NETWORK WORKING GROUP
Internet-Draft
Updates: 4120 (if approved)
Expires: January 17, 2007

L. Zhu
P. Leach
K. Jaganathan
Microsoft Corporation
July 16, 2006

Anonymity Support for Kerberos
draft-ietf-krb-wg-anon-01

Status of this Memo

Copyright Notice

Abstract

This document defines the use of anonymous Kerberos tickets for the purpose of authenticating the servers and enabling secure communication between a client and a server, without identifying the client to the server.

Table of Contents

1. Introduction

In certain situations or environments, the Kerberos [RFC4120] client may wish to authenticate a server and/or protect communications without revealing its own identity. For example, consider an application which provides read access to a research database, and which permits queries by arbitrary requestors. A client of such a service might wish to authenticate the service, to establish trust in the information received from it, but might not wish to disclose its identity to the service for privacy reasons.

To accomplish this, a Kerberos mechanism is specified in this document by which a client requests an anonymous ticket and use that to authenticate the server and secure subsequent client-server communications. This provides Kerberos with functional equivalence to TLS [RFC2246] in environments where Kerberos is a more attractive authentication mechanism.

Using this mechanism, the client has to reveal its identity in its initial request to its own Key Distribution Center (KDC) [RFC4120], and then it can remain anonymous thereafter to KDCs on the cross-realm authentication path, if any, and to the server with which it communicates.

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 [RFC2119].

3. Definitions

The anonymous Kerberos realm name is a reserved realm name as defined in [KRBNAM] and its value is the literal "RESERVED:ANONYMOUS".

The anonymous Kerberos principal name is a reserved Kerberos principal name as defined in [KRBNAM], its name-type [RFC4120] is KRB_NT_RESRVED [KRBNAM], and its name-string [RFC4120] is a sequence of two KerberosString components: "RESERVED", "ANONYMOUS".

In this specification, only the client name or the client realm can be anonymous; the server name or the server realm can not be anonymous.

The transited field [RFC4120] of a ticket is an anonymous authentication path if the tr-type field of the TransitedEncoding

type [RFC4120] is NO-TRANSITED-INFO and the contents field is an empty OCTET STRING.

```
NO-TRANSITED-INFO    TBA
```

This transited encoding type indicates that there is no information available about the authentication path.

The anonymous ticket flag is defined as bit TBA (with the first bit being bit 0) in the TicketFlags:

```
TicketFlags     ::= KerberosFlags
  -- anonymous(TBA)
  -- TicketFlags and KerberosFlags are defined in [RFC4120]
```

An anonymous ticket is a ticket that has all of the following properties:

- The cname field [RFC4120] contains the anonymous Kerberos principal name.

- The crealm field [RFC4120] contains either the realm name of the client who made the request or the anonymous kerberos realm name, based on the local policy of the KDC.

- The transited field [RFC4120] can contain either the client's "normal" authentication path according to Section 3.3.3.2 of [RFC4120] or the anonymous authentication path.

- It contains no information that can reveal the client's identity. However the ticket can contain the client realm and the realms on the authentication path, and the authorization data may provide additional information of the client. For example, an anonymous principal that is only identifiable within a particular group of users can be implemented by using authorization data.

- The anonymous ticket flag is set.

Notes: The anonymous ticket flag MUST NOT be set by implementations of this specification if the ticket is not an anonymous ticket. The server principal name and the server realm in a cross-realm referral TGT are not dependent on whether the client is the anonymous principal or not.

The request-anonymous KDC option is defined as bit TBA (with the first bit being bit 0) in the KDCOptions:

```
KDCOptions      ::= KerberosFlags
  -- request-anonymous(TBA)
  -- KDCOptions and KerberosFlags are defined in [RFC4120]
```

4. Protocol Description

In order to request an anonymous ticket, the client sets the request-anonymous KDC option in an Authentication Exchange (AS) or Ticket Granting Service (TGS) request [RFC4120]. The client can request an anonymous TGT based on a normal TGT. Note that if the ticket in the PA-TGS-REQ [RFC4120] is anonymous, the request-anonymous KDC option MUST be set in the request.

