DHC Working Group
INTERNET-DRAFT
Category: Standards Track
<draft-hornstein-dhc-kerbauth-06.txt>
11 October 2001

Ken Hornstein
NRL
Ted Lemon
Internet Engines, Inc.
Bernard Aboba
Microsoft
Jonathan Trostle
Cisco Systems

DHCP Authentication Via Kerberos V

Abstract

This document describes how Kerberos V may be used in order to allow a DHCP client and server to mutually authenticate as well as to protect the integrity of the DHCP exchange. The protocol described in this document is capable of handling both intra-realm and inter-realm authentication.

Table of Contents

1. Introduction

The Dynamic Host Configuration Protocol (DHCP) provides a mechanism for host configuration. In some circumstances, it is useful for the DHCP client and server to be able to mutually authenticate as well as to guarantee the integrity of DHCP packets in transit. This document describes how Kerberos V may be used in order to allow a DHCP client and server to mutually authenticate as well as to protect the integrity of the DHCP exchange. The protocol described in this document is capable of handling both intra-realm and inter-realm authentication.

1.1. Terminology

This document uses the following terms:

DHCP client
: A DHCP client or "client" is an Internet host using DHCP to obtain configuration parameters such as a network address.

DHCP server
: A DHCP server or "server" is an Internet host that returns configuration parameters to DHCP clients.

Home KDC
: The KDC corresponding to the DHCP client's realm.

Local KDC
: The KDC corresponding to the DHCP server's realm.

1.2. Requirements language

In this document, the key words "MAY", "MUST, "MUST NOT", "OPTIONAL", "RECOMMENDED "SHOULD", and "SHOULD NOT", are to be interpreted as described in [1].

2. Protocol overview

In DHCP authentication via Kerberos V, DHCP clients and servers utilize a Kerberos session key in order to compute a message integrity check value included within the DHCP authentication option. The message integrity check serves to authenticate as well as integrity protect the messages, while remaining compatible with the operation of a DHCP relay. Replay protection is also provided by a replay counter within the authentication option, as described in [3].

Each server maintains a list of session keys and identifiers for clients, so that the server can retrieve the session key and identifier used by a client to which the server has provided previous configuration information. Each server MUST save the replay counter from the previous authenticated message. To avoid replay attacks, the server MUST discard

any incoming message whose replay counter is not strictly greater than the replay counter from the previous message.

DHCP authentication, described in [3], must work within the existing DHCP state machine described in [4]. For a client in INIT state, this means that the client must obtain a valid TGT, as well as a session key, within the two round-trips provided by the DHCPDISCOVER/OFFER/REQUEST/ACK sequence.

In INIT state, the DHCP client submits an incomplete AS_REQ to the DHCP server within the DHCPDISCOVER message. The DHCP server then completes the AS_REQ using the IP address to be assigned to the client, and submits this to the client's home KDC in order to obtain a TGT on the client's behalf. Once the home KDC responds with an AS_REP, the DHCP server extracts the client TGT and submits this along with its own TGT to the home KDC, in order to obtain a user-to-user ticket to the DHCP client. The AS_REP as well as the AP_REQ are included by the DHCP server in the DHCPOFFER. The DHCP client can then decrypt the AS_REP to obtain a home realm TGT and TGT session key, using the latter to decrypt the user-to-user ticket to obtain the user-to-user session key. It is the user-to-user session key that is used to authenticate and integrity protect the client's DHCPREQUEST, and DHCPDECLINE messages. Similarly, this same session key is used to compute the integrity attribute in the server's DHCPOFFER, DHCPACK and DHCPNAK messages, as described in [3].

In the INIT-REBOOT, REBINDING, or RENEWING states, the server can submit the home realm TGT in the DHCPREQUEST, along with authenticating and integrity protecting the message using an integrity attribute within the authentication option. The integrity attribute is computed using the existing session key. The DHCP server can then return a renewed user-to-user ticket within the DHCPACK message. The authenticated DHCPREQUEST message from a client in INIT-REBOOT state can only be validated by servers that used the same session key to compute the integrity attribute in their DHCPOFFER messages.

Other servers will discard the DHCPREQUEST messages. Thus, only servers that used the user-to-user session key selected by the client will be able to determine that their offered configuration information was not selected, returning the offered network address to the server's pool of available addresses. The servers that cannot validate the DHCPREQUEST message will eventually return their offered network addresses to their pool of available addresses as described in section 3.1 of the DHCP specification [4].

When sending a DHCPINFORM, there are two possible procedures. If the client knows the DHCP server it will be interacting with, then it can obtain a ticket to the DHCP server from the local realm KDC. This will require obtaining a TGT to its home realm, as well as possibly a cross-

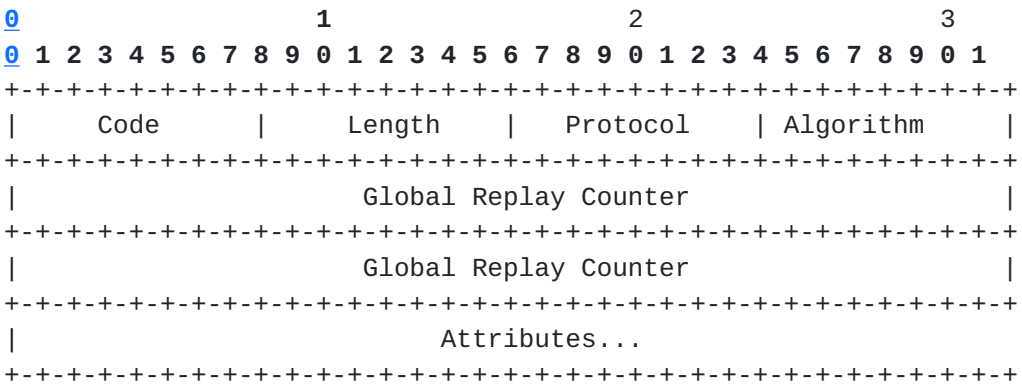
realm TGT to the local realm if the local and home realms differ. Once the DHCP client has a local realm TGT, it can then request a DHCP server ticket in a TGS_REQ. The DHCP client can then include AP_REQ and integrity attributes within the DHCPINFORM. The integrity attribute is computed as described in [3], using the session key obtained from the TGS_REP. The DHCP server replies with a DHCPACK/DHCPNAK, authenticated using the same session key.

If the DHCP client does not know the DHCP server it is interacting with then it will not be able to obtain a ticket to it and a different procedure is needed. In this case, the client will include in the DHCPINFORM an authentication option with a ticket attribute containing its home realm TGT. The DHCP server will then use this TGT in order to request a user-to-user ticket from the home KDC in a TGS_REQ. The DHCP server will return the user-to-user ticket and will authenticate and integrity protect the DHCPACK/DHCPNAK message. This is accomplished by including AP_REQ and integrity attributes within the authentication option included with the DHCPACK/DHCPNAK messages.

In order to support the DHCP client's ability to authenticate the DHCP server in the case where the server name is unknown, the Kerberos principal name for the DHCP server must be of type KRB_NT_SRV_HST with the service name component equal to 'dhcp'. For example, the DHCP server principal name for the host srv.foo.org would be of the form dhcp/srv.foo.org. The client MUST validate that the DHCP server principal name has the above format. This convention requires that the administrator ensure that non-DHCP server principals do not have names that match the above format.

