

DHC
Internet-Draft
Expires: August 24, 2003

T. Lemon
nominum
M. Richardson
SSW
February 23, 2003

Securing DHCP with DNSSEC bourne public keys
draft-richardson-dhc-auth-sig0-00.txt

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

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/lid-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 August 24, 2003.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

The abstract.

This document is intended as a standards track document.

Internet-Draft

auth-sig0

February 2003

Table of Contents

1.	Introduction	3
2.	Definition of RSA authentication option for DHCP	4
3.	Definition of DSA authentication option for DHCP	5
4.	Model of operation	6
5.	Samples	10
6.	IANA Considerations	11
7.	Acknowledgments	12
	Normative references	13
	Authors' Addresses	13
	Full Copyright Statement	14

Internet-Draft

auth-sig0

February 2003

[1.](#) Introduction

[1] defines a method for authenticating DHCP messages. It does provide for a way to do key management for the many relationships that a DHCP server may have.

In particular, the scaling problem of pre-shared keys fails badly in open networks such as those that occur at conferences such as IETF. In the context of conferences, it is not just malicious attacks that are a problem to the network, but also rogue DHCP servers present due to misconfiguration on the part of attendees.

[illegible]

This section defines the contents of the Authentication Information

field of this payload. [5] defines the RSA signature algorithm. [4] provides a more concise definition. The RSA signature is defined with MD5 as the hash algorithm.

[3.](#) Definition of DSA authentication option for DHCP

a diagram of the auth section for DSA, i.e. with Algorithm=2.

[4.](#) Model of operation

[4.1](#) Additions to client side state machine

Section 4.4 of [\[2\]](#) defines the state machine for the DHCP client.

[4.2](#) Client INIT state changes

No changes to the transitions for this state.

When the client sends the DHCP DISCOVER message, it MUST sign the request with its private key, including an authentication option in the DISCOVER message in an option as defined above. The client SHOULD cache the resulting signature such that it can retransmit it.

(XXX - is there any value in this? The xid will change each time).

The client MUST include its proposed fully-qualified domain name in a client FQDN, as specified in [6].

The client MUST include a parameter request list option that includes the DHCP authentication option, and the Server Name option.

[4.3](#) Client SELECTING state changes

No changes to the transitions for this state.

The client SHOULD prefer DHCP OFFERS that include a authentication option that are signed by keys that the client currently has cached.

If no preferred offer is seen, then the client MUST select among the offers in a non-deterministic manner (ideally, random). This step is important so that a client that has been deceived into binding to the wrong DHCP server will have a chance to select a different server.

A client SHOULD NOT assume that offers that do not include valid and verifiable signature options are exclusively preferred. There may be no DHCP security on the network in question, and attackers could keep the client from ever selecting the "real", unauthenticated server. (XXX - yet, if one can remember them all, one would prefer to try the offers with signatures first)

Note that this behaviour differs from that described in point 2 of section 5.5.1 of [1]. This is because a client may not be able to determine the authenticity of the offer until after it has connected to the network. Should an appropriate DHCP server key be pre-configured, or cached, then the behaviour is the same.

[4.4](#) Client REQUESTING state changes

A new state called "Provisionally BOUND" MUST be added. The system will transition to this new state upon receipt of a DHCP ACK that contains a DHCP authentication option, and a DHCP Server name option.

When sending the DHCP REQUEST to the server, it MUST also be signed.

The DHCP REQUEST MUST also include the same client FQDN as was sent in the DISCOVER message.

XXX - should the DHCP Decline be signed? I think so.

4.5 Provisionally BOUND state

The provisionally bound state is operationally similar to the BOUND state. The timers should be recorded as with the previous state. Additional DHCP offers received should be discarded.

The system should be sufficiently configured with the provided IP address such that DNS requests to the root name server(s) may be done. If the system is going to be configured with the a DNS server as specified in the Domain Name Server option of [3], and this name server is directly reachable, it may be reasonable to defer any additional system configuration until the BOUND state. Some systems may not provide such a "partially configured" state.

In any case, if the system has any kind of system event that indicates that it is on the network, this event SHOULD be deferred until the BOUND state has been reached.

Upon entering this state, after performing the partial configuration, the client MUST authenticate the DHCP ACK. To do this, if it does not already have the public key of the DHCP server, it must look it up.

The client MUST lookup the KEY resource record (subtype DNSSEC) associated with the name provided by the server in its DHCP server name option. The DNS lookup SHOULD be done with DNSSEC enabled.

{XXX - DHCP server name option. Is there such a thing? The original idea was to lookup the KEY record in the reverse map (in-addr.arpa/ip6.arpa), based upon the IP address in the server identifier. Ted suggested that we wanted to use FQDN, but I'm not sure where it will get stored. Do we need a new option}

If the DHCP ACK can not be authenticated (either because the KEY can not be retrieved, the DNSSEC does not authenticate the key, or integrity check on the message fails), then the lease MUST be

discarded. The client transitions back to INIT state, having sent a DHCPNAK to the server, and then halting the network.

