Forcerenew Key Authentication
draft-miles-dhc-forcerenew-key-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on September 4, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents in effect on the date of publication of this document (http://trustee.ietf.org/license-info). Please review these documents carefully, as they describe your rights and restrictions with respect to this document.
Abstract

DHCP Forcerenew allows for the reconfiguration of a single host by forcing the DHCP client into a Renew state on a trigger from the DHCP server. In Forcerenew Key Authentication the server exchanges a key with the client on the initial DHCP ACK that is used for subsequent validation of a Forcerenew message.

Table of Contents

1. Introduction .................................................. 3
   1.1. Requirements Language .................................. 3
2. Message authentication ......................................... 3
   2.1. Forcerenew Key Authentication ............................ 3
       2.1.1. Forcerenew Key Protocol Capability Option ............ 4
       2.1.2. Forcerenew Key Protocol ............................... 4
       2.1.3. Server considerations for Forcerenew Key Authentication .................................................. 5
       2.1.4. Client considerations for Forcerenew Key Authentication .................................................. 6
3. Contributors .................................................... 6
4. IANA Considerations ........................................... 7
5. Security Considerations ......................................... 7
   5.1. Protocol vulnerabilities .................................... 7
6. References ....................................................... 7
   6.1. Normative References ....................................... 7
   6.2. Informative References ..................................... 8
Authors’ Addresses ................................................ 8
1. Introduction

This document defines extensions to Authentication for DHCP(v4) Messages [RFC3118] to create a new authentication protocol for DHCPv4 Forcerenew [RFC3203] messages. Authentication for DHCP [RFC3118] is mandatory for Forcerenew, however as it is currently defined [RFC3118] requires distribution of constant token or shared-secret out-of-band to DHCP clients. The Forcerenew Key is exchanged between server and client on initial DHCP ACK and is used for verification of any subsequent Forcerenew message.

Forcerenew Key Authentication follows the model set forward in DHCPv6 [RFC3315] as the Reconfigure Key Authentication Protocol.

1.1. 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].

2. Message authentication

The FORCERENEW message must be authenticated using either [RFC3118] or the proposed Forcerenew Key Authentication protocol.

2.1. Forcerenew Key Authentication

The Forcerenew key authentication protocol provides protection against misconfiguration of a client caused by a Forcerenew message sent by a malicious DHCP server. In this protocol, a DHCP server sends a Forcerenew Key to the client in the initial exchange of DHCP messages. The client records the Forcerenew Key for use in authenticating subsequent Forcerenew messages from that server. The server then includes an HMAC computed from the Forcerenew Key in subsequent Forcerenew messages.

Both the Forcerenew Key sent from the server to the client and the HMAC in subsequent Forcerenew messages are carried as the Authentication information in a DHCP Authentication option. The format of the Authentication information is defined in the following section.

The Forcerenew Key protocol is used (initiated by the server) only if the client and server are not using any other authentication protocol and the client and server have negotiated to use the Forcerenew Key Authentication protocol.
2.1.1. Forcerenew Key Protocol Capability Option

A DHCP client indicates DHCP Forcerenew Key Protocol capability by including a FORCERENEW_KEY_CAPABLE(<TBD>) option in DHCP Discover and Request messages sent to the server.

The inclusion of this option by the DHCP client indicates support for the Forcerenew Key Protocol authentication. The use of this option avoids the client attempting to negotiate a DHCP authentication protocol through the authentication option where a server does not support it and would otherwise fail. A DHCP server that does not support Forcerenew Key Protocol authentication should ignore the FORCERENEW_KEY_CAPABLE(<TBD>) option.

A DHCP client MUST NOT send DHCP Discover messages with authentication options where the protocol is (<TBD>).

The format of option TBD is as follows:

```
+-----+-----+-----+
| TBD |  1  |  1  |
+-----+-----+-----+
```

The client would indicate that it supports the functionality by inserting an Parameter Request List option (option 55, [RFC2131]) containing option <TBD> in the DHCP Discover message.

2.1.2. Forcerenew Key Protocol

[RFC3118] defined an extensible DHCPv4 authentication option which supports multiple protocols. The Forcerenew Key Protocol makes use of the DHCP authentication option defined in [RFC3118] re-using the option format.

The following fields are set in an DHCP authentication option for the Forcerenew Key Authentication Protocol:

- protocol <TBD (IANA)>
- algorithm 1
- RDM 0

The format of the Authentication information for the Forcerenew Key Authentication Protocol is:
<table>
<thead>
<tr>
<th>Type</th>
<th>Value (128 bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Forcerenew Server Capability (Offer message)</td>
</tr>
<tr>
<td>1</td>
<td>Forcerenew Key value (used in ACK message).</td>
</tr>
<tr>
<td>2</td>
<td>HMAC-MD5 digest of the message (FORCERENEW message).</td>
</tr>
</tbody>
</table>

2.1.3. Server considerations for Forcerenew Key Authentication

The use of Forcerenew Key Protocol is dependent on the client indicating its capability through the FORCERENEW_KEY_CAPABLE(<TBD>) DHCP option in any DHCP Discover or Request messages. The DHCP Discovery or Request message from the client MUST contain the FORCERENEW_KEY_CAPABLE(<TBD>) option if the Forcerenew Key Protocol is to be used by the server. The absence of the FORCERENEW_KEY_CAPABLE(<TBD>) option indicates to the server that the Forcerenew Key Authentication protocol is not supported and thus the server MUST NOT include a Forcerenew Key Protocol Authentication option in the DHCP Offer or Ack.