2.1. Authentication Option Format

A summary of the authentication option format for DHCP authentication via Kerberos V is shown below. The fields are transmitted from left to right.



Code

TBD - DHCP Authentication

Length

The length field is a single octet and indicates the length of the Protocol, Algorithm, and Authentication Information fields. Octets outside the range of the length field should be ignored on reception.

Protocol

TBD - DHCP Kerberos V authentication

Algorithm

The algorithm field is a single octet and defines the specific algorithm to be used for computation of the authentication option. Values for the field are as follows:

0 - reserved
1 - HMAC-MD5
2 - HMAC-SHA
3 - 255 reserved

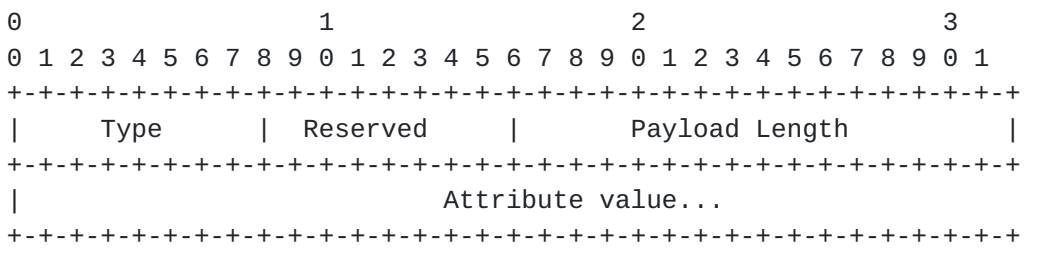
Global Replay Counter

As described in [3], the global replay counter field is 8 octets in length. It MUST be set to the value of a monotonically increasing counter. Using a counter value such as the current time of day (e.g.,

an NTP-format timestamp [10]) can reduce the danger of replay attacks.

Attributes

The attributes field consists of type-length-value attributes of the following format:



Type

The type field is a single octet and is defined as follows:

0 - Integrity check
1 - TICKET
2 - Authenticator
3 - EncTicketPart
10 - AS_REQ
11 - AS_REP
12 - TGS_REQ
13 - TGS_REP
14 - AP_REQ
15 - AP_REP
20 - KRB_SAFE
21 - KRB_PRIV
22 - KRB_CRED
25 - EncASRepPart
26 - EncTGSRepPart
27 - EncAPRepPart
28 - EncKrbPrvPart
29 - EncKrbCredPart
30 - KRB_ERROR

Note that the values of the Type field are the same as in the Kerberos MSG-TYPE field. As a result, no new number spaces are created for IANA administration.

The following attribute types are allowed within the following messages:

DISCOVER	OFFER	REQUEST	DECLINE	#	Attribute
0	1	1	1	0	Integrity check
0	0	0-1	0	1	Ticket
1	0	0	0	10	AS_REQ
0	1	0	0	11	AS_REP
0	1	0	0	14	AP_REQ
0	0-1	0	0	30	KRB_ERROR

RELEASE	ACK	NAK	INFORM w/known server	INFORM w/unknown server	#	Attribute
1	1	1	1	0	0	Integrity check
0	0	0	0	1	1	Ticket
0	0	0	0	0	10	AS_REQ
0	0	0	0	0	11	AS_REP
0	0-1	0	1	0	14	AP_REQ
0	0	0-1	0	0	30	KRB_ERROR

2.2. Client behavior

The following section, which incorporates material from [3], describes client behavior in detail.

2.2.1. INIT state

When in INIT state, the client behaves as follows:

[1] As described in [3], the client MUST include the authentication request option in its DHCPDISCOVER message along with option 61 [6] to identify itself uniquely to the server. An AS_REQ attribute MUST be included within the authentication request option. This (incomplete) AS_REQ will set the FORWARDABLE and RENEWABLE flags and MAY include pre-authentication data (PADATA) if the client knows what PADATA its home KDC will require. The ADDRESSES field in the AS_REQ will be omitted since the client does not yet know its IP address. The ETYPE field will be set to an encryption type that the client can accept.

[2] The client MUST validate DHCPOFFER messages that include an authentication option. Messages including an authentication option with a KRB_ERROR attribute and no integrity attribute are treated as though they are unauthenticated. More typically, authentication

options within the DHCPOFFER message will include AS_REP, AP_REQ, and integrity attributes. To validate the authentication option, the client decrypts the enc-part of the AS_REP in order to obtain the TGT session key. This is used to decrypt the enc-part of the AP_REQ in order to obtain the user-to-user session key. The user-to-user session key is then used to compute the message integrity check as described in [3], and the computed value is compared to the value within the integrity attribute. The client MUST discard any messages which fail to pass validation and MAY log the validation failure.

As described in [3], the client selects one DHCPOFFER message as its selected configuration. If none of the DHCPOFFER messages received by the client include an authentication option, the client MAY choose an unauthenticated message as its selected configuration. DHCPOFFER messages including an authentication option with a KRB_ERROR attribute and no integrity attribute are treated as though they are unauthenticated. The client SHOULD be configurable to accept or reject unauthenticated DHCPOFFER messages.

[3] The client replies with a DHCPREQUEST message that MUST include an authentication option. The authentication option MUST include an integrity attribute, computed as described in [3], using the user to user session key recovered in step 2.

[4] As noted in [3], the client MUST validate a DHCPACK message from the server that includes an authentication option. DHCPACK or DHCPNAK messages including an authentication option with a KRB_ERROR attribute and no integrity attribute are treated as though they are unauthenticated. The client MUST silently discard the DHCPACK if the message fails to pass validation and MAY log the validation failure. If the DHCPACK fails to pass validation, the client MUST revert to the INIT state and return to step 1. The client MAY choose to remember which server replied with an invalid DHCPACK message and discard subsequent messages from that server.

2.2.2. INIT-REBOOT state

When in INIT-REBOOT state, if the user-to-user ticket is still valid, the client MUST re-use the session key from the DHCP server user-to-user ticket in its DHCPREQUEST message. This is used to generate the integrity attribute contained within the authentication option, as described in [3]. In the DHCPREQUEST, the DHCP client also includes its home realm TGT in a ticket attribute in the authentication option in order to assist the DHCP server in renewing the user-to-user ticket. To ensure that the user-to-user ticket remains valid throughout the DHCP lease period so that the renewal process can proceed, the Kerberos

ticket lifetime SHOULD be set to exceed the DHCP lease time. If the user-to-user ticket is expired, then the client MUST return to the INIT state.

The client MAY choose to accept unauthenticated DHCPACK/DHCPNAK messages if no authenticated messages were received. DHCPACK/DHCPNAK messages with an authentication option containing a KRB_ERROR attribute and no integrity attribute are treated as though they are unauthenticated. The client MUST treat the receipt (or lack thereof) of any DHCPACK/DHCPNAK messages as specified in section 3.2 of the DHCP specification [4].