XXX - Do we go back and authenticate the DHCP OFFER?

[4.6](#) Client BOUND state changes

There is a new transition from the Provisionally BOUND state.

The only change in behaviour of this state is that when lease renewal occurs, the DHCP REQUEST SHOULD be signed. This is done even if the lease was not originally acquired through a signature, as it MAY be that the server will adopt security in the interim.

[4.7](#) Client RENEWING state changes

There is a new transition to the Provisionally BOUND state.

If a DHCP ACK is received that has a DHCP Authentication option in it, then the client transitions to the Provisionally BOUND state rather than directly back to the BOUND state.

[4.8](#) Client REBINDING state changes

The system will transition to Provisionally BOUND upon receipt of a DHCP ACK that contains a DHCP authentication option, and a DHCP Server name option.

The broadcast DHCP REQUEST SHOULD contain an authentication option, as with the one sent by state SELECTING.

[4.9](#) Additions to server side state machine

Section 4.4 of [2] defines the state machine for the DHCP client.

[4.9.1](#) DHCP DISCOVER processing changes

Upon receipt of a DHCP DISCOVER that includes an Authentication option of the type defined in this document, then it MUST verify that there is a provided client FQDN option, and that it is fully qualified.

The server MUST then do a DNSSEC lookup on the provided FQDN, looking for a KEY resource record (sub-type DNSSEC). The server SHOULD cache this result for at least as long as the DHCP OFFER that will be made would be valid for. The server MAY cache it for as long as the DNS time to live value.

Internet-Draft

auth-sig0

February 2003

Having found a valid KEY (with the matching keyid), the server MAY verify the signature at this point. If the server feels that it is overloaded or under denial of service attack, it may defer authentication at this step.

If appropriate authentication material is not found, then the request SHOULD be treated as if none were present. If authentication material was found, but the signature check fails, then the message MUST be discarded. Audit entries SHOULD be made, including the keyid that was used, and the computed vs actual MD5 checks.

[4.9.2](#) DHCP REQUEST processing changes

Upon receipt of a DHCP REQUEST that includes an Authentication option of the type defined in this document, then it MUST verify that there is a provided client FQDN option, and that it is fully qualified.

The server MAY have already cached the KEY record associated with this FQDN. If it has not, then it MUST lookup the record again, as described above.

The signature MUST be authenticated in this step.

The server MAY then insert the provided FQDN into the reverse map using dynamic update, as described in [\[6\]](#).

If the client has requested it, via the DHCP IPSECKEY option, then the server should also insert the public key taken from the FQDN into the reverse map.

[4.9.3](#) DHCP DECLINE processing changes

XXX - unclear yet.

[4.9.4](#) Annotated exchange between client and server

Internet-Draft

auth-sig0

February 2003

[5. Samples](#)

[5.1 Sample RSA keys and signature options for client](#)

Using a private key of: XXXX, having a public key value of: YYYY. We produced the following authentication option:

[5.2 Sample DSA keys and signature options for client](#)

Using a private key of: XXXX, having a public key value of: YYYY. We produced the following authentication option:

[5.3 Sample DSA keys and signature options for server](#)

Using a private key of: XXXX, having a public key value of: YYYY. We produced the following authentication option:

[5.4 Sample DSA keys and signature options for server](#)

Using a private key of: XXXX, having a public key value of: YYYY. We produced the following authentication option:

[6.](#) IANA Considerations

IANA will need to assign X.

[7](#). Acknowledgments

Original ideas due to Randy Bush, ...

Normative references

- [1] Droms, R., Editor, Arbaugh, W. and Editor, "Authentication for DHCP Messages", [RFC 3118](#), June 2001.
- [2] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [3] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", [RFC 2132](#), March 1997.
- [4] Eastlake, D., "RSA/MD5 KEYS and SIGs in the Domain Name System (DNS)", [RFC 2537](#), March 1999.
- [5] Jonsson, J. and B. Kaliski, "Public-Key Cryptography Standards

(PKCS) #1: RSA Cryptography Specifications Version 2.1", [RFC 3447](#), February 2003.

- [6] Stapp, M. and Y. Rekhter, "The DHCP Client FQDN Option", ID internet-draft ([draft-ietf-dhc-fqdn-option-05.txt](#)), November 2002.

Authors' Addresses

Ted Lemon
Nominum
Some City, AZ
USA

EMail: Ted.Lemon@nominum.com

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA

EMail: mcr@sandelman.ottawa.on.ca
URI: <http://www.sandelman.ottawa.on.ca/>

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any

kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

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