DNSSEC: Защита DNS

Офис технического директора ICANN

Давид Конрад (David Conrad)
OCTO-006v3
июль 2020

ICANN

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	**3**
ЧТО ТАКОЕ DNSSEC?	**3**
КАК РАБОТАЕТ DNSSEC?	**3**
КАКИЕ ВЫГОДЫ НЕСЕТ РАЗВЕРТЫВАНИЕ DNSSEC?	**4**
КАК ПРИВЕСТИ DNSSEC В ДЕЙСТВИЕ?	**4**
КАКИЕ РАСХОДЫ СВЯЗАНЫ С DNSSEC?	**5**
ЧТО ПРОИЗОЙДЕТ, ЕСЛИ НЕ РАЗВЕРТЫВАТЬ DNSSEC?	**5**
НЕМНОГО ИСТОРИИ DNSSEC	**6**
РОЛЬ ICANN В DNSSEC	**7**
ПОДРОБНОСТИ	**7**

Этот документ входит в состав серии документов OCTO. См. страницу публикаций OCTO - здесь приведен список документов по порядку. Вопросы или предложения по любому из этих документов отправляйте на адрес octo@icann.org.

Эта редакция содержит обновление от многих пользователей, которые читают OCTO-006v2. ICANN высоко ценит присланные нам отзывы.

Введение

Расширения безопасности системы доменных имен (DNSSEC) помогают обеспечить безопасность передачи данных в интернете.

Система доменных имен (*DNS*) ежедневно используется всеми, кто подключается к интернету, и почти всеми устройствами в интернете. Одна из многих функций DNS — используя автоматизированный процесс, называемый *поиском* или *разрешением*, сопоставлять легко запоминающиеся имена (например, example.com) с уникальными номерами (*IP-адресами*) (например, 192.0.2.189 или 2001:DB8:107A:61F7). Эти IP-адреса затем используются устройствами для идентификации и связи друг с другом. Таким образом, DNS часто сравнивают с телефонным справочником или списком контактов, преобразующим имена в числа.

Что такое DNSSEC?

При создании DNS в начале 1980-х годов безопасность не находилась в центре внимания разработчиков. Из-за конструктивных особенностей, которые были оправданы в то время, злоумышленникам изредка удавалось отправить при поиске доменных имен свои ответы на поисковые запросы вместо ответов владельца домена. Например, вместо того, чтобы перейти на веб-сайт, который вы запрашивали в своем браузере, злоумышленник может скомпрометировать DNS-сообщения, чтобы перенаправить вас на веб-сайт, который выглядит как веб-сайт, на который вы хотели перейти, но который вместо этого контролируется злоумышленником. В 1990-х годах техническое сообщество DNS нашло окончательное решение этой проблемы, которое называется расширениями безопасности DNS, или *DNSSEC*.

Как работает DNSSEC?

Владелец домена - это лицо или организация, которые контролируют информацию, относящуюся к доменному имени, то есть сопоставление имени с адресом и другие данные. DNSSEC позволяет владельцам доменов добавить цифровую подпись к данным, которые они размещают в DNS. Благодаря этому клиентские приложения (например, браузер) могут убедиться, что ответы DNS, полученные в ответ на поисковые запросы, не были изменены после того, как они были подписаны.

В 2010 году ICANN обеспечила возможность использования подписи DNSSEC на самом верхнем уровне DNS, который называется корневым, что существенно облегчает глобальное развертывание DNSSEC. Однако даже десять лет спустя темпы внедрения DNSSEC по-прежнему остаются низкими.

Какие выгоды несет развертывание DNSSEC?

- **DNSSEC защищает интернет**: Поскольку DNS важна для работы интернета, защита предоставляемых DNS данных имеет решающее значение. По аналогии, DNS можно рассматривать как дорожные указатели в интернете, позволяющие проложить маршрут до правильного контента или услуги. Как и в случае с дорожными знаками на реальных дорогах, если злоумышленники изменят указатель, поток транспорта может быть направлен по неверному маршруту, скажем, в опасный район города.

- **DNSSEC защищает конечных пользователей**: DNSSEC может гарантировать, что полученные конечными пользователями данные о доменном имени являются именно теми данными, которые владелец домена собирался передать конечному пользователю. DNSSEC помогает обеспечить подлинность сайта, с которым осуществляется обмен данными, при попытке конечного пользователя или устройства получить контент или услугу, на которые указывает доменное имя.

- **DNSSEC защищает компании, организации и правительства**: DNSSEC снижает вероятность того, что конечные пользователи, желающие воспользоваться услугами или просмотреть контент, будут перенаправлены на сайт, где они могут быть обмануты злоумышленником. Интернет-провайдеры (ISP) могут повысить ценность услуг, которые они предоставляют своим клиентам, включив проверку DNSSEC на своих резолверах. Организации, которые подписывают свои доменные имена с DNSSEC, снижают риск того, что люди, которые ищут их в интернете, будут направлены по ложному адресу.

