DNSSEC: доверие по цепочке

Автор статьи: Александр Венедюхин, ведущий аналитик ТЦИ

Встроенные в «классический» сервис доменных имён механизмы защиты от подмены ответов привязаны к свойствам протокола DNS-обмена, а поэтому предотвращают только самые примитивные атаки. Например, эти механизмы не позволяют противодействовать активной подмене пакетов на уровне сетевого транспорта, а это означает, что всякий промежуточный узел может полностью заменить картину адресации, видимую через DNS. Разнообразие угроз в современной глобальной Сети достаточно велико для того, чтобы попробовать использовать некоторый универсальный инструмент безопасности, позволяющий защитить информацию об именах и адресах вне зависимости от низкоуровневых свойств DNS и сетевого транспорта. Такая надстройка доступна достаточно давно – она основана на электронной подписи и называется DNSSEC.

Подписанному – верить

Основной логической особенностью DNSSEC является то, что эта технология работает на другом, относительно протоколов DNS, уровне. Да, ключи и подписи DNSSEC публикуются так же, как и другие ресурсные записи DNS, но проверка подлинности полученных данных происходит уже за пределами доменной системы.

Это означает, что *авторизованные и удостоверенные* данные об адресации внутри той или иной зоны даже не обязательно получать через DNS. Главное, чтобы они сопровождались корректными DNSSEC-подписями, а поступить соответствующие записи могли по любому каналу, не только по доверенному. Это существенное преимущество, если смотреть с точки зрения приложений. Для приложения, умеющего проверять DNSSEC-подписи, выстраивая цепочку доверия от локальной копии корневого ключа, становится не так важно, является ли доверенным доступный источник DNS-записей, например, резолвер провайдера доступа. То же самое можно сказать и про любой промежуточный узел, который мог подменить информацию на пути от сервера к клиенту: DNSSEC позволяет обнаружить такую подмену.
В «классической» DNS тоже существуют защитные механизмы, основанные на сходных алгоритмах (это, прежде всего, TSIG), но они доступны только тем узлам, которые заранее договорились об общем секрете. Понятно, что такой вариант не годится для массового, открытого применения, когда к DNS-серверу может обратиться произвольный узел, поскольку этот узел не может заранее знать секретный ключ. Как говорится, DNSSEC позволяет «неопределённому кругу» программ-клиентов эффективно использовать хорошо известную схему с иерархией *открытых ключей*, в которой выстраиваются цепочки подписей, а нужные ключи можно безопасно получить по незащищённому каналу.
Итак, DNSSEC решает задачу обеспечения целостности данных: сторона, получившая данные из DNS, может проверить, что эти данные не были изменены на пути от авторитативного сервера, а также получена именно та информация, которая опубликована в доменной зоне её администратором. Администратором является тот, кто имеет доступ к соответствующему секретному ключу (ключам) и, таким образом, может генерировать подписи DNSSEC, удостоверяющие DNS-записи. В большинстве практических случаев – это администратор доменной зоны.

Алгоритмы

Рассмотрим работу DNSSEC на простом примере. Пусть клиенту необходимо определить IP-адрес, соответствующий имени test.ru. При этом зона test.ru является безопасной, то есть серверы имён, на которые она делегирована, поддерживают DNSSEC, также DNSSEC поддерживается и в вышестоящих зонах (ru и корневая зона). Для получения IP-адреса необходимо провести в DNS поиск A-записи (ресурсная запись, позволяющая публиковать адреса для имён узлов). Клиентский резолвер, поддерживающий DNSSEC, получит из DNS не только A-запись для test.ru, но ещё и ряд значений подписей, которые удостоверяют подлинность переданных значений. Подписи передаются в дополнительных DNS-записях, которые называются RRSIG. Для проверки подписей требуются открытые ключи. Ключи (кроме корневого ключа!) проверяющая сторона также получает из DNS. Наборы открытых ключей соответствуют доменным зонам. Так, в случае с test.ru, резолвер должен получить ключи для зоны test.ru, для зоны ru и для корневой зоны. Нужные ключи передаются в записях DNSKEY (в DNSSEC два типа ключей – KSK:
“ключ для подписи ключей”; ZSK: “ключ для подписи зоны”. Далее, для упрощения изложения, эти типы не различаются, за исключением корневого KSK). Записи со значениями ключей тоже подписываются. Это очень важный момент: необходим механизм, позволяющий проверить подлинность самих значений ключей.