2.2.3. RENEWING state

When in RENEWING state, the DHCP client can be assumed to have a valid IP address, as well as a TGT to the home realm, a user-to-user ticket provided by the DHCP server, and a session key with the DHCP server, all obtained during the original DHCP conversation. If the user-to-user ticket is still valid, the client MUST re-use the session key from the user-to-user ticket in its DHCPREQUEST message to generate the integrity attribute contained within the authentication option.

Since the DHCP client can renew the TGT to the home realm, it is possible for it to continue to hold a valid home realm TGT. However, since the DHCP client did not obtain the user-to-user ticket on its own, it will need to rely on the DHCP server to renew this ticket. In the DHCPREQUEST, the DHCP client includes its home realm TGT in a ticket attribute in the authentication option in order to assist the DHCP server in renewing the user-to-user ticket.

If the DHCP server user-to-user ticket is expired, then the client MUST return to INIT state. To ensure that the user-to-user ticket remains valid throughout the DHCP lease period so that the renewal process can proceed, the Kerberos ticket lifetime SHOULD be set to exceed the DHCP lease time. If client receives no DHCPACK messages or none of the DHCPACK messages pass validation, the client behaves as if it had not received a DHCPACK message in section 4.4.5 of the DHCP specification [4].

2.2.4. REBINDING state

When in REBINDING state, the DHCP client can be assumed to have a valid IP address, as well as a TGT to the home realm, a user-to-user ticket and a session key with the DHCP server, all obtained during the original DHCP conversation. If the user-to-user ticket is still valid, the client MUST re-use the session key from the user-to-user ticket in its DHCPREQUEST message to generate the integrity attribute contained within the authentication option, as described in [3].

Since the DHCP client can renew the TGT to the home realm, it is possible for it to continue to hold a valid home realm TGT. However, since the DHCP client did not obtain the user-to-user ticket on its own, it will need to rely on the DHCP server to renew this ticket. In the DHCPREQUEST, the DHCP client includes its home realm TGT in a ticket attribute in the authentication option in order to assist the DHCP server in renewing the user-to-user ticket.

If the user-to-user ticket is expired, then the client MUST return to INIT state. To ensure that the user-to-user ticket remains valid throughout the DHCP lease period so that the renewal process can proceed, the Kerberos ticket lifetime SHOULD be set to exceed the DHCP lease time. If client receives no DHCPACK messages or none of the DHCPACK messages pass validation, the client behaves as if it had not received a DHCPACK message in section 4.4.5 of the DHCP specification [4].

2.2.5. DHCPRELEASE message

Clients sending a DHCPRELEASE MUST include an authentication option. The authentication option MUST include an integrity attribute, computed as described in [3], using the user to user session key.

2.2.6. DHCPDECLINE message

Clients sending a DHCPDECLINE MUST include an authentication option. The authentication option MUST include an integrity attribute, computed as described in [3], using the user to user session key.

2.2.7. DHCPINFORM message

Since the client already has some configuration information, it can be assumed that it has the ability to obtain a home or local realm TGT prior to sending the DHCPINFORM.

If the DHCP client knows which DHCP server it will be interacting with, then it SHOULD include an authentication option containing AP_REQ and integrity attributes within the DHCPINFORM. The DHCP client first requests a TGT to the local realm via an AS_REQ and then using the TGT returned in the AS_REP to request a ticket to the DHCP server from the local KDC in a TGS_REQ. The session key obtained from the TGS_REP will be used to generate the integrity attribute as described in [3].

If the DHCP client does not know what DHCP server it will be talking to, then it cannot obtain a ticket to the DHCP server. In this case, the DHCP client MAY send an unauthenticated DHCPINFORM or it MAY include an authentication option including a ticket attribute only. The ticket attribute includes a TGT for the home realm. The client MUST validate

that the DHCP server name in the received Kerberos AP_REQ message is of the form dhcp/.... as described in section 4.

The client MAY choose to accept unauthenticated DHCPACK/DHCPNAK messages if no authenticated messages were received. DHCPACK/DHCPNAK messages with an authentication option containing a KRB_ERROR attribute and no integrity attribute are treated as though they are unauthenticated. The client MUST treat the receipt (or lack thereof) of any DHCPACK/DHCPNAK messages as specified in section 3.2 of the DHCP specification [4].

2.3. Server behavior

This section, which relies on material from [3], describes the behavior of a server in response to client messages.

2.3.1. After receiving a DHCPDISCOVER message

For installations where IP addresses are required within tickets, the DHCP server MAY complete the AS_REQ by filling in the ADDRESSES field based on the IP address that it will include in the DHCPOFFER. The DHCP server sends the AS_REQ to the home KDC with the FORWARDABLE flag set. The home KDC then replies to the DHCP server with an AS_REP. The DHCP server extracts the client TGT from the AS_REP and forms a TGS_REQ, which it sends to the home KDC.

If the DHCP server and client are in different realms, then the DHCP server will need to obtain a TGT to the home realm from the KDC of its own (local) realm prior to sending the TGS_REQ. The TGS_REQ includes the DHCP server's TGT within the home realm, has the ENC-TKT-IN-SKEY flag set and includes the client home realm TGT in the ADDITIONAL-TICKETS field, thus requesting a user-to ticket to the DHCP client. The home KDC then returns a user-to-user ticket in a TGS_REP. The user-to-user ticket is encrypted in the client's home realm TGT session key.

In order to recover the user-to-user session key, the DHCP server decrypts the enc-part of the TGS_REP. To accomplish this, the DHCP server uses the session key that it shares with the home realm, obtained in the AS_REQ/AS_REP conversation that it used to obtain its own TGT to the home realm.

The DHCP server then sends a DHCPOFFER to the client, including AS_REP, AP_REQ and integrity attributes within the authentication option. The AS_REP attribute encapsulates the AS_REP sent to the DHCP server by the home KDC. The AP_REQ attribute includes an AP_REQ constructed by the DHCP server based on the TGS_REP sent to it by the home KDC. The server also includes an integrity attribute generated as specified in [3] from the user-to-user session key. The server MUST record the user-to-user session key selected for the client and use that session key for

validating subsequent messages with the client.

2.3.2. After receiving a DHCPREQUEST message

The DHCP server uses the user-to-user session key in order to validate the integrity attribute contained within the authentication option, using the method specified in [3]. If the message fails to pass validation, it MUST discard the message and MAY choose to log the validation failure.

If the message passes the validation procedure, the server responds as described in [4], including an integrity attribute computed as specified in [3] within the DHCPACK or DHCPNAK message.

If the authentication option included within the DHCPREQUEST message contains a ticket attribute then the DHCP server will use the home realm TGT included in the ticket attribute in order to renew the user-to-user ticket, which it returns in an AP_REQ attribute within the DHCPACK. DHCPACK or DHCPNAK messages then include an integrity attribute generated as specified in [3], using the new user-to-user session key included within the AP_REQ.

2.3.3. After receiving a DHCPINFORM message

The server MAY choose to accept unauthenticated DHCPINFORM messages, or only accept authenticated DHCPINFORM messages based on a site policy.

When a client includes an authentication option in a DHCPINFORM message, the server MUST respond with an authenticated DHCPACK or DHCPNAK message. If the DHCPINFORM message includes an authentication option including AP_REQ and integrity attributes, the DHCP server decrypts the AP_REQ attribute and then recovers the session key. The DHCP server than validates the integrity attribute included in the authentication option using the session key. If the integrity attribute is invalid then the DHCP server MUST silently discard the DHCPINFORM message.

