

# Как подписали корень

## DURZ

Итак, 15 июля 2010 года пользователи впервые получили возможность криптографически удостовериться в подлинности ответов, получаемых от корневых серверов. Этому событию предшествовало шесть месяцев кропотливой подготовительной работы.

Полгода потребовались для обеспечения возможности постепенного внедрения этого значительного для глобального DNS изменения в систему. Как ни странно, основным изменением, связанным с внедрением DNSSEC в корневой зоне, является не собственно подписание зоны, а существенное увеличение размера ответа на запрос клиента. Большие DNS-ответы подстерегают различные опасности: это и фрагментация пакетов на пути их следования, и невозможность их сборки клиентом, и фильтрация пакетов, превышающих по длине исторические 512 байт, маршрутизаторами и устройствами безопасности. Другими словами, при значительном увеличении размера ответов возрастает риск, что клиент не сможет получить ответ на запрос к корневому серверу.

Поэтому DNSSEC в корневой зоне было решено внедрять постепенно: сначала на одном сервере, потом на следующем, и так далее, пока подписанная зона не будет публиковаться всеми 13 корневыми серверами (точнее, внедрение происходило по группам, всего 6 групп серверов). При этом велись наблюдения за возможным перераспределением нагрузки на серверы, потому что это означало бы наличие проблем: структурная "миграция" клиентов от сервера, на котором опубликована подписанная зона, к другим серверам скорее всего означает, что клиенты либо не могут получить ответа от этого сервера, либо выполнение запроса занимает существенно больше времени, чем для остальных серверов.

Также, для обеспечения возможности возвращения "на круги своя", то есть к неподписанной корневой зоне, в случае каких-либо проблем, было принято решение подписать зону таким образом, чтобы подписи невозможно было бы проверить. Такую зону назвали DURZ - Deliberately Unvalidatable Root Zone, или корневая зона, которая не может быть криптографически проверена. Я подробно писал об этом в статье "Все, что вы хотели знать о подписании корневой зоны".

Процесс "распространения" DURZ по КС начался в январе 2010 и завершился 5 мая, когда DURZ была опубликована на последнем сервере - "J" (j.root-servers.net). Без каких-либо заметных негативных последствий в функционировании Интернета. Можно было переходить к следующему этапу - подписанию зоны "правильным" ключом.

Однако перед этим было необходимо решить еще один вопрос, в свое время вызывавший оживленные дискуссии, - кто же "владеет" ключом к корневой зоне?

## Сообщество, представители, ключи

Для начала посмотрим, как были распределены роли в системе управления корневой зоной с внедрением DNSSEC. Об участниках этого процесса вы можете прочитать в статье "У корня DNS".

Те, кто немного знаком с DNSSEC, знают, что для каждой зоны используются два типа ключей: один, ZSK (Zone Signing Key) служит для подписи записей зоны, а другой, KSK (Key Signing Key), является более долгосрочным и используется для подписания ключей ZSK.

Так вот, ICANN отвечает за KSK, также называемый Trust Anchor, агентство NTIA Министерства Торговли США по-прежнему утверждает изменения в содержимом зоны, а VeriSign владеет ключом подписания зоны (Zone Signing Key, ZSK) и осуществляет ее публикацию на скрытом мастер-сервере. Далее зона публикуется в DNS корневыми серверами.

Политика ключей устанавливает продолжительность жизни ключа KSK в пять лет, а ключей ZSK - около 90 дней. Можно сказать, что владелец ключа KSK ежеквартально продлевает "лицензию" оператора зоны (в настоящее время - Verisign, выполняющий эту функцию по

контракту с министерством торговли США).

Для хранения ключей KSK были выбраны два датацентра с повышенной безопасностью, расположенных на значительном расстоянии друг от друга в США: один недалеко от столицы Вашингтон, а другой в Калифорнии, недалеко от офиса ICANN. Все операции с ключами (включая их генерацию и хранение) производятся с использованием специальных криптографических устройств (HSM, Hardware Security Module). Доступ к устройствам HSM предусматривает несколько степеней защиты. Была также разработана специальная процедура создания и хранения резервного ключа.

