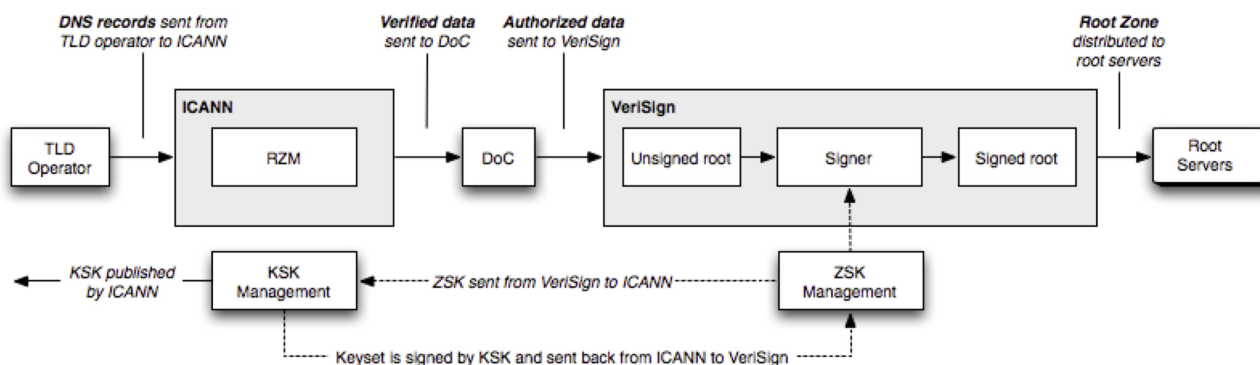


Все что вы хотели знать о подписании корневой зоны

Годы велись дискуссии о том, когда же будет подписана зона, кто будет контролировать ключи, как это отразится на системе DNS и Интернете в целом. Осенью прошлого года подразделение министерства торговли США, Национальная Администрация по Телекоммуникациям и Информации (NTIA), опубликовала возможные схемы подписания корневой зоны. Среди представленных сценариев были также предложение ICANN и предложение VeriSign. Спустя почти год публичных комментариев и, очевидно, внутренних дискуссий, ICANN, VeriSign и NTIA договорились о прагматичной схеме, при которой существующий процесс внесения изменений в зону остается прежним, а основные игроки получают дополнительные роли: ICANN контролирует т.н. Trust Anchor – ключ для подписания ключей (Key Signing Key, KSK), NTIA по-прежнему утверждает изменения, а VeriSign владеет ключом подписания зоны (Zone Signing Key, ZSK), который используется для генерирования подписанной корневой зоны, и осуществляет ее публикацию на скрытом мастер-сервере. Далее, зона публикуется операторами корневой зоны (RIPE NCC является одним из них, отвечая за корневой сервер k.root-servers.net). Надо отметить, что в соответствии с технологией DNSSEC, ключ KSK подписывает ключ(и) ZSK. Другими словами, контроль за подписанием зоны в конечном итоге остается за ICANN.



Распределение ролей и ответственности (RZM – управление корневой зоной, <http://www.ripe.net/ripe/meetings/ripe-59/presentations/abley-dnssec-root-zone.pdf>)

Когда политические страсти вокруг подписания корневой зоны постепенно улеглись, настало время взглянуть на технические аспекты этого изменения. А их немало. Помимо внутренней защищенной архитектуры хранения и использования ключей, защищенного взаимодействия между игроками, сама публикация подписанной зоны представляет серьезную задачу. Это, в первую очередь, связано с масштабом последствий, которые изменения в корневой зоне могут иметь для глобального сообщества пользователей Интернета.

Зри в корень

Корневая зона содержит информацию обо всех доменах самого верхнего уровня: национальные домены (например .ru), домены общего назначения (например .com) и спонсированные домены (например .museum). Эта информация указывает клиенту, на какие серверы DNS отправить последующий запрос для продолжения разрешения полного доменного имени. Другими словами, любой "свежий" (т.е. не сохраненный в кэше клиента) запрос начинается с обращения к корневому серверу. При этом самый первый запрос, который также называется "первоначальным" (priming), клиент осуществляет для получения текущего списка корневых серверов.

Корневая зона является критическим ресурсом Интернета. Отсутствие доступа к этой зоне для клиентов означает невозможность разрешения доменных имен, а для большинства пользователей – неработающий Интернет. Поэтому, хотя технология DNSSEC достаточно хорошо обкатана и даже уже внедрена в нескольких доменах верхнего уровня, осторожность в данном случае

совсем не помешает.

Чего бояться?

Начну с того, чего клиентам, которые не поддерживают технологию DNSSEC, бояться нечего. Для них подписание корневой зоны ситуацию совершенно не изменит. Это связано с тем, что протокол DNSSEC "включается" только по запросу клиента (например, корпоративного сервера DNS). Однако во многих современных версиях программного обеспечения поддержка DNSSEC установлена по умолчанию, о чем сами администраторы этих систем порой не догадываются.

Основную потенциальную опасность для клиентов представляет размер ответа, который значительно увеличивается с подписанием зоны – в некоторых случаях почти вдвое. Например, в ответ на запрос списка серверов, обслуживающих зону .RU, вместо 257 байт с внедрением DNSSEC клиент получит 440 (?) байт. Здесь следует рассмотреть несколько случаев:

- Клиент не может принять ответы, размер которых превышает 512 байт.