When propagating authorization data, care MUST be taken by the TGS to ensure that the client confidentiality is not violated: the TGS MUST either fail the request or remove authorization data that may reveal the client's identity. An optional authorization element unknown by the TGS MUST be removed if it can be ignored (such as ones enclosed in the AD-IF-RELEVANT or the AD-KDCIssued containers [RFC4120]). The TGS can strip critical unknown authorization data if such data do not convey any rights based on the requesting client's identity. Here is a table of the known authorization-data elements, flagged with whether they interfere with client anonymity and recommendations for how to process them.

ad-type	References	Can Breach Confidentiality?
AD-IF-RELEVANT	RFC4120	Yes, remove if unknown
AD-KDCIssued	RFC4120	Yes, remove if unknown
AD-AND-OR	RFC4120	Yes, remove if unknown
AD-MANDATORY-FOR-KDC	RFC4120	Yes, fail the request if unknown

If it is inappropriate to remove an authorization element from the TGS request in order to produce an anonymous ticket, the KDC MUST return an error message with the code KDC_ERR_POLICY [RFC4120].

When policy allows, the KDC issues an anonymous ticket. The client realm in the anonymous ticket can be the anonymous realm name based on local policy. The client name and the client realm the EncKDCRepPart of the reply [RFC4120] MUST match with the corresponding client name and the client realm of the anonymous reply ticket. The client then MUST use the client name and the client realm returned in the EncKDCRepPart in subsequent message exchanges when using that anonymous ticket.

If there is a key known by both the client and the KDC for encrypting the KDC reply, the cname field in the request [RFC4120] can be

anonymous. If the client is anonymous and the KDC does not have a key to encrypt the reply, the KDC MUST return an error message with the code KDC_ERR_NULL_KEY [RFC4120]. For AS exchange, if the reply key is selected from the client keys (for example, as described in Section 3.1.3 of [RFC4120]), then the client principal MUST NOT be anonymous. The client can use the client keys to request an anonymous TGT in the AS request. The anonymous client name, for example, can be used in conjunction with PKINIT [RFC4556]. An anonymous PKINIT client can authenticate the KDC based on the KDC certificate. For TGS exchange, the reply key is selected according to Section 3.3.3 of [RFC4120] as normal.

The KDC fills out the transited field of the anonymous ticket in the reply as follows: If the service ticket in a TGS request is an anonymous ticket with a "normal" authentication path, then the authentication path in the reply ticket MUST also contain a "normal" authentication path: the TGS MUST add the name of the previous realm. However, if the service ticket in a TGS request is an anonymous ticket with an anonymous authentication path, then the reply ticket can contain either an anonymous authentication path or a "normal" authentication path, based on the local policy of the KDC. Thus a "normal" authentication path in an anonymous ticket can be a partial path: it may not include all the intermediate realms on the authentication path.

The KDC fills out the authtime field of the anonymous ticket in the reply as follows: If the anonymous ticket is returned in an AS exchange, the authtime field of the ticket contains the request time. If the anonymous ticket is returned in a TGS exchange, the authtime field contains the time of the initial authentication for the principal who has made the request. An anonymous ticket can be renewed, and the authtime field of a renewed ticket is the authtime in the anonymous ticket that the renewed ticket was based on.

If a client requires anonymous communication then the client MUST check to make sure that the ticket in the reply is actually anonymous by checking the presence of the anonymous ticket flag. Because KDCs ignore unknown KDC options, a KDC that does not understand the request-anonymous KDC option will not return an error, but will instead return a normal ticket.

The subsequent client and server communications then proceed as described in [RFC4120]. No transited policy checking is needed for the anonymous authentication path. However, transited policy checks defined in Section 2.7 of [RFC4120] would apply to an anonymous ticket that contains a "normal" authentication path.

A server accepting an anonymous service ticket may assume that

subsequent requests using the same ticket originate from the same client. Requests with different tickets are likely to originate from different clients.

