Network Working Group D. Eastlake
Request for Comments: 2540 IBM
Category: Experimental March 1999

Обособленная информация DNS

Detached Domain Name System (DNS) Information

Статус документа

В этом документе описывается экспериментальный протокол, предложенный сообществу Internet. Документ не содержит каких-либо стандартов Internet. Документ служит приглашением к дискуссии в целях совершенствования протокола и может распространяться без ограничений.

Тезисы

Определен стандартный формат для представления обособленной (detached) информации DNS. Предполагается, что предложенный формат будет полезен при хранении информации, полученной от DNS, включая данные системы безопасности, в системах архивирования или системах, не подключенных к Internet.

Оглавление

1. Введение

Система доменных имен DNS (Domain Name System) представляет собой реплицируемую иерархическую распределенную базу данных [RFC 1034, 1035], которая может обеспечивать высокий уровень доступности сервиса. DNS Эта система служит основой для преобразования имен хостов Internet в адреса, автоматической маршрутизации почты SMTP и реализации других базовых функций Internet. Система DNS была расширена в соответствии с [RFC 2535] для поддержки хранения открытых ключей шифрования в DNS и обеспечения возможности аутентификации данных, полученных через DNS с помощью цифровых подписей (сертификатов).

Система DNS изначально не была предназначена для хранения информации за пределами активных зон и аутентичных master-файлов, которые являются частью подключенных DNS. Однако возникают ситуации, когда такое хранение становится полезным (в частности для архивирования данных системы безопасности).

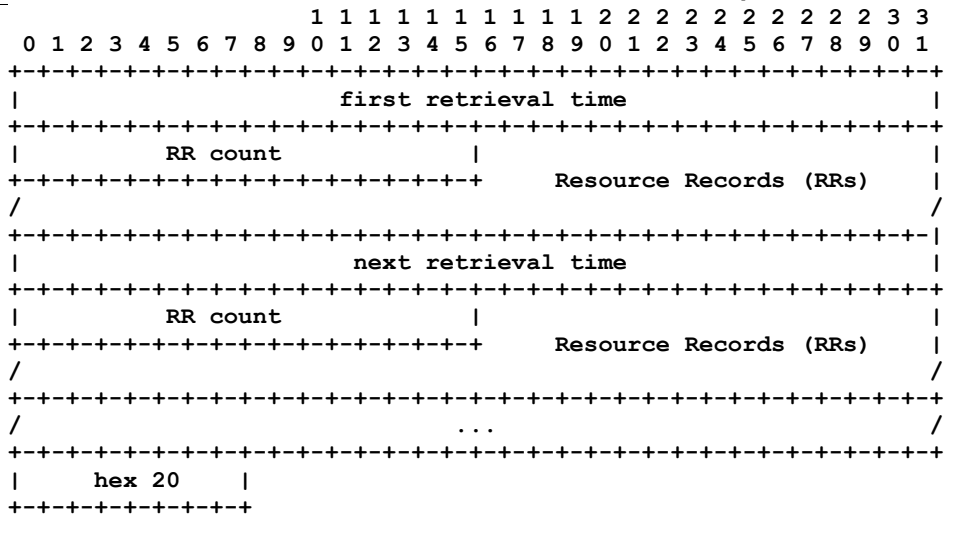
2. Формат общего назначения

Формат, используемый для обособленной информации DNS, похож на формат, применяемый в подключенных DNS. Основное различие состоит в том, что элементы подключенной системы DNS (если они не являются уполномоченными серверами для содержащей информацию зоны) должны уменьшать значение времени жизни (TTL) связанное с каждой записью RR (Resource Record) и отбрасывать записи (возможно с запросом свежей копии) с TTL=0. В противоположность этому обособленная информация может сохраняться в статическом (off-line) файле, где она не может обновляться. Эта информация может использоваться для аутентификации исторических данных или может быть получена с использованием отличных от DNS протоколов много позже того момента, когда она была получена от DNS. Следовательно, нет смысла уменьшать значения TTL для обособленных данных DNS и может потребоваться хранение информации уже после завершения срока ее жизни (поле TTL задается беззнаковым целым числом). Для сохранения информации как обособленных данных, она сопровождается временем получения данных от системы DNS.

Всякий раз при получении информации от DNS с ней должна быть связана временная метка момента получения данных. Эта метка сохраняется и не изменяется в последствии. Когда разница текущего времени и значения временной метки превышает значение TTL для любой обособленной записи RR, эта запись перестает быть корректной в нормальной схеме подключенных DNS. Такая запись может стать некорректной и в контексте некоторых обособленных операций. Если RR является SIG (signature – подпись), эта RR имеет срок действия (expiration time). Независимо от значения TTL, эта запись и любые подписанные с ее помощью RR не могут считаться аутентифицированными после завершения срока действия подписи.