Проверка подлинности требует переноса доверия по всей иерархической цепочке зон. Это означает, что в зоне ru должны находиться данные, позволяющие проверить подлинность ключей, полученных для зоны test.ru. Технически, зона ru в нашем примере *делегирует права администрирования* зоны test.ru, а такое делегирование в DNSSEC должно сопровождаться передачей доверия. Кстати, если бы делегирования в данном конкретном случае не было, то ответ на запрос A-записи для test.ru, вместе со всеми подписями, прислали бы серверы зоны ru (конечно, только в случае, если такое имя присутствует в зоне). Такая же схема работает для имён вида www.test.ru, если они находятся непосредственно в зоне test.ru. Делегирование в DNSSEC имеет столь же важное значение, как и в «классической» DNS, но устроено несколько иначе. Напомним, что в DNS делегирование реализуется отправкой в ответ на запрос резолвера (клиента) списка имён авторитативных серверов, которые соответствуют заданной DNS-зоне. В случае с DNSSEC – делегирующий ответ DNS сохраняется и устроен так же. При этом список серверов в делегирующем ответе не

удостоверяется подписью, так как выстраивание доверия в DNSSEC происходит через криптографические ключи. Каждая обособленная доменная зона имеет собственный набор ключей подписи DNSSEC, потому что различные администраторы *не обязаны* использовать одни и те же ключи. Так как подписи внутри зон тоже обособлены, возникает задача проверки того, что подписи, которые видит клиент, соответствуют ключам администратора доменной зоны, а не были заменены на пути к клиенту.
Действительно, предположим, что злоумышленник перехватывает все DNS-запросы клиента и может отправлять произвольные ответы. В таком случае, злоумышленник мог бы сгенерировать собственные наборы ключей для test.ru, вычислить подписи от этих ключей и передать атакуемому клиенту требуемый набор данных вместе с *корректными* подписями. Это, впрочем, хорошо известная проблема, свойственная практически всем массовым схемам электронной подписи. Логика построения DNS требует, чтобы ключи, соответствующие конкретной доменной зоне, публиковались в ней же. Поэтому для противодействия только что описанной атаке в DNSSEC используется механизм безопасного делегирования: в делегирующей зоне размещается *отпечаток* доверенного открытого ключа делегируемой зоны; для этого служит специальная DS-запись. Значение отпечатка ключа подписывается при помощи ключей делегирующей зоны - это позволяет убедиться, что ключ не был подменён (отпечаток вычисляется с помощью криптографической хеш-функции, поэтому подменить ключ так, чтобы совпали отпечатки, не выйдет).
Итак, в делегирующей зоне размещается подпись, удостоверяющая отпечаток ключа делегируемой зоны. Цепочка доверия выстраивается следующим образом: резолвер, получив очередной ключ из той или иной зоны, вычисляет его отпечаток и сверяет значение с отпечатком, полученным из зоны уровнем выше, который удостоверен подписью. Процесс продолжается до тех пор, пока не дойдёт до корневого ключа (KSK). Вернёмся к примеру с test.ru и A-записью. Резолвер получает набор ключей, соответствующих зоне test.ru, и проверяет, что хотя бы один из них соответствует DS-записи для test.ru, которая размещена в зоне ru (то есть в зоне уровнем выше). Для зоны ru выполняются аналогичные шаги, но DS-запись уже запрашивается из корня DNS. Наличие DS-записей позволяет выстроить ключи в иерархическую цепочку и проверить подписи. Началом в этой цепочке является корневой ключ DNS, при помощи которого удостоверяется набор ключей корневой зоны. Корневой открытый ключ должен быть получен по доверенному каналу,

отличному от DNS. Обычно, этот ключ встроен в дистрибутив клиентского приложения, которое выполняет валидацию DNSSEC.

Отдельный интерес представляет такой аспект, как доверенное подтверждение отсутствия записей. Предположим, что злоумышленник хочет подделать ответы о зоне test.ru, перехватывая трафик. Тогда он мог бы имитировать отсутствие поддержки DNSSEC для зоны test.ru, подменяя ответы серверов имён, относящиеся к DNSSEC, а именно ответ с DS-записью (либо для зоны ru, либо для test.ru). Если зона не поддерживает DNSSEC, то подменять относящиеся к ней ответы не составляет особой проблемы: никаких подписей подделывать не придётся. Другими словами, возможность такой атаки нивелирует всю пользу от DNSSEC: злоумышленнику достаточно имитировать отсутствие DNSSEC.

Конечно, в DNSSEC встроены механизмы защиты от данной атаки: то, что некоторая запись отсутствует в зоне, тоже подтверждается при помощи электронной подписи. Для этого используются специальные схемы, позволяющие подписывать «интервалы» между возможными именами и типами записей, подтверждая, что эти интервалы действительно «пустые». В частности, чтобы валидирующий DNSSEC резолвер признал зону «небезопасной» (то есть, без поддержки DNSSEC), потребуются подтверждённые подписью записи из зоны уровнем выше.