If the authentication option only includes a ticket attribute and no integrity or AP_REQ attributes, then the DHCP server should assume that the client needs the server to obtain a user-to-user ticket from the home realm KDC. In this case, the DHCP server includes the client home realm TGT and its own home realm TGT in a TGS_REQ to the home realm KDC. It then receives a user-to-user ticket from the home realm KDC in a TGS_REP. The DHCP server will then include AP_REQ and integrity attributes within the DHCPACK/DHCPNAK.

If the client does not include an authentication option in the DHCPINFORM, the server can either respond with an unauthenticated DHCPACK message, or a DHCPNAK if the server does not accept

unauthenticated clients.

2.3.4. After receiving a DHCPRELEASE message

The DHCP server uses the session key in order to validate the integrity attribute contained within the authentication option, using the method specified in [3]. If the message fails to pass validation, it MUST discard the message and MAY choose to log the validation failure.

If the message passes the validation procedure, the server responds as described in [4], marking the client's network address as not allocated.

2.3.5. After receiving a DHCPDECLINE message

The DHCP server uses the session key in order to validate the integrity attribute contained within the authentication option, using the method specified in [3]. If the message fails to pass validation, it MUST discard the message and MAY choose to log the validation failure.

If the message passes the validation procedure, the server proceeds as described in [4].

2.4. Error handling

When an error condition occurs during a Kerberos exchange, Kerberos error messages can be returned by either side. These Kerberos error messages MAY be logged by the receiving and sending parties.

In some cases, it may be possible for these error messages to be included within the authentication option via the KRB_ERROR attribute. However, in most cases, errors will result in messages being silently discarded and so no response will be returned.

For example, if the home KDC returns a KRB_ERROR in response to the AS_REQ submitted by the DHCP server on the client's behalf, then the DHCP server will conclude that the DHCPDISCOVER was not authentic, and will silently discard it.

However, if the AS_REQ included PADATA and the home KDC responds with an AS_REP, then the DHCP server can conclude that the client is authentic. If the subsequent TGS_REQ is unsuccessful, with a KRB_ERROR returned by the home KDC in the TGS_REP, then the fault may lie with the DHCP server rather than with the client. In this case, the DHCP server MAY choose to return a KRB_ERROR within the authentication option included in the DHCPOFFER. The client will then treat this as an unauthenticated DHCPOFFER.

Similarly, if the integrity attribute contained in the DHCPOFFER proves invalid, the client will silently discard the DHCPOFFER and instead accept an offer from another server if one is available. If the integrity attribute included in the DHCPACK/DHCPNAK proves invalid, then the client behaves as if it did not receive a DHCPACK/DHCPNAK.

When in INIT-REBOOT, REBINDING or RENEWING state, the client will include a ticket attribute and integrity attribute within the authentication option of the DHCPREQUEST, in order to assist the DHCP server in renewing the user-to-user ticket. If the integrity attribute is invalid, then the DHCP server MUST silently discard the DHCPREQUEST.

However, if the integrity attribute is successfully validated by the DHCP server, but the home realm TGT included in the ticket attribute is invalid (e.g. expired), then the DHCP server will receive a KRB_ERROR in response to its TGS_REQ to the home KDC. In this case, the DHCP server MAY respond with a DHCPNAK including a KRB_ERROR attribute and no integrity attribute within the authentication option. This will force the client back to the INIT state, where it can receive a valid home realm TGT.

Where the client included PADATA in the AS_REQ attribute of the authentication option within the DHCPDISCOVER and the AS_REQ was successfully validated by the KDC, the DHCP server will conclude that the DHCP client is authentic. In this case if the client successfully validates the integrity attribute in the DHCPOFFER, but the server does not validate the integrity attribute in the client's DHCPREQUEST, the server MAY choose to respond with an authenticated DHCPNAK containing a KRB_ERROR attribute.

2.5. PKINIT issues

When public key authentication is supported with Kerberos as described in [8], the client certificate and a signature accompany the initial request in the pre-authentication fields. As a result, it is conceivable that the incomplete AS_REQ included in the DHCPDISCOVER packet may exceed the size of a single DHCP option, or even the MTU size. As noted in [4], a single option may be as large as 255 octets. If the value to be passed is larger than this the client concatenates together the values of multiple instances of the same option.

2.6. Examples

2.6.1. INIT state

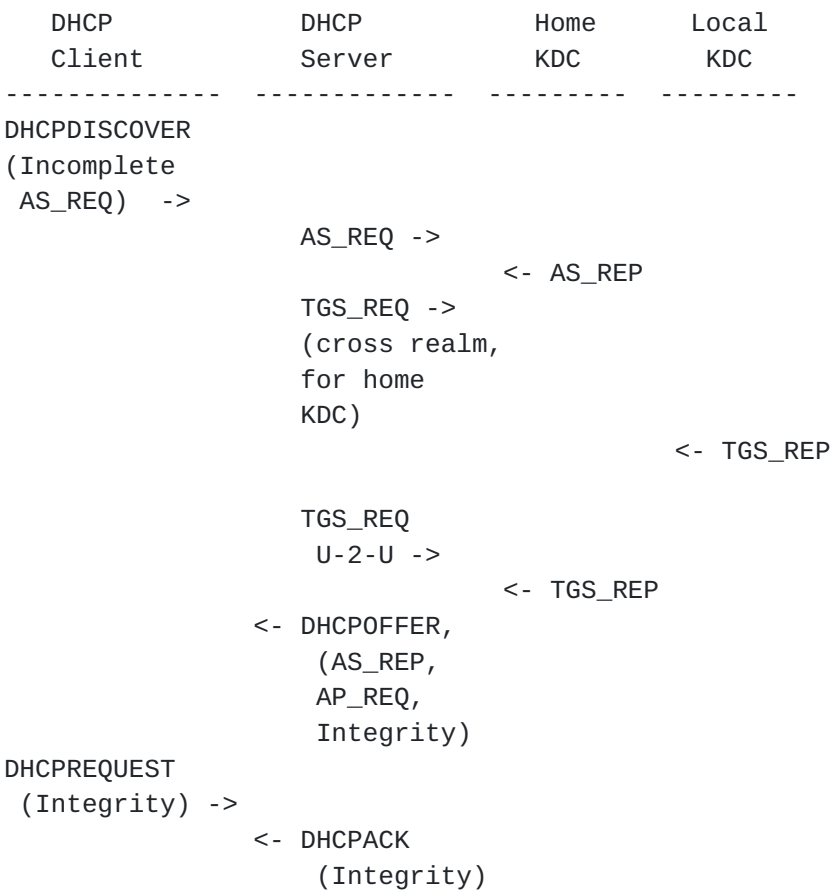
In the intra-realm case where the DHCP Kerberos mutual authentication is successful, the conversation will appear as follows:

```
   DHCP               DHCP
   Client             Server            KDC
--------------     -------------     ---------
DHCPDISCOVER
 (Incomplete
 AS_REQ)  ->
                  AS_REQ ->
                                     <- AS_REP
                  TGS_REQ
                   U-2-U ->
                                     <- TGS_REP
               <- DHCPOFFER,
                   (AS_REP,
                   AP_REQ,
                   Integrity)
DHCPREQUEST
 (Integrity) ->
               <- DHCPACK
                   (Integrity)
```