2.1 Двоичный формат

Стандартный двоичный формат обособленной информации DNS показан на рисунке.



Retrieval time

Значение времени, отмеченное сразу же после получения информации от подключенной системы DNS. Временные метки задаются числом секунд, прошедших с 1 января 1970 г по Гринвичу (GMT) и сохраняются в форме беззнакового целого числа с сетевым порядком (big-endian) байтов. Отметим, что значение этого поля не может быть раньше момента предложения этого стандарта.

Следовательно, первый байт временной метки, рассматриваемой как 32-битовое целое число без знака, всегда должен быть больше шестнадцатеричного число 20. Завершение обособленной информации DNS указывается фиксированным полем, содержащим значение 0x20. Использование поля "retrieval time" с нулевым значением старшего байта говорит о том, что данное поле имеет размер 64 бита (на самом деле 56, поскольку первые 8 битов всегда имеют значение 0) вместо 32. 64-битовый формат требуется в тех случаях, когда значение временной метки превышает 0xFFFFFFFF (это произойдет в 2106 г.). Значения первого байта поля retrieval time в диапазоне от 0x01 до 0x1F зарезервированы (см. параграф 5). Временные метки в общем случае не выравниваются по 32-битовой границе, поскольку записи RR имеют переменную длину.

RR count

Беззнаковое целое число (сетевой порядок байтов), указывающее количество записей RR, полученных к моменту записи временной метки retrieval time.

Resource Records

Данные DNS в том же формате, который используется при передаче откликов DNS. В частности, допускается сжатие имен с помощью указателей с включением поля origin в начале того или иного раздела обособленной информации после поля RR count.

2.2. Текстовый формат

Текстовый формат обособленной информации DNS соответствует формату файлов зон [RFC 1035] за исключением запрета на использование управляющих полей $INCLUDE и добавления обязательной записи $DATE (если информация не является пустой). Ключевое слово $DATE сопровождается датой и временем, соответствующим моменту получения следующих далее данных от системы DNS (как описано для поля retrieval time в параграфе 2.10. Дата и время указываются в формате YYYYMMDDHHMMSS, где YYYY – значение года (которое может содержать более 4 цифр для использования формата после 9999 г.), первая пара MM означает 2-значный номер месяца (01-12), DD – число месяца (01-31), HH – количество часов в 24-часовом формате (00-23), вторая пара MM - количество минут (00-59) и SS – количество секунд (00-59). Таким образом, поле $DATE должно помещаться до первой записи RR и изменяться всякий раз при получении новой информации.

3. Пример использования

Документ может быть аутентифицирован ключом, полученным от DNS в записи KEY. Для дополнительной аутентификации документа желательно сохранить запись KEY RR для этого открытого ключа, запись SIG RR, подписывающую данный ключ KEY RR, запись KEY RR для ключа, используемого для аутентификации данной записи SIG и т. д. для всех записей SIG и KEY вплоть до доверенного ключа (возможно это будет ключ для DNS или центра аутентификации). В некоторых случаях запись KEY RR будет представлять собой набор KEY RR с совпадающим владельцем и классом, поскольку в реальности записи SIG подписывают такие наборы записей.

Информация может представляться как набор информационных блоков обособленных DNS.

4. Согласование с IANA

Выделение значений первого байта поля retrieval в диапазоне от 0x01 до 0x1F требует разрешения с IETF.

5. Вопросы безопасности

Весь документ посвящен представлению обособленной информации DNS. Такие обособленные записи о ресурсах могут иметь отношение к безопасности и содержать связанную с безопасностью информацию, как описано в [RFC 2535]. Обособленный формат сам по себе не обеспечивает защиты для обособленной информации или связи этих данных с моментом их получения. Для обеспечения защиты обособленной информации могут использоваться некоторые формы цифровых подписей. Однако, если обособленная информация сопровождается записями SIG RR, срок корректности обособленных данных указывается в SIG RR, поэтому важность времени получения обособленных данных снижается.

Литература

[RFC 1034] Mockapetris, P., "Domain Names - Concepts and Facilities", STD 13, RFC 1034[1], November 1987.

[RFC 1035] Mockapetris, P., " Domain Names - Implementation and Specifications", STD 13, RFC 1035[1], November 1987.

[1]Перевод этого документа доступен на сайте www.protocols.ru. *Прим. перев.*

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

Адрес автора

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

Перевод на русский язык

Николай Малых

nmalykh@gmail.com

Полное заявление авторских прав