Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: February 28, 2016

P. Spacek
Red Hat, Inc.

August 27, 2015

Clarifications to the Dynamic Updates in the Domain Name System (DNS UPDATE) specification
draft-spacek-dnsop-update-clarif-01

Abstract

This document clarifies interaction among Dynamic Updates in the Domain Name System (DNS UPDATE), Classless IN-ADDR.ARPA delegation, and Secure Domain Name System (DNS) Dynamic Update in the presence of CNAME/DNAME redirections.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on February 28, 2016.

Copyright Notice

Table of Contents

1. Introduction

This document clarifies interaction among Dynamic Updates in the Domain Name System (DNS UPDATE) [RFC2136], Classless IN-ADDR.ARPA delegation [RFC2317], and Secure Domain Name System (DNS) Dynamic Update [RFC3007].

It was identified that common implementations using DNS update protocol often ignore existence of CNAME/DNAME redirections and, as a result, fail to update records if redirection is used. One common example is failure to update PTR records in classless IN-ADDR.ARPA zones.

[RFC2317] describes how to use the CNAME records in IN-ADDR.ARPA DNS zones to split administrative control over IN-ADDR.ARPA data for classless networks. The described method is perfectly compatible with standard DNS resolution but DNS update requests need special handling described in this document.

This clarification is applicable to parties wanting to update records in IN-ADDR.ARPA and other zones without changing existing CNAME/DNAME redirections. A typical example are PTR record updates in zones which might potentially use [RFC2317]. This clarification is not applicable to cases where the purpose of the DNS update is to change CNAME/DNAME redirection.

2. Document Conventions

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].

Terms "requestor", "update message", and names of update message's sections are used in the same sense as in [RFC2136].

Examples involving IN-ADDR.ARPA zone and PTR records are referring to [RFC2317].

3. Problem Description

The problem described herein typically occurs when an implementation intends to update resource records resolvable by using particular owner name while keeping all CNAME/DNAME redirections intact. In other words, the purpose of the update is to change resource records associated with terminal node of (potential) chain of redirections starting at a known owner name.

Typically, this is the case when the resource records are associated with a known owner name or an owner name that is derived from data obtained outside of DNS. For example, implementations often translate IPv4 address to DNS owner name using the algorithm from [RFC1034] section 5.2.1.4:

192.0.2.1 -> 1.2.0.192.in-addr.arpa.

The problem is that implementations often use this original node name in an Update Message without checking for redirections. If the original owner name contains redirection, then this behavior results in an attempt to add or delete another record to or from a node that already contains the CNAME record, and the update fails.

Such inappropriately constructed update request will be silently ignored in accordance with [RFC2136] section 3.4.2.2. Alternatively, an error will be reported to the requestor if the non-existence of the CNAME record was added as a prerequisite to the Update Message.

4. Clarification to Requestor Behaviour

Please see applicability note in Introduction (Section 1, Paragraph 4).

A Requestor MUST resolve (canonicalize) the original owner name (e.g. the one derived from an IPv4 address) to a canonical owner name

before constructing the Update Message. The requestor MUST follow whole chain of redirections until the terminal node of the chain is reached and use canonical name found at the terminal node. Implementations MUST detect infinite loops.

Canonical owner name MUST be used instead of the original owner name in the resulting Update Message:

- All names used in the Prerequisite and Update sections MUST be canonicalized as specified above. Only prerequisites concerning the CNAME or DNAME records are an exception to this rule and should not be canonicalized.

- ZNAME in the Zone Section has to contain the name of the zone that encloses the canonical owner names.

- An implementation MAY chose to use canonicalized names in RDATA and an Additional Section. This is an application specific decision.

5. IANA Considerations

This draft does not involve IANA Considerations.

6. Security Considerations

Canonicalization process changes the owner name which is going to be affected by the update. An active attacker might interfere with the canonicalization process and trick the requestor to update a node of the attacker's choice if the canonicalization process is not secured by using DNSSEC or by other means.

Security properties of DNS updates using only DNS UPDATE [RFC2136] without any security mechanisms on top of it are vulnerable anyway because an active attacker can very well modify the update message itself.

Canonicalization generally increases overall risk for implementations of Secure DNS Dynamic Update [RFC3007] because an attacker might have a chance to modify the owner name in an Update Message before the message is signed by the requestor. An implementation might decide to accept canonicalized names only on condition that the overall

security status of the canonicalization process is sufficient according to the local policy. Because the chain of redirections might involve multiple DNS zones, implementations MUST use the lowest security status from all links in the chain of redirections when doing security decisions.

For example, a strict implementation might accept canonicalized names only on condition that all redirections were secured by DNSSEC and the security state of all redirections was "secure". Another implementation might decide that security checks on a server side are sufficient, so requestors will accept canonical names obtained using insecure protocols. In case of PTR records, a server might require the TCP transport and map an IP address of the requestor to the canonical owner name and/or check data in an Update Message with the requestor's identity.

7. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

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

[RFC2136] Vixie, P., Thomson, S., Rekhter, Y., and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

[RFC2317] Eidnes, H., de Groot, G., and P. Vixie, "Classless IN-ADDR.ARPA delegation", BCP 20, RFC 2317, March 1998.

[RFC3007] Wellington, B., "Secure Domain Name System (DNS) Dynamic Update", RFC 3007, November 2000.

Author's Address

Petr Spacek
Red Hat, Inc.

Email: pspacek@redhat.com