- **DNSSEC способствует инновациям**: DNSSEC предоставляет средства проверки и защиты данных DNS, что позволяет доверять этим данным. Это, в свою очередь, позволяет использовать глобальную DNS для создания защищенной базы данных имя/значение (например, вы отправляете имя, а DNS возвращает значения, ассоциированные с этим именем), которая распространена по всему миру и доступна любому интернет-пользователю. В результате эта защищенная база данных дает возможность внедрения инноваций и новых технологий, услуг и оборудования. Например, одна из таких технологий, DNS-аутентификация именованных объектов (DANE), создает новый способ защиты каналов связи в интернете. DANE использует данные DNS, защищенные DNSSEC, и устраняет некоторые уязвимости в текущем подходе к созданию безопасных подключений в интернете. Это повышает безопасность интернет-коммерции и обмена данными.

Как привести DNSSEC в действие?

Вообще говоря, у DNS две стороны: публикация, которая выполняется владельцами доменов или их представителями, и поиск (также известный как разрешение), который обычно выполняется сетевыми операторами, такими как интернет-провайдеры. Чтобы извлечь пользу из DNSSEC, их должны использовать обе стороны.

- **Владельцы доменов:** Лица, ответственные за публикацию данных DNS, должны обеспечить подписание своих данных DNS с помощью DNSSEC. Исторически этот процесс оставался сложным и был подвержен ошибкам. Тем не менее, сегодня в состав большинства современных пакетов программного обеспечения DNS и систем регистрации входят инструменты, которые автоматизируют подписание публикуемых владельцами доменов данных с помощью DNSSEC. В результате владельцам доменов или их представителям просто необходимо включить DNSSEC-подпись на своих DNS-серверах (или у своих регистраторов) и передать регистратору немного информации, которая называется *DS-записью*, чтобы только что подписанные данные вызывали доверие.

- **Сетевые операторы:** Что касается поиска, дело обстоит еще проще: сетевым операторам нужно всего лишь включить проверку DNSSEC на резолверах, которые обрабатывают DNS-запросы для пользователей. Программное обеспечение резолверов все чаще включает проверку DNSSEC по умолчанию.

- **Конечные пользователи интернета:** Обычно конечным пользователям не нужно ничего делать, кроме как подталкивать своих сетевых операторов к включению проверки DNSSEC и добавлению цифровой подписи к используемым ими доменным именам.

Какие расходы связаны с DNSSEC?

DNS-серверы должны поддерживать DNSSEC как на стороне публикации, так и на стороне поиска. Поэтому организациям, возможно, придется обновить свои пакеты программного обеспечения DNS (это рекомендуется делать независимо от того, развернуты ли DNSSEC).

- Что касается публикации, владельцам доменов или их представителям тоже, возможно, придется изменить свои процессы, чтобы разрешить отправку DS-записей регистратору. Стоимость таких модификаций может оказаться значительной, однако это будет однократное изменение и единовременные расходы.

- С другой стороны, если предположить, что программное обеспечение DNS-сервера достаточно современное, затраты должны быть незначительными, поскольку все, что может потребоваться, — это однократное изменение конфигурациидля обеспечения валидации DNSSEC.

Что произойдет, если не развертывать DNSSEC?

- **Пользователи могут быть уязвимы к атакам:** Если организация принимает решение не развертывать или не включать DNSSEC, ее пользователи уязвимы к определенному типу атак, который называется «отравление кэша». Когда конечный пользователь выполняет поиск, злоумышленники могут беспрепятственно вставить свои ответы на DNS-запросы пользователя,

пытающегося установить связь, и перенаправить его на контролируемые злоумышленниками устройства. Затем злоумышленники могут имитировать веб-сайты или другие службы, похищать имена пользователей и пароли и т. д. Неправильные ответы также будут храниться на сервере, выполняющем поиск, в течение некоторого периода времени, что приведет к продолжению перенаправления до истечения срока действия или удаления ответов. Хотя подобные виды атак редки, поскольку для противодействия им уже в течение некоторого времени доступны DNSSEC, пострадавшим от наличия этой уязвимости организациям, возможно, придется долго объяснять своим пользователям, почему не были развернуты DNSSEC. По мере успешного предотвращения других видов атак злоумышленники скорее всего будут использовать в своих интересах сайты, где не развернуты DNSSEC, так как атаки через DNS получают все более широкое распространение.

- **Может замедлиться внедрение инноваций:** Отказ от развертывания DNSSEC препятствует инновациям и замедляет развертывание новых технологий, использующих DNS как базу данных, которой доверяют во всем мире. Некоторые из этих технологий обещают улучшить механизмы надежного подключения к интернет-сервисам, таким как электронная почта или всемирная паутина.

