-CAMMAC
container so that its contents can be protected. The AD-
AUTHENTICATION-INDICATOR MAY safely be ignored by the applications
and KDCs that do not implement this element.

4. Security Considerations

AD-AUTHENTICATION-INDICATOR is wrapped in AD-CAMMAC which supersedes
AD-KDC-ISSUED container. AD-CAMMAC allows both the application
service and the KDC to verify the authenticity of the contained
Authorization Data.

A malicious service can replace AD-CAMMAC in a service ticket with a
legitimate AD-CAMMAC present in some other ticket that the service

has received. The KDC MUST ensure that the service does not tamper
with the contents of AD-CAMMAC or the ticket by including a kdc-
verifier in the containing CAMMAC. This binding protects AD-
AUTHENTICATION-INDICATOR in case of constrained delegation such as
S4U2Proxy [MS-SFU] extension.

Using multiple strings in AD-AUTHENTICATION-INDICATOR MAY lead to
ambiguity when a service tries to make a decision based on the AD-
AUTHENTICATION-INDICATOR values. This ambiguity can be avoided if
indicator values are always used as a positive indication of certain
requirements being met during the initial authentication.

5. References

5.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/
              RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

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

   [RFC6113] Hartman, S. and L. Zhu, "A Generalized Framework for
              Kerberos Pre-Authentication", RFC 6113, DOI 10.17487/
              RFC6113, April 2011,
              <http://www.rfc-editor.org/info/rfc6113>.

   [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,
              <http://www.rfc-editor.org/info/rfc7751>.

5.2. Informative References

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

   [RFC6711] Johansson, L., "An IANA Registry for Level of Assurance
              (LoA) Profiles", RFC 6711, DOI 10.17487/RFC6711, August
              2012, <http://www.rfc-editor.org/info/rfc6711>.

Appendix A. ASN.1 Module

```
KerberosV5AuthenticationIndicators {
        iso(1) identified-organization(3) dod(6) internet(1)
        security(5) kerberosV5(2) modules(4)
        authentication-indicators(9)
} DEFINITIONS EXPLICIT TAGS ::= BEGIN

AD-AUTHENTICATION-INDICATOR ::= SEQUENCE OF UTF8String

END
```

Appendix B.   Acknowledgements

   Dmitri Pal (Red Hat)
   Simo Sorce (Red Hat)

Authors' Addresses

   Anupam Jain
   Georgia Tech
   225 North Ave NW
   Atlanta, GA 30332
   USA

   EMail: ajain323@gatech.edu

   Nathan Kinder
   Red Hat, Inc.
   444 Castro St.
   Suite 500
   Mountain View, CA 94041

USA

   EMail: nkinder@redhat.com

   Nathaniel McCallum
   Red Hat, Inc.
   100 East Davie Street
   Raleigh, NC 27601
   USA

   EMail: npmccallum@redhat.com