Network Working Group
Request for Comments: 2540
Category: Experimental

D. Eastlake
IBM

March 1999

Detached Domain Name System (DNS) Information

Status of this Memo

Copyright Notice

Abstract

A standard format is defined for representing detached DNS information. This is anticipated to be of use for storing information retrieved from the Domain Name System (DNS), including security information, in archival contexts or contexts not connected to the Internet.

Table of Contents

1. Introduction

The Domain Name System (DNS) is a replicated hierarchical distributed database system [RFC 1034, 1035] that can provide highly available service. It provides the operational basis for Internet host name to address translation, automatic SMTP mail routing, and other basic Internet functions. The DNS has been extended as described in [RFC 2535] to permit the general storage of public cryptographic keys in

the DNS and to enable the authentication of information retrieved from the DNS though digital signatures.

The DNS was not originally designed for storage of information outside of the active zones and authoritative master files that are part of the connected DNS. However there may be cases where this is useful, particularly in connection with archived security information.

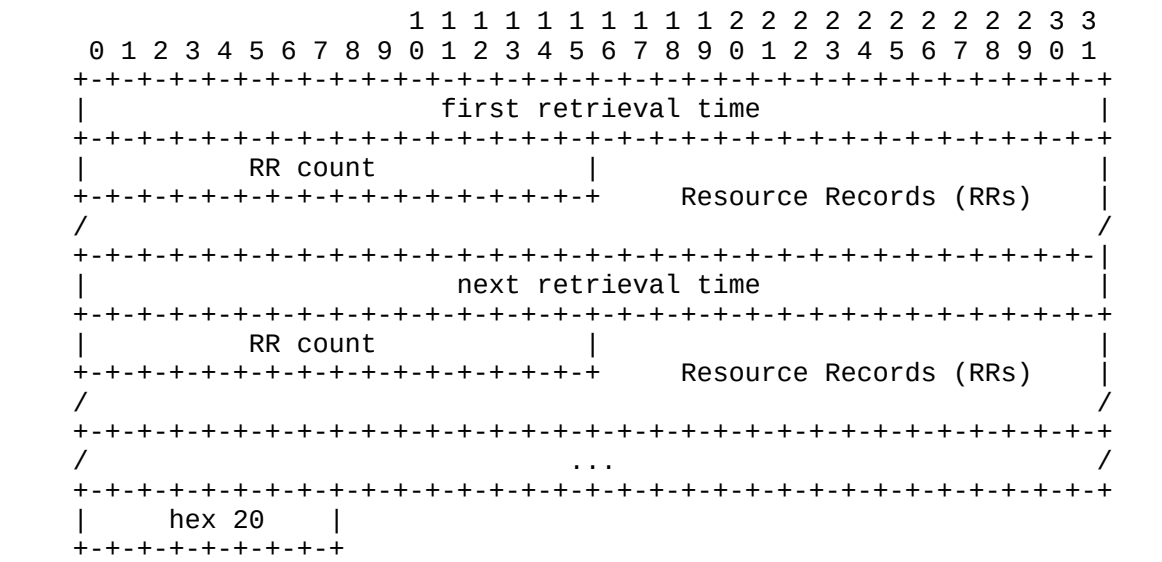
2. General Format

The formats used for detached Domain Name System (DNS) information are similar to those used for connected DNS information. The primary difference is that elements of the connected DNS system (unless they are an authoritative server for the zone containing the information) are required to count down the Time To Live (TTL) associated with each DNS Resource Record (RR) and discard them (possibly fetching a fresh copy) when the TTL reaches zero. In contrast to this, detached information may be stored in a off-line file, where it can not be updated, and perhaps used to authenticate historic data or it might be received via non-DNS protocols long after it was retrieved from the DNS. Therefore, it is not practical to count down detached DNS information TTL and it may be necessary to keep the data beyond the point where the TTL (which is defined as an unsigned field) would underflow. To preserve information as to the freshness of this detached data, it is accompanied by its retrieval time.