Interoperability and backward-compatibility notes: the KDC is given the task of rejecting a request for an anonymous ticket when the anonymous ticket is not acceptable by the server.

5. GSS-API Implementation Notes

At the GSS-API [RFC2743] level, the use of an anonymous principal by the initiator/client requires a software change of the initiator/client software (to assert the "anonymous" flag when calling GSS_Init_Sec_Context().

GSS-API does not know or define "anonymous credentials", so the (printable) name of the anonymous principal will rarely be used by or relevant for the initator/client. The printable name is relevant for the acceptor/server when performing an authorization decision based on the name that pops up from GSS_Accept_Sec_Context() upon successful security context establishment.

A GSS-API initiator MUST carefully check the resulting context attributes from the initial call to GSS_Init_Sec_Context() when requesting anonymity, because (as in the GSS-API tradition and for backwards compatibility) anonymity is just another optional context attribute. It could be that the mechanism doesn't recognize the attribute at all or that anonymity is not available for some other reasons -- and in that case the initiator must NOT send the initial security context token to the acceptor, because it will likely reveal the initiators identity to the acceptor, something that can rarely be "un-done".

GSS-API defines the name_type GSS_C_NT_ANONYMOUS [RFC2743] to represent the anonymous identity. In addition, Section 2.1.1 of [RFC1964] defines the single string representation of a Kerberos principal name with the name_type GSS_KRB5_NT_PRINCIPAL_NAME. For the anonymous principals, the name component within the exportable name as defined in Section 2.1.3 of [RFC1964] MUST signify the realm name according to Section 2.1.1 of [RFC1964]. In this specification only the client/initiator can be the anonymous identity.

Portable initiators are RECOMMENDED to use default credentials whenever possible, and request anonymity only through the input anon_req_flag [RFC2743] to GSS_Init_Sec_Context().

6. Security Considerations

Since KDCs ignore unknown options [RFC4120], a client requiring anonymous communication needs to make sure that the ticket is actually anonymous. A KDC that that does not understand the anonymous option would not return an anonymous ticket.

By using the mechanism defined in this specification, the client does not reveal its identity to the server but its identity may be revealed to the KDC of the server principal (when the server principal is in a different realm than that of the client), and any KDC on the cross-realm authentication path. The Kerberos client MUST verify the ticket being used is indeed anonymous before communicating with the cross-realm KDC or the server, otherwise the client's identity may be revealed to the server unintentionally.

In cases where specific server principals must not have access to the client's identity (for example, an anonymous poll service), the KDC can define server principal specific policy that insure any normal service ticket can NEVER be issued to any of these server principals.

If the KDC that issued an anonymous ticket were to maintain records of the association of identities to an anonymous ticket, then someone obtaining such records could breach the anonymity. Additionally, the implementation of most (for now all) KDC's respond to requests at the time that they are received. Traffic analasys on the connection to the KDC will allow an attacket to match client identities to anonymous tickets issued. Because there are plaintext parts of the tickets that are exposed on the wire, such matching by a third party observer is relatively straigtforward.

7. Acknowledgements

The authors would like to thank the following individuals for their insightful comments and fruitful discussions: Sam Hartman, Clifford Neuman, Martin Rex, Nicolas Williams, Jeffery Altman, Tom Yu, Chaskiel M Grundman, Love Hoernquist Aestrand, and Jeffery Hutzelman.

8. IANA Considerations

No IANA actions are required for this document.

9. Normative References

[KRBNAM] Zhu, L., "Additonal Kerberos Naming Contraints", draft-ietf-krb-wg-naming, work in progress.

[RFC1964] Linn, J., "The Kerberos Version 5 GSS-API Mechanism", RFC 1964, June 1996.

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

[RFC2246] Dierks, T. and C. Allen, "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000.

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

[RFC4556] Zhu, L. and B. Tung, "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)", RFC 4556, June 2006.

Authors' Addresses

Larry Zhu
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Email: lzhu@microsoft.com

Paul Leach
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Email: paulle@microsoft.com

Karthik Jaganathan
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Email: karthikj@microsoft.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

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