In the case where the KDC returns a KRB_ERROR in response to the AS_REQ, the server will silently discard the DHCPDISCOVER and the conversation will appear as follows:

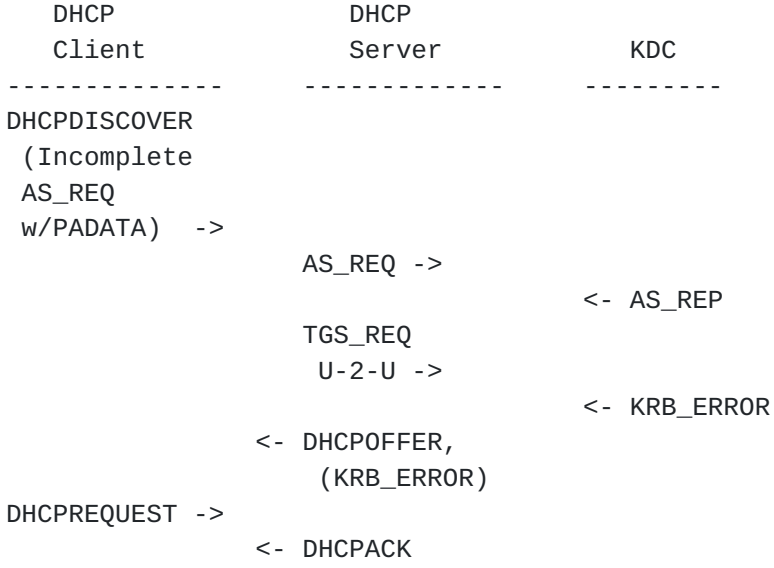
```
   DHCP               DHCP
   Client             Server            KDC
--------------     -------------     ---------
DHCPDISCOVER
 (Incomplete
 AS_REQ)  ->
                  AS_REQ ->
                                     <- KRB_ERROR
```

In the inter-realm case where the DHCP Kerberos mutual authentication is successful, the conversation will appear as follows:

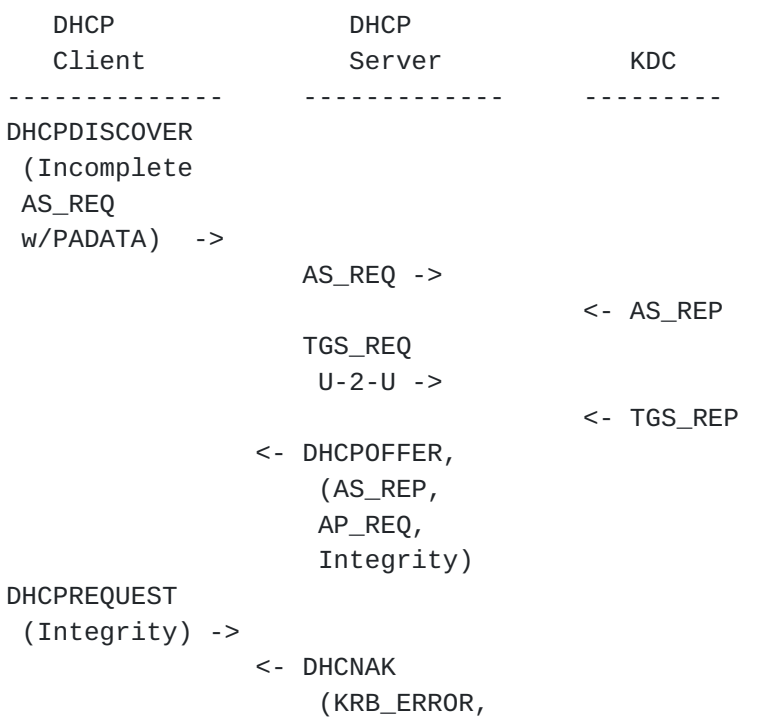


In the case where the client includes PADATA in the AS_REQ attribute within the authentication option of the DHCPDISCOVER and the KDC returns an error-free AS_REP indicating successful validation of the PADATA, the DHCP server will conclude that the DHCP client is authentic. If the KDC then returns a KRB_ERROR in response to the TGS_REQ, indicating a fault that lies with the DHCP server, the server MAY choose not to silently discard the DHCPDISCOVER. Instead it MAY respond with a DHCPOFFER including a KRB_ERROR attribute within the authentication option. The client will then treat this as an unauthenticated DHCPOFFER.

The conversation will appear as follows:



In the intra-realm case where the client included PADATA in the AS_REQ attribute of the authentication option and the AS_REQ was successfully validated by the KDC, the DHCP server will conclude that the DHCP client is authentic. In this case if the client successfully validates the integrity attribute in the DHCPOFFER, but the server does not validate the integrity attribute in the client's DHCPREQUEST, the server MAY choose to respond with an authenticated DHCPNAK containing a KRB_ERROR attribute. The conversation will appear as follows:



```
                    Integrity)
DHCPDISCOVER
 (Incomplete
 AS_REQ)  ->
```

In the intra-realm case where the DHCP client cannot validate the integrity attribute in the DHCPOFFER, the client silently discards the DHCPOFFER. The conversation will appear as follows:

```
   DHCP               DHCP
   Client             Server            KDC
--------------     -------------     ---------
DHCPDISCOVER
 (Incomplete
 AS_REQ)  ->
                  AS_REQ ->
                                    <- AS_REP
                  TGS_REQ
                   U-2-U ->
                                    <- TGS_REP
               <- DHCPOFFER,
                  (AS_REP,
                  AP_REQ,
                  Integrity)
DHCPREQUEST
 [To another server]
 (Integrity) ->
```

In the intra-realm case where the DHCP client cannot validate the integrity attribute in the DHCPACK, the client reverts to INIT state. The conversation will appear as follows:

```
   DHCP               DHCP
   Client             Server            KDC
--------------     -------------     ---------
DHCPDISCOVER
(Incomplete
 AS_REQ)  ->
                  AS_REQ ->
                                    <- AS_REP
                  TGS_REQ
                   U-2-U ->
                                    <- TGS_REP
               <- DHCPOFFER,
                   (AS_REP,
                   AP_REQ,
                   Integrity)
DHCPREQUEST
```

```
 (Integrity) ->
                <- DHCPACK
                    (Integrity)
DHCPDISCOVER
 (Incomplete
 AS_REQ)  ->
```

2.6.2. INIT-REBOOT, RENEWING or REBINDING

In the intra-realm or inter-realm case where the original user-to-user ticket is still valid, and the DHCP server still has a valid TGT to the home realm, the conversation will appear as follows:

```
   DHCP               DHCP             Home
   Client             Server            KDC
--------------     -------------     ---------

DHCPREQUEST
 (TGT,
 Integrity)  ->
                  TGS_REQ
                   U-2-U ->
                                  <- TGS_REP
                <- DHCPACK
                    (AP_REQ,
                    Integrity)
```