Whatever retrieves the information from the DNS must associate this retrieval time with it. The retrieval time remains fixed thereafter. When the current time minus the retrieval time exceeds the TTL for any particular detached RR, it is no longer a valid copy within the normal connected DNS scheme. This may make it invalid in context for some detached purposes as well. If the RR is a SIG (signature) RR it also has an expiration time. Regardless of the TTL, it and any RRs it signs can not be considered authenticated after the signature expiration time.

2.1 Binary Format

The standard binary format for detached DNS information is as follows:



Retrieval time - the time that the immediately following information was obtained from the connected DNS system. It is an unsigned number of seconds since the start of 1 January 1970, GMT, ignoring leap seconds, in network (big-endian) order. Note that this time can not be before the initial proposal of this standard. Therefore, the initial byte of an actual retrieval time, considered as a 32 bit unsigned quantity, would always be larger than 20 hex. The end of detached DNS information is indicated by a "retrieval time" field initial byte equal to 0x20. Use of a "retrieval time" field with a leading unsigned byte of zero indicates a 64 bit (actually 8 leading zero bits plus a 56 bit quantity). This 64 bit format will be required when retrieval time is larger than 0xFFFFFFFF, which is some time in the year 2106. The meaning of retrieval times with an initial byte between 0x01 and 0x1F is reserved (see section 5). Retrieval times will not generally be 32 bit aligned with respect to each other due to the variable length nature of RRs.

RR count - an unsigned integer number (with bytes in network order) of following resource records retrieved at the preceding retrieval time.

Resource Records - the actual data which is in the same format as if it were being transmitted in a DNS response. In particular, name compression via pointers is permitted with the origin at the beginning of the particular detached information data section, just after the RR count.

2.2. Text Format

The standard text format for detached DNS information is as prescribed for zone master files [RFC 1035] except that the $INCLUDE control entry is prohibited and the new $DATE entry is required (unless the information set is empty). $DATE is followed by the date and time that the following information was obtained from the DNS system as described for retrieval time in section 2.1 above. It is in the text format YYYYMMDDHHMMSS where YYYY is the year (which may be more than four digits to cover years after 9999), the first MM is the month number (01-12), DD is the day of the month (01-31), HH is the hour in 24 hours notation (00-23), the second MM is the minute (00-59), and SS is the second (00-59). Thus a $DATE must appear before the first RR and at every change in retrieval time through the detached information.

3. Usage Example

A document might be authenticated by a key retrieved from the DNS in a KEY resource record (RR). To later prove the authenticity of this document, it would be desirable to preserve the KEY RR for that public key, the SIG RR signing that KEY RR, the KEY RR for the key used to authenticate that SIG, and so on through SIG and KEY RRs until a well known trusted key is reached, perhaps the key for the DNS root or some third party authentication service. (In some cases these KEY RRs will actually be sets of KEY RRs with the same owner and class because SIGs actually sign such record sets.)

This information could be preserved as a set of detached DNS information blocks.

4. IANA Considerations

Allocation of meanings to retrieval time fields with a initial byte of between 0x01 and 0x1F requires an IETF consensus.

5. Security Considerations

The entirety of this document concerns a means to represent detached DNS information. Such detached resource records may be security relevant and/or secured information as described in [RFC 2535]. The detached format provides no overall security for sets of detached

information or for the association between retrieval time and information. This can be provided by wrapping the detached information format with some other form of signature. However, if the detached information is accompanied by SIG RRs, its validity period is indicated in those SIG RRs so the retrieval time might be of secondary importance.

References

[RFC 1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034, November 1987.

[RFC 1035] Mockapetris, P., " Domain Names - Implementation and Specifications", STD 13, RFC 1035, November 1987.

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

Author's Address

Donald E. Eastlake 3rd
IBM
65 Shindegan Hill Road, RR #1
Carmel, NY 10512

Phone: +1-914-276-2668(h)
+1-914-784-7913(w)
Fax: +1-914-784-3833(w)
EMail: dee3@us.ibm.com

Full Copyright Statement