Однако хотя ICANN и является оператором KSK, "владение" ключом, а именно проведение таких операций как генерация ключа или подписание ключом, осуществляется с широким привлечением общественности через так называемых доверенных представителей сообщества (Trusted Community Representative, TCR). Такой подход был выбран ICANN для обеспечения высокого доверия к ключу корневой зоны, или Trust Anchor, со стороны пользователей Интернета, что является необходимым условием успешного внедрения DNSSEC. Он также явился ответом на существенную критику вокруг подписания корневой зоны, связанную с ролью правительства США в системе управления таким глобальным критическим ресурсом как корень DNS.

В результате выборного процесса, в котором широкому Интернет-сообществу было предложено номинировать своих представителей, была сформирована группа из 21 доверенных представителей - членов Интернет сообщества с высокой репутацией. Часть из них (14 человек, по 7 на каждый датацентр) отвечает за генерацию ключа KSK и подписание ключей ZSK на предстоящие 90 дней, другая группа из семи человек совместно владеет восстановительным ключом, используемым для шифрования резервных копий ключа KSK. Кстати, одним из таких представителей стал наш соотечественник - Дмитрий Бурков, член Совета RIPE NCC.

## Рождение правильного ключа

Процесс создания обычного крипто-ключа, например PGP, занимает не больше минуты случайных движений мышкой или нажатия произвольных клавиш клавиатуры для повышения энтропии. Создание ключа KSK корневой зоны заняло почти месяц и происходило в два этапа с участием доверенных представителей и значительной группы поддержки.

После первой "церемонии подписания", в процессе которой 7 доверенных представителей были сопровождены в защищенную зону, где они совместно активировали HSM. После этого был сгенерирован ключ и создана его резервная копия. Также были подписаны ключи ZSK на предстоящие 90 дней.

Вторая "церемония подписания" имела место на противоположном побережье США через 3 недели после первой, 12-13 июля 2010 года. Ритуал практически не отличался от первой, за исключением того, что уже существующий KSK был установлен во втором компьютерном центре и были подписаны ZSK на следующий квартал.



Рис. 1. Церемония подписания с доверенными представителями и наблюдателями. Западное побережье США, 12-13 июля 2010 г.

## Насколько защищен DNS

Итак, корневая зона наконец подписана. Хотя это событие имеет гораздо большую политическую, чем техническую значимость, решение этой задачи необходимо для будущего успешного внедрения DNSSEC.

Для того, что бы лучше понять значение внедрения этой технологии для безопасности DNS, рассмотрим, насколько уязвима система в целом. Различные уязвимые места системы показаны на рисунке 2, а методы защиты - на рисунке 3.

Напомню, что DNSSEC обеспечивает возможность проверки аутентичности и целостности данных DNS. Другими словами, с помощью DNSSEC пользователь имеет возможность убедиться, что полученные данные не были модифицированы в процессе публикации и передачи. DNSSEC можно сравнить с сургучной печатью, которая хотя и не защищает письмо от посторонних глаз, но позволяет получателю убедиться, что письмо не было вскрыто, прочитано или подменено.

Первый вопрос - насколько защищен собственно процесс подготовки данных, редактирования и создания зоны DNS. Ошибочные данные, умышленно или случайно оказавшиеся в зоне, например, неправильные адреса вэб-сайта или почтовых серверов, будут переданы пользователю в ответ на его запрос независимо от использования DNSSEC. В данном случае значение имеет уровень внутренней безопасности и защищенности процесса.