Согласно протоколу DNS клиент должен сообщить об этом серверу, который, в свою очередь, постарается уместить ответ в установленные 512 байт. При этом часть информативных данных может быть обрезана. В случае, если даже необходимая информация (т.н. authoritative section) не умещается, сервер сообщит об этом клиенту установкой т.н. бита "обрезания" (truncation bit). Обычной реакцией клиента является переключение с транспортного протокола UDP на TCP, на который данное ограничение не распространяется.

- Сетевая инфраструктура препятствует передаче DNS-ответов, размер которых превышает 512 байт, хотя клиент способен принять ответы большего размера.

Это может быть вызвано, например, конфигурацией маршрутизаторов или устройств безопасности, основанной на вышедшем из употребления старинного правила об ограничении в 512 байт для DNS (заметим, что 512 байт данных DNS соответствует несколько большему размеру пакета UDP). Также, это может быть последствием фрагментации пакетов (для передачи по "узким" каналам связи), когда промежуточные устройства не пропускают фрагменты ответа DNS. При этом в случае IPv6 фрагментация в сети вообще не возможна и слишком большие пакеты (скажем, превышающие "безопасный" размер в 1280 байт) скорее всего, будут просто отброшены промежуточным устройством.

В этих случаях ситуация получается немного хитрее. Клиент посылает запрос и не получает никакого ответа. Дальнейшие события зависят от конкретного программного обеспечения. Например, современные версии BIND осуществляют 3 попытки контакта с сервером, после чего установят ограничение ответа в 512 байт, то есть мы получаем первый случай. Некоторые другие DNS-резолверы будут продолжать попытки и так и не получат ответа. Для таких клиентов Интернет окажется сломанным, поскольку они не смогут даже получить ответ на первоначальный (priming) запрос.

Хорошей новостью является то, что, скорее всего для таких клиентов Интернет умер уже довольно давно, т.к. с некоторый пор размер ответа на первоначальный запрос превышает заветные 512 байт. Однако с подписанием зоны размеры ответов корневой зоны на некоторые запросы увеличиваются настолько значительно, что фрагментация пакетов, до этого времени являвшейся редким явлением в DNS, может играть существенную негативную роль.

Предварительное обследование

Было бы здорово, если бы пользователи до подписания зоны смогли бы проверить, грозит ли им одна из указанных ситуаций. Для этого мы в RIPE NCC установили специальную программу, разработанную в центре OARC, в непосредственной близости от всех глобальных узлов сервера K-root. Эта программа позволяет определить максимальный размер DNS ответа, который клиент

может рассчитывать получить от ближайшего anycast-узла K-root.

Если вы знакомы с утилитой dig, вам достаточно набрать:

```
dig txt test.rs.ripe.net +short
```

В результате ваш DNS-резолвер вступит в диалог тестером test.rs.ripe.net и в конце концов выдаст ответ, показывающий максимальный размер DNS-ответа.

Например:

```
rst.x477.test.rs.ripe.net.  
rst.x486.x477.test.rs.ripe.net.  
rst.x456.x486.x477.test.rs.ripe.net.  
"192.168.1.1 DNS reply size limit is at least 486 bytes"  
"192.168.1.1 lacks EDNS, defaults to 512"  
"192.168.1.1 summary bs=512,rs=486,edns=0,do=0"
```

Последние 3 строчки содержат нужную информацию. Из них мы узнаем, что наш порог как минимум 486 байт и наша инфраструктура не поддерживает DNSSEC. Информация к размышлению для администратора DNS.

Мы также работаем над созданием веб-приложения, позволяющего осуществить проверку локальной DNS-инфраструктуры без знания DNS и наличия специальных утилит. Это приложение сообщит вам о существующих или потенциальных проблемах с конфигурацией DNS в преддверии подписания корневой зоны. Даже если вы не имеете к администрированию DNS никакого отношения, эта информация может быть полезной для системного администратора DNS вашей сети. Мы опубликуем это приложение на сайте RIPE Labs (<http://labs.ripe.net>), так что заходите сюда время от времени.

А как же серверы?

Подписание корневой зоны будет иметь определенные последствия для серверов, обслуживающих ее - 13 серверов ббббб. Учитывая поведение некоторых клиентов, описанное выше, можно опасаться увеличения частоты запросов из-за многократных попыток получения ответа, и увеличение числа запросов, осуществляемых с помощью протокола TCP. Оба фактора увеличивают нагрузку на серверы, но не представляют большой проблемы, так как система корневых серверов способна поддерживать нагрузку в несколько раз превышающую текущую.

План

Итак, основные возможные последствия подписания корневой зоны известны, но масштаб явления - нет. Что если количество клиентов, неспособных переварить укрупненные и подписанные ответы значительно и большая часть пользователей не может работать в Интернете? Что если поведение клиентов настолько неадекватно, что нагрузка на систему корневых серверов возрастает настолько, что заметно сказывается на ее производительности? Что если

Все эти ситуации маловероятны, но что если...

Для более точного контроля изменений в работе корневого DNS и минимизации возможных негативных последствий, командой разработчиков ICANN и Verisign был предложен план постепенного внедрения подписанной зоны с возможностью возврата в прежнее, неподписанное состояние, если события начнут развиваться непредсказуемым образом. Этот план был представлен участникам совещания RIPE59 в октябре этого года в презентации Matt Larson