Итак, DNSSEC позволяет публиковать защищённые от изменения данные в DNS. Клиент, поддерживающий DNSSEC, может удостовериться в подлинности информации об адресации, вне зависимости от того, по какому каналу эта информация получена.

Управление ключами

Современная версия DNSSEC позволяет использовать различные алгоритмы электронной подписи, среди которых и ECDSA (на эллиптических кривых), и RSA. Корневой ключ глобальной DNS всё ещё использует RSA, несмотря на то, что данная криптосистема сейчас считается устаревшей, а более подходящим вариантом была бы криптосистема ECDSA.

ECDSA основана на криптографических алгоритмах, использующих эллиптические кривые. Это позволяет сократить длину записи ключей, что уменьшает размеры пакетов данных, необходимых для передачи DNS-ответов. Кроме того, в ряде случаев ECDSA предоставляет пути для дополнительной оптимизации операций на стороне сервера (что опять же связано с меньшей, по сравнению с RSA, длиной ключей в криптосистемах на эллиптических кривых). Другой вариант электронной подписи, использующей эллиптические кривые, это российские алгоритмы, известные под собирательным названием «ГОСТ-подпись» (стандарты семейства ГОСТ 34.10).
«ГОСТ-подпись» для DNSSEC предлагалась даже раньше, чем ECDSA, поскольку некоторое время являлась едва ли не единственной криптосистемой на эллиптических кривых в статусе государственного стандарта, с минимумом возможных проблем в области «патентной защиты». Дело в том, что и сама криптосистема ECDSA, и реализации ряда криптографических операций потенциально попадали под действие многочисленных патентов компании Certicom (до 2014-2018 гг.; сейчас период защиты самых «ограничительных» патентов закончился). А наличие проблем, вызванных защитой исключительных прав на используемые методы реализации криптографических операций, конечно, является заметным препятствием на пути внедрения открытых спецификаций.

Таким образом, «ГОСТ-подпись» получила поддержку в DNSSEC достаточно давно. Однако за время, прошедшее с момента внедрения, изменился соответствующий российский стандарт. Старый вариант подписи, ГОСТ Р 34.10-2001, больше не рекомендован для применения. На смену этому стандарту пришёл новый — ГОСТ Р 34.10-2012, а его поддержка требует обновления RFC. Со стороны Технического центра Интернет подготовку новых спецификаций в рамках IETF ведёт Дмитрий Белявский. Соответствующий черновик (draft) RFC, разработанный российскими специалистами, сейчас находится в процессе обсуждения рабочими группами IETF.
Необходимо отметить, что DNSSEC позволяет использовать несколько различных криптосистем для защиты одной и той же доменной зоны. Это означает, что российская ГОСТ-криптография может использоваться как отдельно, так и вместе с ECDSA или RSA.

Корневая зона глобальной DNS была подписана DNSSEC в 2010 году. Глобальными корневыми ключами DNSSEC управляет IANA (или «организация, осуществляющая IANA-функцию в Интернете»). Выбор исполнителя этой роли вполне логичен, поскольку IANA является техническим администратором корневой зоны DNS. Функции *оператора* выполняет компания Verisign, которая по заданию IANA и ICANN осуществляет периодическую генерацию подписей в корневой зоне DNS. Verisign использует ключи подписи зоны (ZSK), которые, в свою очередь, должны быть подписаны корневым ключом подписи ключей (корневым KSK – это «самый главный» ключ, который находится вне DNS). Согласно распорядку, копии корневого KSK хранятся с высокой степенью защиты, а доступ к нему строго регламентирован. Вообще, такой доступ необходим всякий раз, когда производится замена корневых ZSK.
Изначально предполагалось, что новые ZSK подписываются в рамках особой очной церемонии, проводимой прибывающими в защищённое хранилище из разных концов мира доверенными лицами, в число которых входят криптоофицеры, являющиеся держателями частей секретных ключей доступа, а также наблюдатели. Такой порядок помогает исключить возможность «несанкционированного использования» ключей, а также создаёт дополнительное доверие к системе в целом.

Однако уже в 2020 году, следуя общемировой ситуации, от очных церемоний решили временно отказаться, сгенерировав на одной из них сразу несколько наборов ZSK и создав, таким образом, запас на будущее. В дальнейшем, вместо очередной церемонии, сгенерированные ранее ключи просто передавались в Verisign согласно графику ротации ZSK. Возможно, к очным церемониям вернутся позже, хоть практика и поставила под сомнение их реальную значимость и необходимость.