The server indicates its support of the Forcerenew Key Protocol authentication by including the DHCP authentication option in the DHCP Offer message where the type of the Authentication option is set to 0 (Forcerenew Server Capability) and the value is set to 128-bits of zero(0). The presence of the authentication option in the DHCP offer may be used by clients to prefer Forcerenew Key Protocol authentication-capable DHCP Offers over those Offers which do not include such capability.

The server selects a Forcerenew Key for a client during both the Request/Ack message exchange. The server records the Forcerenew Key and transmits that key to the client in an Authentication option in the DHCP Ack message.
The Forcerenew Key is 128 bits long, and MUST be a cryptographically strong random or pseudo-random number that cannot easily be predicted.

To provide authentication for a Forcerenew message, the server selects a replay detection value according to the RDM selected by the server, and computes an HMAC-MD5 of the Forcerenew message using the Forcerenew Key for the client. The server computes the HMAC-MD5 over the entire DHCP Forcerenew message, including the Authentication option; the HMAC-MD5 field in the Authentication option is set to zero for the HMAC-MD5 computation. The server includes the HMAC-MD5 in the authentication information field in an Authentication option included in the Forcerenew message sent to the client.

### 2.1.4. Client considerations for Forcerenew Key Authentication

The client must indicate Forcerenew Key Capability by including the FORCERENEW_KEY_CAPABLE(<TBD>) DHCP option (Section 2.1.1) in all DHCP Discover and Request messages. DHCP servers that support Forcerenew Key Protocol authentication will include the DHCP Forcerenew Key protocol authentication option in DHCP Offers with type set to zero(0), allowing the client to use this capability in selecting DHCP servers should multiple Offers arrive.

A DHCP client that has advertised Forcerenew Key Protocol authentication capability and a DHCP server has indicated its support through the inclusion of the DHCP authentication option in the DHCP Offer, the client MUST validate the DHCP Ack message contains a Forcerenew Key in a DHCP authentication option. If the server has indicated capability for Forcerenew Key Protocol authentication in the DHCP Offer and a subsequent Ack omits a valid DHCP authentication option for the Forcerenew Key Protocol, the client MUST send a DHCP Decline message and return to the DHCP Init state.

The client will receive a Forcerenew Key from the server in the initial DHCP Ack message from the server. The client records the Forcerenew Key for use in authenticating subsequent Forcerenew messages.

To authenticate a Forcerenew message, the client computes an HMAC-MD5 over the DHCP Forcerenew message, using the Forcerenew Key received from the server. If this computed HMAC-MD5 matches the value in the Authentication option, the client accepts the Forcerenew message.

### 3. Contributors

Comments are solicited and should be addressed to the DHC WG mailing
4. IANA Considerations

This document requests IANA to allocate an option code for the newly defined DHCP option FORCERENEW_KEY_CAPABLE as described in the text.

This document requests IANA to allocate a DHCP Authentication Option(90) protocol number be assigned for Forcerenew Key Authentication, per [RFC3118].

This document requests IANA to create a new namespace associated with the Forcerenew Key Authentication protocol: algorithm, per [RFC3118].

5. Security Considerations

As in some network environments FORCERENEW can be used to snoop and spoof traffic, the FORCERENEW message MUST be authenticated using the procedures as described in [RFC3118] or this proposal. FORCERENEW messages failing the authentication should be silently discarded by the client.

5.1. Protocol vulnerabilities

The mechanism described in this document is vulnerable to a denial of service attack through flooding a client with bogus FORCERENEW messages. The calculations involved in authenticating the bogus FORCERENEW messages may overwhelm the device on which the client is running.

The mechanism described provides protection against the use of a FORCERENEW message by a malicious DHCP server to mount a denial of service or man-in-the-middle attack on a client. This protocol can be compromised by an attacker that can intercept the initial message in which the DHCP server sends the key to the client.

6. References

6.1. Normative References


[RFC2131] Droms, R., "Dynamic Host Configuration Protocol".


6.2. Informative References


Authors’ Addresses

David Miles
Alcatel-Lucent
L3 / 215 Spring St
Melbourne, Victoria  3000
Australia

Phone: +61 3 9664 3308
Email: david.miles@alcatel-lucent.com

Wojciech Dec
Cisco Systems
Haarlerbergpark Haarlerbergweg 13-19
Amsterdam, NOORD-HOLLAND  1101 CH
Netherlands

Phone:
Email: wdec@cisco.com

James Bristow
Swisscom Schweiz AG
Zentweg 9
Bern,  3050
Switzerland

Phone:
Email: James.Bristow@swisscom.com