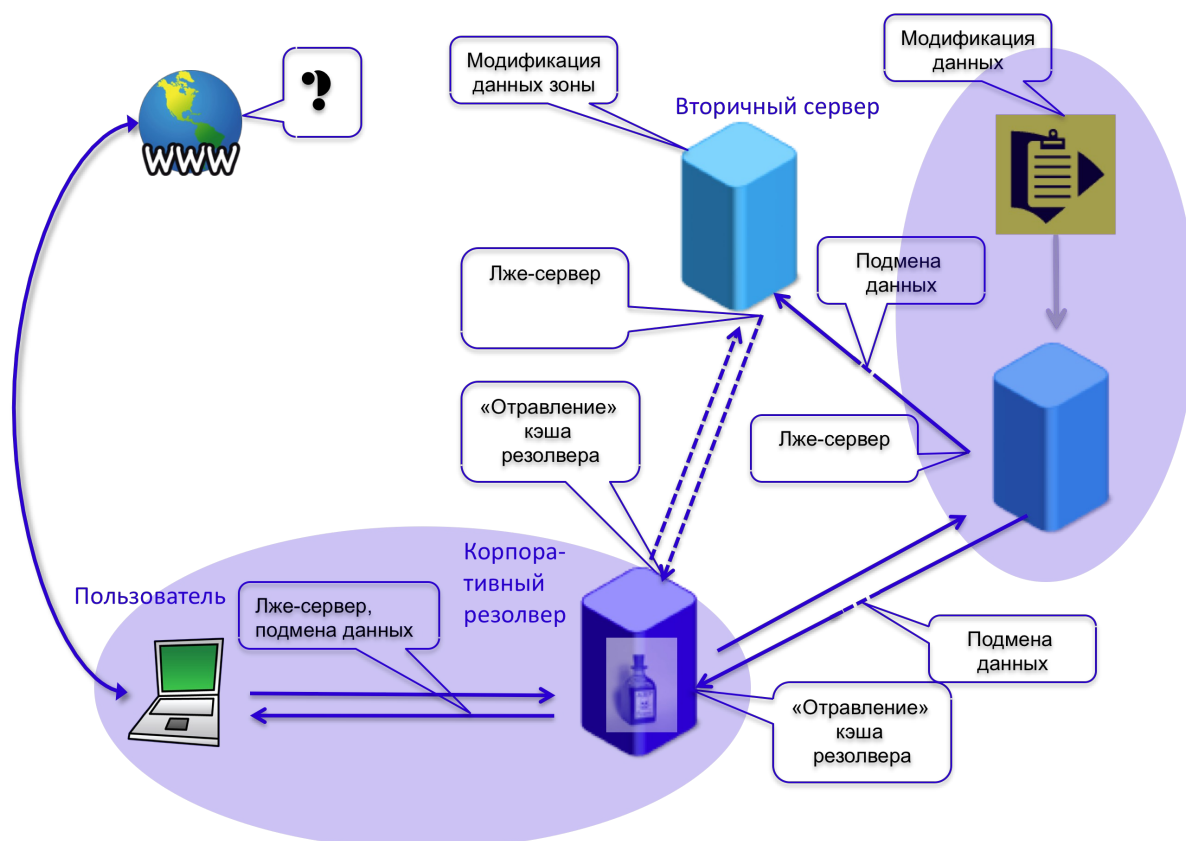


Рис. 2. Уязвимые места DNS

Данные также могут быть модифицированы при передаче от мастер-сервера ко вторичным DNS-серверам, обслуживающих зону. Сегодня, для проверки целостности передачи данных используется протокол TSIG (Transaction SIGnature).

Пожалуй, наибольшую опасность представляет попадание неправильных данных в кэш резолверов - промежуточных серверов DNS, обслуживающих пользователей конкретной сети или организации, - так называемое "отравление" кэша. Дело в том, что продолжительность жизни данных в кэше может быть достаточно значительной. В течение этого времени пользователи будут получать подложные ответы. Более того, внедрение подложных данных в кэш резолвера не представляет особого труда, как было продемонстрировано Дэном Каминским в 2008 году (с тех пор в программное обеспечение большинства стандартных резолверов были введены изменения, усложняющие проведение атаки). DNSSEC является единственным эффективным методом защиты, поскольку позволяет криптографически проверить аутентичность данных перед загрузкой их в кэш.