In the intra-realm or inter-realm case where the DHCP server validates the integrity attribute in the DHCPREQUEST, but receives a KRB_ERROR in response to the TGS_REQ to the KDC, the DHCP sever MAY choose not to silently discard the DHCPREQUEST and MAY return an authenticated DHCPNAK to the client instead, using the user-to-user session key previously established with the client. The conversation appears as follows:

```
   DHCP               DHCP             Home
   Client             Server            KDC
--------------     -------------     ---------

DHCPREQUEST
 (TGT,
 Integrity)  ->
                  TGS_REQ
                   U-2-U ->
                                  <- KRB_ERROR
                <- DHCPNAK
                    (KRB_ERROR,
                    Integrity)
DHCPDISCOVER
```

```
 (Incomplete
 AS_REQ)  ->
```

In the intra-realm or inter-realm case where the DHCP server cannot validate the integrity attribute in the DHCPREQUEST, the DHCP server MUST silently discard the DHCPREQUEST and the conversation will appear as follows:

```
   DHCP               DHCP
   Client             Server            KDC
--------------     -------------     ---------

DHCPREQUEST
 (TGT,
 Integrity)  ->
                  Silent discard
[Sequence repeats
 until timeout]

DHCPDISCOVER
 (Incomplete
 AS_REQ)  ->
```

In the intra-realm or inter-realm case where the original user-to-user ticket is still valid, the server validates the integrity attribute in the DHCPREQUEST, but the client fails to validate the integrity attribute in the DHCPACK, the client will silently discard the DHCPACK. The conversation will appear as follows:

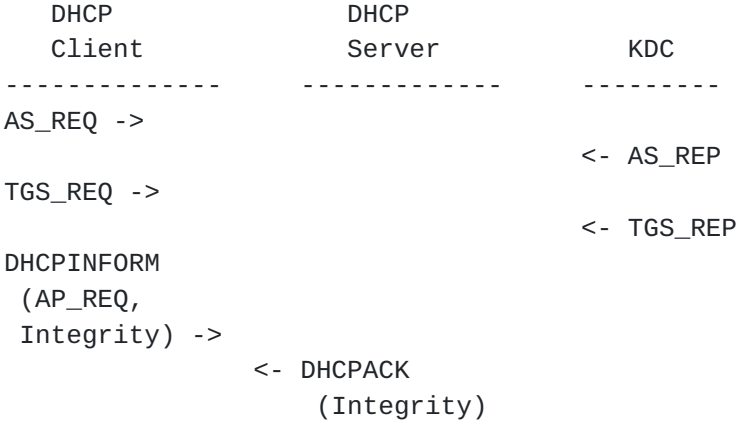
```
   DHCP               DHCP
   Client             Server            KDC
--------------     -------------     ---------

DHCPREQUEST
 (TGT,
 Integrity)  ->

                <- DHCPACK
                    (AP_REQ,
                    Integrity)
DHCPDISCOVER
 (Incomplete
 AS_REQ)  ->
```

2.6.3. DHCPINFORM (with known DHCP server)

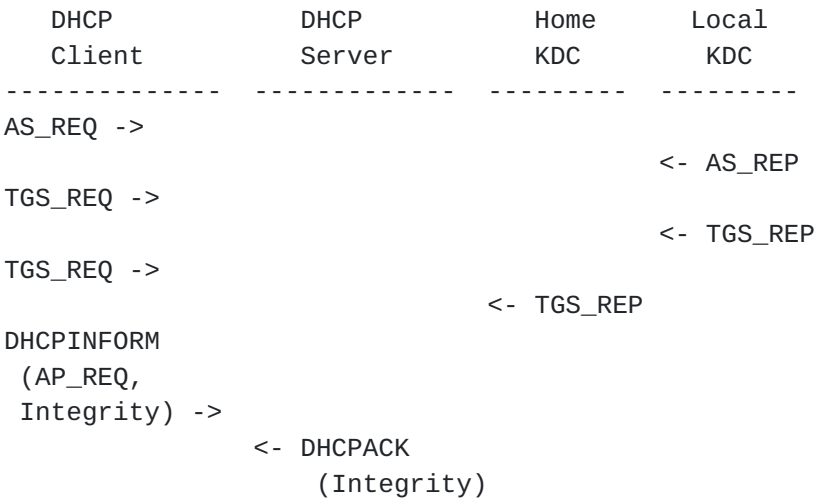
In the case where the DHCP client knows the DHCP server it will be interacting with, the DHCP client will obtain a ticket to the DHCP

server and will include AP_REQ and integrity attributes within the DHCPINFORM.

Where the DHCP Kerberos mutual authentication is successful, the conversation will appear as follows:

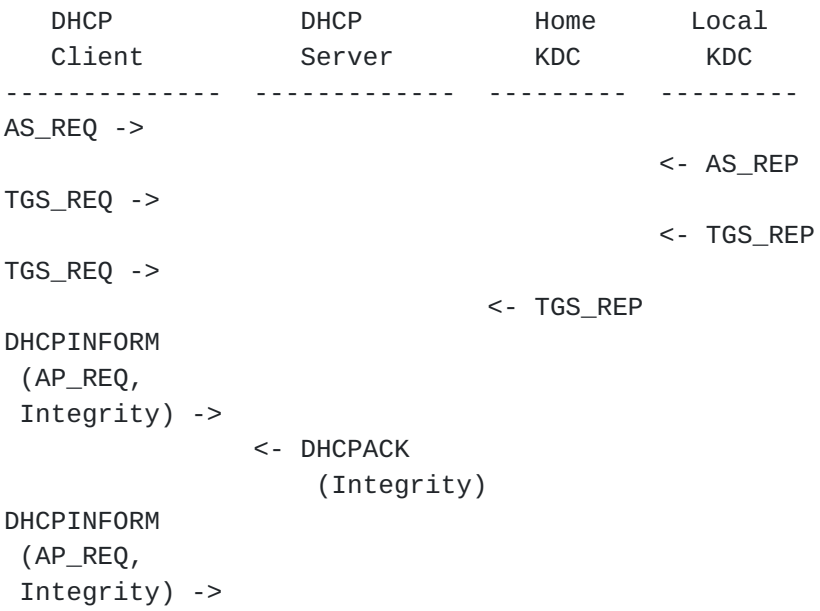


In the inter-realm case where the DHCP Kerberos mutual authentication is successful, the conversation will appear as follows:

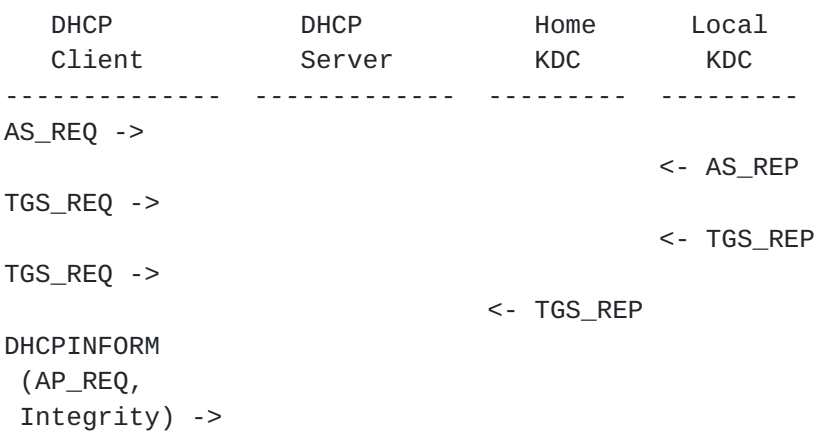


In the inter-realm case where the DHCP server fails to validate the integrity attribute in the DHCPINFORM, the server MUST silently discard the DHCPINFORM.

