DNSEXT
Internet-Draft
Expires: January 14, 2005

M. Stapp
Cisco Systems, Inc.
T. Lemon
A. Gustafsson
Nominum, Inc.

July 16, 2004

A DNS RR for Encoding DHCP Information (DHCID RR)
<draft-ietf-dnsext-dhcid-rr-08.txt>

Status of this Memo

This document is an Internet-Draft and is subject to all provisions of section 3 of RFC 3667. By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she become aware will be disclosed, in accordance with RFC 3668.

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 January 14, 2005.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

It is possible for multiple DHCP clients to attempt to update the same DNS FQDN as they obtain DHCP leases. Whether the DHCP server or the clients themselves perform the DNS updates, conflicts can arise. To resolve such conflicts, "Resolution of DNS Name Conflicts" [1] proposes storing client identifiers in the DNS to unambiguously

associate domain names with the DHCP clients to which they refer. This memo defines a distinct RR type for this purpose for use by DHCP clients and servers, the "DHCID" RR.

Table of Contents

1. Terminology 3
2. Introduction 3
3. The DHCID RR 3
3.1 DHCID RDATA format 4
3.2 DHCID Presentation Format 4
3.3 The DHCID RR Type Codes 4
3.4 Computation of the RDATA 4
3.5 Examples 5
3.5.1 Example 1 6
3.5.2 Example 2 6
4. Use of the DHCID RR 6
5. Updater Behavior 6
6. Security Considerations 7
7. IANA Considerations 7
8. Acknowledgements 7
9. References 8
9.1 Normative References 8
9.2 Informative References 8
Authors' Addresses 9
Intellectual Property and Copyright Statements 10

1. Terminology

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 [2].

2. Introduction

A set of procedures to allow DHCP [7] clients and servers to automatically update the DNS (RFC 1034 [3], RFC 1035 [4]) is proposed in "Resolution of DNS Name Conflicts" [1].

Conflicts can arise if multiple DHCP clients wish to use the same DNS name. To resolve such conflicts, "Resolution of DNS Name Conflicts" [1] proposes storing client identifiers in the DNS to unambiguously associate domain names with the DHCP clients using them. In the interest of clarity, it is preferable for this DHCP information to use a distinct RR type. This memo defines a distinct RR for this purpose for use by DHCP clients or servers, the "DHCID" RR.

In order to avoid exposing potentially sensitive identifying information, the data stored is the result of a one-way MD5 [5] hash computation. The hash includes information from the DHCP client's REQUEST message as well as the domain name itself, so that the data stored in the DHCID RR will be dependent on both the client identification used in the DHCP protocol interaction and the domain name. This means that the DHCID RDATA will vary if a single client is associated over time with more than one name. This makes it difficult to 'track' a client as it is associated with various domain names.

The MD5 hash algorithm has been shown to be weaker than the SHA-1 algorithm; it could therefore be argued that SHA-1 is a better choice. However, SHA-1 is significantly slower than MD5. A successful attack of MD5's weakness does not reveal the original data that was used to generate the signature, but rather provides a new set of input data that will produce the same signature. Because we are using the MD5 hash to conceal the original data, the fact that an attacker could produce a different plaintext resulting in the same MD5 output is not significant concern.

3. The DHCID RR

The DHCID RR is defined with mnemonic DHCID and type code [TBD]. The DHCID RR is only defined in the IN class. DHCID RRs cause no additional section processing. The DHCID RR is not a singleton type.

3.1 DHCID RDATA format

The RDATA section of a DHCID RR in transmission contains RDLENGTH bytes of binary data. The format of this data and its interpretation by DHCP servers and clients are described below.

DNS software should consider the RDATA section to be opaque. DHCP clients or servers use the DHCID RR to associate a DHCP client's identity with a DNS name, so that multiple DHCP clients and servers may deterministically perform dynamic DNS updates to the same zone. From the updater's perspective, the DHCID resource record RDATA consists of a 16-bit identifier type, in network byte order, followed by one or more bytes representing the actual identifier:

```
< 16 bits >     DHCP identifier used
< n bytes >     MD5 digest
```

3.2 DHCID Presentation Format

In DNS master files, the RDATA is represented as a single block in base 64 encoding identical to that used for representing binary data in RFC 2535 [8]. The data may be divided up into any number of white space separated substrings, down to single base 64 digits, which are concatenated to form the complete RDATA. These substrings can span lines using the standard parentheses.