Наконец, ответы резолвера на запросы клиентов могут быть также модифицированы. DNSSEC здесь не поможет, если пользователь не производит валидацию ответов самостоятельно, а полагается на резолвер. Правда, канал между резолвером и пользователем, как правило, находится под административным контролем сервис провайдера или администратора корпоративной сети, и зачастую имеет высокую степень защиты, например с помощью VPN.

## От чего защищает DNSSEC

Итак DNSSEC позволяет закрыть уязвимые места DNS и, предполагая что DNSSEC внедрен повсеместно, существенно усилить защищенность системы разрешения имен в Интернете в целом. Однако эта система, несмотря на свою важность, является вспомогательной, для достижения конечной цели пользователя - посещение вэб-сайта, осуществление электронного платежа через Интернет или обмена электронной почтой.

Отсутствие защиты DNSSEC может привести к тому что имя сервера получит подложный адрес. Последствия могут быть разными - это и обращение в подложному вэб-сайту (например, сайту

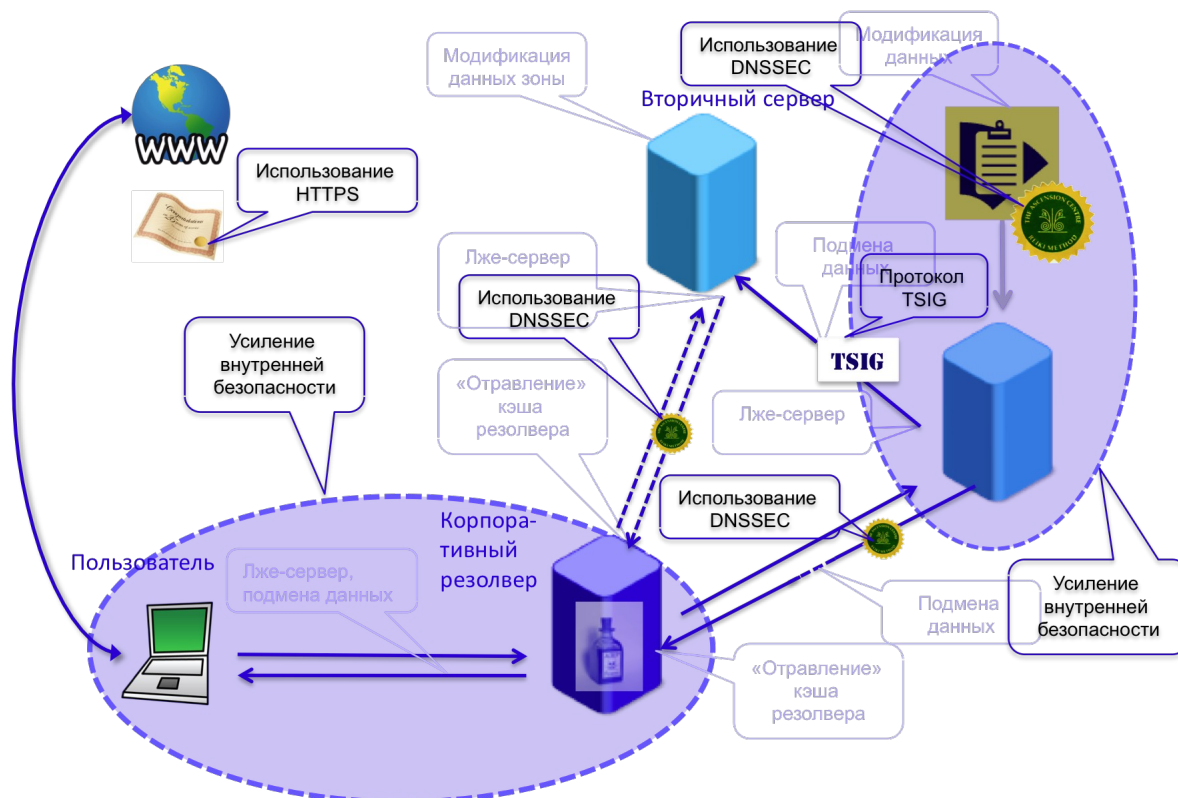


Рис. 3. Методы защиты DNS

электронного магазина), и перехват электронной почты (например, с забытым паролем вашего логина, или просто отказ в обслуживании).

Но DNSSEC не является панацеей. Даже если полученные адреса серверов являются правильными, обмен данными может быть перехвачен или перенаправлен с использованием уязвимых мест системы маршрутизации (см. мою статью "Безопасность системы маршрутизации Интернета"). Также, DNSSEC не обеспечивает шифрование данных, здесь необходима другая, довольно широко распространенная технология TLS (Transport Layer Security), использующая цифровые сертификаты X.509, на которой базируется протокол HTTPS. Наконец, DNSSEC не спасет от гомографии, когда имя сервера внешне очень похоже на другое имя, но на самом деле использует другие символы, например "1" и "l".

Но использование DNSSEC совместно с другими средствами защиты существенно усиливает их эффективность. Например, в противоположность сертификатам доменных имен, используемых в TLS/HTTPS, цепь доверия в DNSSEC следует цепочке делегирования доменов и, таким образом, основана на деловых отношениях, существующих при регистрации доменов. В то же время сертификаты TLS выдаются несколькими десятками удостоверяющих центров, для некоторых из которых процесс регистрации и связанным с ним удостоверением правомерности запроса ограничивается получением платежа за услугу.