Иерархию ключей DNSSEC можно сравнить с иерархией, используемой в TLS-сертификатах веб-браузерами. Основное отличие состоит в том, что DNSSEC сейчас использует единый корень, единый корневой ключ, логически совпадающий с единым корнем самой системы доменных имён. В случае TLS-сертификатов, корней, встроенных в браузеры, достаточно много: каждому из десятков хорошо известных удостоверяющих центров соответствует как минимум один корневой сертификат и ключ. TLS-сертификаты также связаны с доменными именами, поскольку

предназначение сертификата состоит в удостоверении соответствия некоторого ключа сервера некоторому сетевому имени (реже – IP-адресу). Может показаться, что TLS-сертификаты и протокол TLS реализуют такой же механизм защиты, как и DNSSEC.

Действительно, если клиент (веб-браузер) соединяется с веб-узлом, IP-адрес которого был подменён на уровне DNS, то у клиента остаётся возможность проверить подлинность TLS-сертификата сервера и соответствие имён. Так как TLS-сертификат от доверенного УЦ выпускается после проверки права управления доменной зоной (как минимум), то он удостоверяет подлинность узла. Это так, но ситуация радикально отличается от области применения DNSSEC. Во-первых, DNSSEC касается и всех других случаев, в которых используется DNS, а не только веба и веб-браузеров. Во-вторых, даже в случае веб-узла и IP-адреса из A-записи, DNSSEC позволяет обнаружить подмену (и, следовательно, атаку) раньше, чем TLS. Это означает, что практическая поверхность атаки существенно уменьшается, ведь клиент, выявив подмену, *даже не будет соединяться с узлом злоумышленника*. Это весьма важно. Дело в том, что, добившись попытки соединения, злоумышленник может использовать множество других методов для проведения успешной атаки. Это могут быть и нетехнические методы социальной инженерии: например, пользователям корпоративной системы, атакуемым в рамках «целевой атаки» типа spear phishing, рассылаются письма от «службы технической поддержки», сообщающие о якобы проводящейся «замене TLS-сертификата» на сайте и рекомендующие для открытия страницы корпоративного портала «согласиться с предупреждением браузера».
Более того, злоумышленник может тем или иным образом получить валидный сертификат для атакуемого имени. Конечно, в DNSSEC тоже возможна утечка секретных ключей, либо замена их при помощи перехвата административного управления доменной зоной. Но это не отменяет того, что подмена и TLS, и DNSSEC представляет более сложную задачу. Заметьте, что если злоумышленник получил управление DNS с правами, достаточными для замены ключей DNSSEC, то, скорее всего, он сможет получить и валидный TLS-сертификат для того же доменного имени (это так потому, что механизмы проверки права управления используют DNS). А вот обратная ситуация – наличие секретных ключей от TLS-сертификата веб-сервера – подменить записи DNSSEC не позволяет.

Другими технологиями, которые часто сравнивают с DNSSEC, являются DNS-over-TLS (DoT) и DNS-over-HTTPS (DoH) (про них рассказано в предыдущей статье). И DoT, и DoH прежде всего направлены на сокрытие содержания DNS-запросов и аутентификацию узлов. Эти технологии никак не касаются, собственно, DNS-записей. DNSSEC, напротив, не только основана на публикации DNS-записей, но и защищает сами данные, а не каналы доступа к ним. DoH, а в особенности DoT, являются хорошим дополнением к DNSSEC, но, например, не позволяют разместить в DNS какую-то дополнительную информацию доверенным способом. Между тем, именно такая особенность DNSSEC существенно расширяет возможности DNS.

Перспективы

DNSSEC снабжает DNS эффективным механизмом проверки подлинности, распространяющимся на все записи. Это означает, что можно «доверенным способом» опубликовать данные, используемые различными приложениями. Это могут быть и отпечатки криптографических ключей, используемых в других протоколах, и описание политик выпуска TLS-сертификатов для данной зоны, и так далее. Конечно, соответствующие записи (SSHFP, TLSA, CAA и др.) могут быть размещены в DNS и без разворачивания DNSSEC, однако последняя позволяет исключить подмену содержащихся в этих записях идентификаторов и параметров.

К сожалению, поддержка DNSSEC пока не получила должного распространения. Так, по состоянию на июнь 2021 года, в зоне ru DS-записи размещены только для примерно 5,5 тыс. доменных зон, что составляет лишь около 0,1%. Такое положение в основном связано с тем, что внедрение DNSSEC требует модернизации и самих авторитативных серверов имён, и инструментов управления, а выполнить такую модернизацию готовы немногие.