Хотя уязвимости, которые можно устранить с помощью DNSSEC, существуют с момента создания DNS, следует ожидать множества масштабных атак, использующих эти уязвимости. Из-за этого некоторые могут решить, что затраты на развертывание DNSSEC перевешивают преимущества, предоставляемые DNSSEC. Однако стоит отметить, что затраты и риски внедрения DNSSEC значительно уменьшились. На самом деле, польза от DNSSEC растет по мере того, как их используют все больше сетей.

Можно взглянуть на вопрос развертывания DNSSEC еще с одной стороны: «Если усилия на размещение данных в DNS оправданы, разве не стоит приложить усилия для защиты этих данных от фальсификации?»

Немного истории DNSSEC

В 1983 году Пол Мокапетрис из Института информационных наук Университета Южной Калифорнии опубликовал серию статей, в которых была представлена концепция системы доменных имен. В своей первоначальной форме в 1980-х годах DNS не имела встроенной защиты, конфиденциальности или аутентификации; не было никакого механизма, чтобы гарантировать, что полученный ответ был законным и фактически соответствовал заданному вопросу.

Примерно в 1990 году Стив Белловин из AT&T Bell Laboratories написал статью, в которой описывалось, как злоумышленники могут использовать конкретное проектное решение в DNS для взлома систем. В своей статье Белловин рекомендовал использовать криптографическую аутентификацию для улучшения защиты DNS. После публикации статьи Белловина начался формальный процесс превращения его предложения в стандарт протокола Инженерной проектной группы интернета (IETF) под названием «Улучшения безопасности DNS» (*DNSSEC)*.

Программное обеспечение DNS, внедряющее DNSSEC, было первоначально разработано в конце 1990-х годов, а первые реализации DNSSEC начались примерно в 2000 году, в том числе на популярном ccTLD .SE (национальный домен Швеции). Однако эти ранние развертывания выявили многочисленные технические проблемы для широкомасштабной работы DNSSEC в производстве, поэтому IETF продолжила работу по улучшению протокола в течение следующих восьми лет.

С точки зрения развертывания ничего особенного не происходило до 2008 года, когда исследователь безопасности по имени Дэн Камински обнаружил серьезный недостаток в самом протоколе DNS, который позволял злоумышленникам запускать атаки типа «отравление кэша» на стороне поиска DNS. Этот вывод привел к новым попыткам технического сообщества DNS расширить развертывание DNSSEC и, в частности, получить подписанный корень DNS.

В июле 2010 года ICANN впервые подписала корневую зону, предоставив глобальный якорь доверия для всей проверки DNSSEC. В октябре 2018 года ключ подписи ключей корневой зоны был впервые успешно обновлен, что стало важной вехой для DNSSEC.

Серия международных кампаний по захвату DNS в 2018 и 2019 годах привела к появлению первой в мире Директивы по чрезвычайным ситуациям Агентства США по кибербезопасности и безопасности инфраструктуры (US-CERT) и подтолкнула ICANN к повторному призыву ко всем заинтересованным сторонам DNS полностью развернуть DNSSEC.

Роль ICANN в DNSSEC

В рамках своей миссии по продвижению более стабильной, безопасной и отказоустойчивой экосистемы DNS ICANN уже давно является ведущим сторонником развертывания DNSSEC. Официальные операционные соглашения ICANN с регистратурами и регистраторами требуют поддержки DNSSEC. Корпорация ICANN регулярно взаимодействует с заинтересованными сторонами DNS по всему миру, чтобы помочь им понять важность DNSSEC и обучить инженеров тому, как развертывать и эксплуатировать DNSSEC в своих сетях. Помимо повышения осведомленности и развития потенциала, технологи ICANN работают с сообществом IETF над усовершенствованиями DNSSEC.

В операционном плане ICANN продолжает играть критически важную роль. ICANN отвечает за создание, хранение и периодическое обновление ключа подписи корневого ключа – криптографического ключа, которому доверяют все валидирующие резолверы в Интернете, и который используется в процессе подписи корня глобальной DNS.

Подробности

Есть множество ресурсов и технических групп, связанных с DNSSEC и его развертыванием. Вот всего лишь несколько примеров:

- DNSSEC и вся остальная деятельность, имеющая отношение к протоколу DNS, обсуждаются в IETF, в частности в рабочей группе по вопросам функционирования DNS (DNSOP).

- На открытых конференциях ICANN три раза в год проводятся семинары по DNSSEC. Эти семинары, организованные Обществом интернета, позволяют получить полезную оперативную и аналитическую информацию, а также рекомендации по развертыванию DNSSEC. На соответствующем сайте, который поддерживается Обществом интернета, доступен архив этих мероприятий.

- Для предоставления более подробной информации ICANN опубликовала общее описание DNSSEC и обоснование их важности.