## Корень подписан - что дальше?

Подписание корневой зоны - это значительное событие в истории Интернета. И в то же время ее эффект на безопасность DNS весьма скромн, особенно в краткосрочном плане.

Подписание корневой зоны означает, что DNSSEC это всерьез и надолго. В первую очередь - для администраторов доменов верхнего уровня. Теперь они имеют возможность замкнуть цепь доверия на корне, и одним аргументом меньше в пользу обоснования своего

бездействия. В начале сентября 2010 года корневая зона насчитывала 17 ссылок (записей DS) на подписанные домены верхнего уровня (включая ARPA, EDU, LK и NL). Всего на это же время существовало 27 доменов верхнего уровня, поддерживающих DNSSEC.

Однако для заметного эффекта необходимо нечто большее. Во-первых, цепочка доверия должна включать доменные имена, значимые для пользователей, например имена взб или почтовых серверов. Это означает, что зоны второго, третьего и т.д. уровня должны быть подписаны, а их ключи включены в родительские зоны.

Во-вторых, резолверы, обслуживающие запросы DNS пользователей и по-существу предоставляющие им услуги DNS в рамках сети или организации, должны работать в режиме DNSSEC. Это означает, что они должны выполнять дополнительную функцию построения цепи доверия и валидации ответов.

В-третьих, пользовательские приложения, должны понимать DNSSEC и иметь возможность различить между именем, прошедшим проверку DNSSEC (и соответственно более защищенным), и именем без защиты DNSSEC. Подобно тому, как пользователь сегодня определяет защищенность имени сервера технологией TLS по пиктограмме с замочком в окне браузера.

Процесс внедрения DNSSEC в этих областях займет какое-то время. Он вряд ли когда-либо будет завершен, но это не имеет существенного значения. Гораздо более важно, когда будет достигнута критическая масса, и использование DNSSEC будет являться нормальной добросовестной практикой, а не экзотикой передовых технологических компаний.

Будем надеяться, что подписание корневой зоны придаст этому процессу сильный импульс.

Андрей Робачевский, Технический директор RIPE NCC

*Мнения, представленные в статье, не обязательно отражают официальную позицию RIPE NCC*