3.3 The DHCID RR Type Codes

The DHCID RR Type Code specifies what data from the DHCP client's request was used as input into the hash function. The type codes are defined in a registry maintained by IANA, as specified in Section 7. The initial list of assigned values for the type code is:

0x0000 = htype, chaddr from a DHCPv4 client's DHCPREQUEST [7].
0x0001 = The data portion from a DHCPv4 client's Client Identifier option [9].
0x0002 = The client's DUID (i.e., the data portion of a DHCPv6 client's Client Identifier option [10] or the DUID field from a DHCPv4 client's Client Identifier option [12]).

0x0003 - 0xfffe = Available to be assigned by IANA.

0xffff = RESERVED

3.4 Computation of the RDATA

The DHCID RDATA is formed by concatenating the two type bytes with

some variable-length identifying data.

< type > < data >

The RDATA for all type codes other than 0xffff, which is reserved for future expansion, is formed by concatenating the two type bytes and a 16-byte MD5 hash value. The input to the hash function is defined to be:

data = MD5(< identifier > < FQDN >)

The FQDN is represented in the buffer in unambiguous canonical form as described in RFC 2535 [8], section 8.1. The type code and the identifier are related as specified in Section 3.3: the type code describes the source of the identifier.

When the updater is using the client's link-layer address as the identifier, the first two bytes of the DHCID RDATA MUST be zero. To generate the rest of the resource record, the updater computes a one-way hash using the MD5 algorithm across a buffer containing the client's network hardware type, link-layer address, and the FQDN data. Specifically, the first byte of the buffer contains the network hardware type as it appeared in the DHCP 'htype' field of the client's DHCPREQUEST message. All of the significant bytes of the chaddr field in the client's DHCPREQUEST message follow, in the same order in which the bytes appear in the DHCPREQUEST message. The number of significant bytes in the 'chaddr' field is specified in the 'hlen' field of the DHCPREQUEST message. The FQDN data, as specified above, follows.

When the updater is using the DHCPv4 Client Identifier option sent by the client in its DHCPREQUEST message, the first two bytes of the DHCID RR MUST be 0x0001, in network byte order. The rest of the DHCID RR MUST contain the results of computing an MD5 hash across the payload of the option, followed by the FQDN. The payload of the option consists of the bytes of the option following the option code and length.

When the updater is using the DHCPv6 DUID sent by the client in its REQUEST message, the first two bytes of the DHCID RR MUST be 0x0002, in network byte order. The rest of the DHCID RR MUST contain the results of computing an MD5 hash across the payload of the option, followed by the FQDN. The payload of the option consists of the bytes of the option following the option code and length.

3.5 Examples

3.5.1 Example 1

A DHCP server allocating the IPv4 address 10.0.0.1 to a client with Ethernet MAC address 01:02:03:04:05:06 using domain name "client.example.com" uses the client's link-layer address to identify the client. The DHCID RDATA is composed by setting the two type bytes to zero, and performing an MD5 hash computation across a buffer containing the Ethernet MAC type byte, 0x01, the six bytes of MAC address, and the domain name (represented as specified in Section 3.4).

```
client.example.com.        A       10.0.0.1
client.example.com.        DHCID   AAAUMru0ZM5OK/PdVAJgZ/HU
```

3.5.2 Example 2

A DHCP server allocates the IPv4 address 10.0.12.99 to a client which included the DHCP client-identifier option data 01:07:08:09:0a:0b:0c in its DHCP request. The server updates the name "chi.example.com" on the client's behalf, and uses the DHCP client identifier option data as input in forming a DHCID RR. The DHCID RDATA is formed by setting the two type bytes to the value 0x0001, and performing an MD5 hash computation across a buffer containing the seven bytes from the client-id option and the FQDN (represented as specified in Section 3.4).

```
chi.example.com.   A       10.0.12.99
chi.example.com.   DHCID   AAHdd5jiQ3kEjANDm82cbObk\012
```