The conversation will appear as follows:



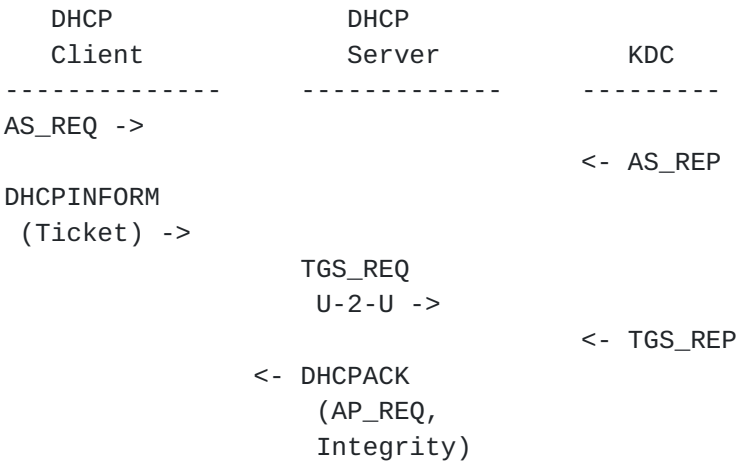
In the inter-realm case where the DHCP client fails to validate the integrity attribute in the DHCPACK, the client MUST silently discard the DHCPACK. The conversation will appear as follows:



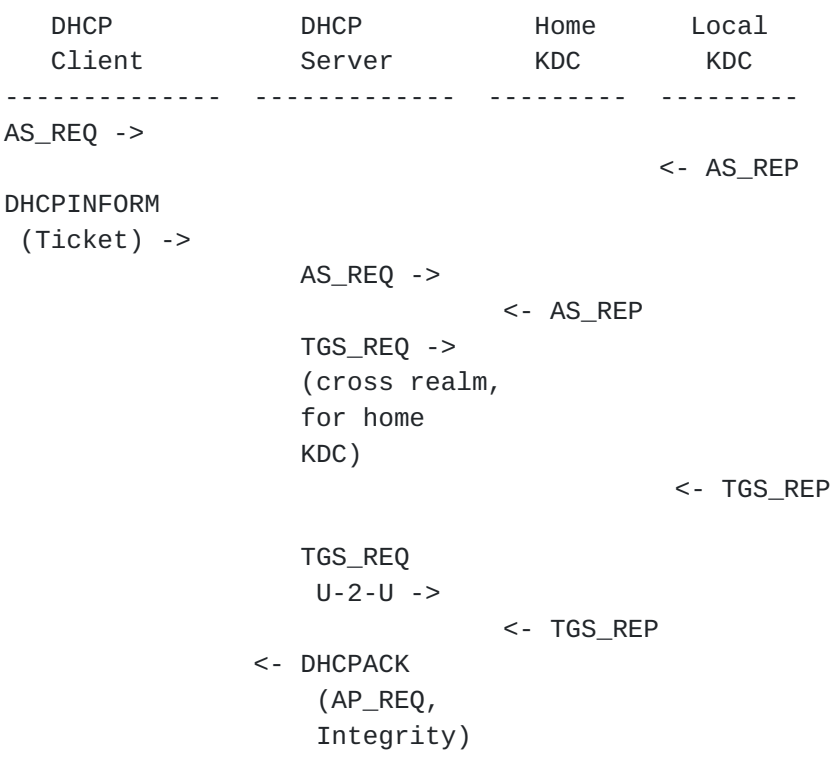
2.6.4. DHCPINFORM (with unknown DHCP server)

In the case where the DHCP client does not know the DHCP server it will be interacting with, the DHCP client will only include a ticket attribute within the DHCPINFORM. Thus the DHCP server will not be able to validate the authentication option.

Where the DHCP client is able to validate the DHCPACK and no error occurs, the conversation will appear as follows:

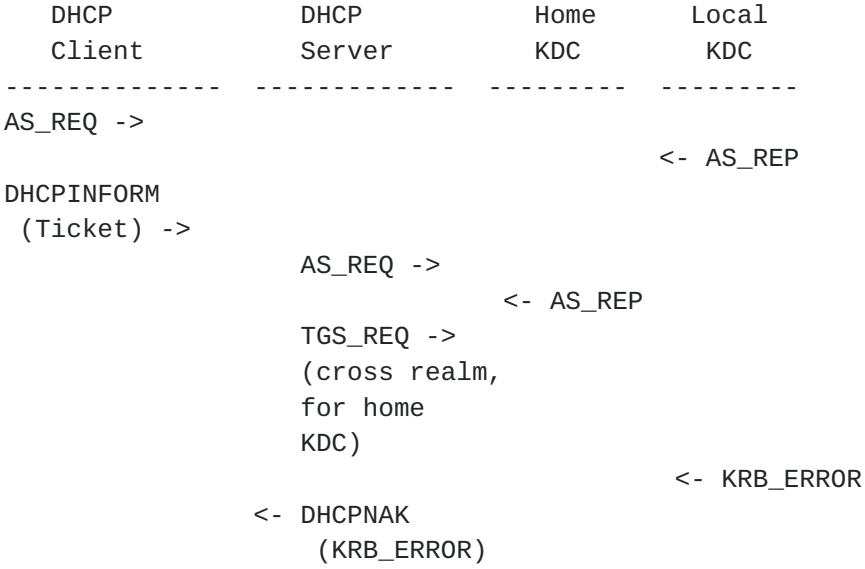


In the inter-realm case where the DHCP server needs to obtain a TGT to the home realm, and where the client successfully validates the DHCPACK, the conversation will appear as follows:

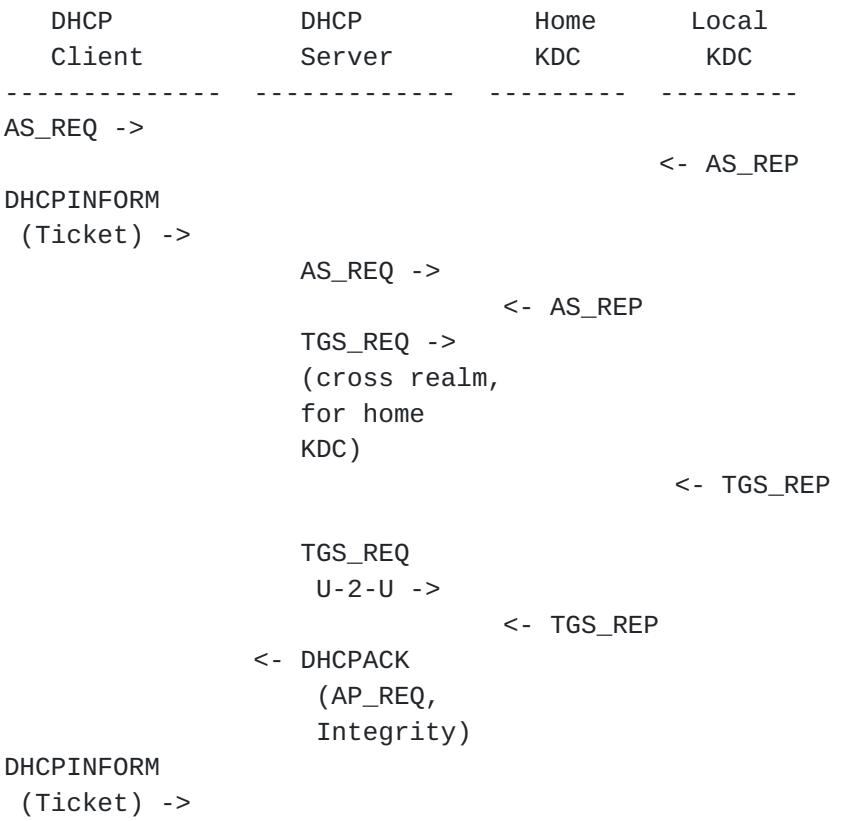


In the inter-realm case where the local KDC returns a KRB_ERROR in response to the TGS_REQ from the DHCP server, the DHCP server MAY return a KRB_ERROR within the DHCP authentication option included in a DHCPNAK.

The conversation will appear as follows:



In the inter-realm case where the DHCP client fails to validate the integrity attribute in the DHCPACK, the client MUST silently discard the DHCPACK. The conversation will appear as follows:



3. References

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

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

[3] Droms, R., Arbaugh, W., "Authentication for DHCP Messages", RFC 3118, June 2001.

[4] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[5] Alexander, S., Droms, R., "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[6] Henry, M., "DHCP Option 61 UUID Type Definition", Internet draft (work in progress), draft-henry-DHCP-opt61-UUID-type-00.txt, November 1998.

[7] IEEE Standards for Local and Metropolitan Area Networks: Port based Network Access Control, IEEE Std 802.1X-2001, June 2001.

[8] Tung, B., Neuman, C., Hur, M., Medvinsky, A., Medvinsky, S., Wray, J., Trostle, J., "Public Key Cryptography for Initial Authentication in Kerberos", Internet draft (work in progress), draft-ietf-cat-kerberos-pk-init-14.txt, July 2001.

[9] Hur, M., Tung, B., Ryutov, T., Neuman, C., Medvinsky, A., Tsudik G., Sommerfeld, B., "Public Key Cryptography for Cross-Realm Authentication in Kerberos", Internet draft (work in progress), draft-ietf-cat-kerberos-pk-cross-07.txt, December 2001.

[10] Mills, D., "Network Time Protocol (Version 3)", RFC-1305, March 1992.

4. Security Considerations

DHCP authentication, described in [3], addresses the following threats:

- Modification of messages
- Rogue servers
- Unauthorized clients

This section describes how DHCP authentication via Kerberos V addresses each of these threats.

4.1. Client security

As noted in [3], it may be desirable to ensure that IP addresses are only allocated to authorized clients. This can serve to protect against denial of service attacks. To address this issue it is necessary for DHCP client messages to be authenticated. In order to guard against message modification, it is also necessary for DHCP client messages to be integrity protected.

Note that this protocol does not make use of KRB_SAFE, so as to allow modification of mutable fields by the DHCP relay. Replay protection is therefore provided within the DHCP authentication option itself.

In DHCP authentication via Kerberos V the DHCP client will authenticate, integrity and replay-protect the DHCPREQUEST, DHCPDECLINE and DHCPRELEASE messages using a user-to-user session key obtained by the DHCP server from the home KDC. If the DHCP client knows the DHCP server it will be interacting with, then the DHCP client MAY also authenticate, integrity and replay-protect the DHCPINFORM message using a session key obtained from the local realm KDC for the DHCP server it expects to converse with.

Since the client has not yet obtained a session key, DHCPDISCOVER packets cannot be authenticated using the session key. However, the client MAY include pre-authentication data in the PADATA field included in the DHCPDISCOVER packet. Since the PADATA will then be used by the DHCP server to request a ticket on the client's behalf, the DHCP server will learn from the AS_REP whether the PADATA was acceptable or not. Therefore in this case, the DHCPDISCOVER will be authenticated but not integrity protected.

Where the DHCP client does not know the DHCP server it will be interacting with ahead of time, the DHCPINFORM message will not be authenticated, integrity or replay protected.

Note that snooping of PADATA and TGTs on the wire may provide an attacker with a means of mounting a dictionary attack, since these items

are typically encrypted with a key derived from the user's password. Thus use of strong passwords and/or pre-authentication methods utilizing strong cryptography (see [8]) are recommended.

4.2. Network access control

DHCP authentication has been proposed as a method of limiting access to network media that are not physically secured such as wireless LANs and ports in college residence halls. However, DHCP is not well suited to this purpose since even if address allocation is denied an unauthentic client may use a statically assigned IP address instead, or may attempt to access the network using non-IP protocols. As a result, other methods, such as IEEE 802.1X Network Port access control [7], have been proposed for controlling access to wireless media and switched LANs.

4.3. Server security

As noted in [3], it may be desirable to protect against rogue DHCP servers put on the network either intentionally or by accident. To address this issue it is necessary for DHCP server messages to be authenticated. In order to guard against message modification, it is also necessary for DHCP server messages to be integrity protected. Replay protection is also provided within the DHCP authentication option.

All messages sent by the DHCP server are authenticated and integrity and replay protected using a session key. This includes the DHCPOFFER, DHCPACK, and DHCPNAK messages. The session key is used to compute the DHCP authentication option, which is verified by the client.

In order to provide protection against rogue servers it is necessary to prevent rogue servers from obtaining the credentials necessary to act as a DHCP server. As noted in Section 4, the Kerberos principal name for the DHCP server must be of type KRB_NT_SRV_HST with the service name component equal to 'dhcp'. The client MUST validate that the DHCP server principal name has the above format. This convention requires that the administrator ensure that non-DHCP server principals do not have names that match the above format.

5. IANA Considerations

This draft does not create any new number spaces for IANA administration.

Acknowledgments

The authors would like to acknowledge Ralph Droms and William Arbaugh, authors of the DHCP authentication draft [3]. This draft incorporates material from their work; however, any mistakes in this document are solely the responsibility of the authors.

Authors' Addresses

Ken Hornstein
US Naval Research Laboratory
Bldg A-49, Room 2
4555 Overlook Avenue
Washington DC 20375 USA

Phone: +1 (202) 404-4765
EMail: kenh@cmf.nrl.navy.mil

Ted Lemon
Internet Engines, Inc.
950 Charter Street
Redwood City, CA 94063

Phone: +1 (650) 779 6031
Email: mellon@iengines.net

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 (425) 936-6605
EMail: bernarda@microsoft.com

Jonathan Trostle
170 W. Tasman Dr.
San Jose, CA 95134, U.S.A.

Email: jtrostle@cisco.com
Phone: +1 (408) 527-6201

Intellectual Property Statement

Full Copyright Statement

Expiration Date

This memo is filed as <draft-hornstein-dhc-kerbauth-06.txt>, and expires May 1, 2002.