4. Use of the DHCID RR

This RR MUST NOT be used for any purpose other than that detailed in "Resolution of DNS Name Conflicts" [1]. Although this RR contains data that is opaque to DNS servers, the data must be consistent across all entities that update and interpret this record. Therefore, new data formats may only be defined through actions of the DHC Working Group, as a result of revising [1].

5. Updater Behavior

The data in the DHCID RR allows updaters to determine whether more than one DHCP client desires to use a particular FQDN. This allows site administrators to establish policy about DNS updates. The DHCID RR does not establish any policy itself.

Updaters use data from a DHCP client's request and the domain name

that the client desires to use to compute a client identity hash, and then compare that hash to the data in any DHCID RRs on the name that they wish to associate with the client's IP address. If an updater discovers DHCID RRs whose RDATA does not match the client identity that they have computed, the updater SHOULD conclude that a different client is currently associated with the name in question. The updater SHOULD then proceed according to the site's administrative policy. That policy might dictate that a different name be selected, or it might permit the updater to continue.

6. Security Considerations

The DHCID record as such does not introduce any new security problems into the DNS. In order to avoid exposing private information about DHCP clients to public scrutiny, a one-way hash is used to obscure all client information. In order to make it difficult to 'track' a client by examining the names associated with a particular hash value, the FQDN is included in the hash computation. Thus, the RDATA is dependent on both the DHCP client identification data and on each FQDN associated with the client.

Administrators should be wary of permitting unsecured DNS updates to zones which are exposed to the global Internet. Both DHCP clients and servers SHOULD use some form of update authentication (e.g., TSIG [11]) when performing DNS updates.

7. IANA Considerations

IANA is requested to allocate an RR type number for the DHCID record type.

This specification defines a new number-space for the 16-bit type codes associated with the DHCID RR. IANA is requested to establish a registry of the values for this number-space.

Three initial values are assigned in Section 3.3, and the value 0xFFFF is reserved for future use. New DHCID RR type codes are tentatively assigned after the specification for the associated type code, published as an Internet Draft, has received expert review by a designated expert. The final assignment of DHCID RR type codes is through Standards Action, as defined in RFC 2434 [6].

8. Acknowledgements

Many thanks to Josh Littlefield, Olafur Gudmundsson, Bernie Volz, and Ralph Droms for their review and suggestions.

9. References

9.1 Normative References

[1] Stapp, M. and B. Volz, "Resolution of DNS Name Conflicts Among DHCP Clients (draft-ietf-dhc-dns-resolution-*)", July 2004.

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

[3] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[4] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[5] Rivest, R., "The MD5 Message-Digest Algorithm", RFC 1321, April 1992.

[6] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 2434, October 1998.

9.2 Informative References

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

[8] Eastlake, D., "Domain Name System Security Extensions", RFC 2535, March 1999.

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

[10] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[11] Vixie, P., Gudmundsson, O., Eastlake, D. and B. Wellington, "Secret Key Transaction Authentication for DNS (TSIG)", RFC 2845, May 2000.

[12] Lemon, T. and B. Sommerfeld, "Node-Specific Client Identifiers for DHCPv4 (draft-ietf-dhc-3315id-for-v4-*)", February 2004.

Authors' Addresses

Mark Stapp
Cisco Systems, Inc.
1414 Massachusetts Ave.
Boxborough, MA 01719
USA

Phone: 978.936.1535
EMail: mjs@cisco.com

Ted Lemon
Nominum, Inc.
950 Charter St.
Redwood City, CA 94063
USA

EMail: mellon@nominum.com

Andreas Gustafsson
Nominum, Inc.
950 Charter St.
Redwood City, CA 94063
USA

EMail: gson@nominum.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM 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.

Copyright Statement

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

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