МОНРЕАЛЬ — DNSSEC для всех: руководство для начинающих
3 ноября 2019 года, 17:00–18:30 по EDT
ICANN66 | Монреаль, Канада

ДЭН ЙОРК (DAN YORK): Чуть позже мы собираемся ответить на несколько вопросов, и я предложил бы вам подойти немного ближе. Сегодня мы в этом огромном зале, так что не стесняйтесь подходить ближе. У нас будет микрофон; мы будем ходить по залу и беседовать с вами.

Итак, меня зовут Дэн Йорк. Я работаю в Обществе интернета, занимаюсь технической информационно-разъяснительной деятельностью, которую мы там ведем, и сегодня мы хотим поговорить о том, что такое DNSSEC и какой цели они служат? И мы сделаем это несколькими способами. Мы расскажем вам небольшую историю, разыграем сценку, парочку сценок, немного поговорим об этом и постараемся развлечься в этот воскресный вечер.

Прежде всего, могу я задать вопрос? Кто из вас в какой-то мере внедрил DNSSEC? Несколько человек, хорошо. На а сколько людей понятия не имеют, что такое DNSSEC? Да, есть парочка. Я замечаю частичное совпадение с теми, кто это внедрил, так что у нас все в порядке, все хорошо. Итак, мы собираемся вернуть вас в прошлое и рассказать историю происхождения DNSSEC в 5000 году до нашей эры.

Итак, как гласит наша история, это Угвина. Она живет в пещере на одной стороне Большого Каньона. А это Ог, который живет в пещере на другой стороне. Чтобы встретиться, им надо проделать долгий путь, и поэтому им не часто удается поговорить, сходить друг к другу в гости или что-нибудь еще в этом роде. И во время одной из встреч они замечают, что от костра Ога идет дым. И вот, они понимают, что могут общаться с помощью дымовых сигналов; они могли бы посылать дымовые сигналы через каньон и, разумеется, рассказывать друг другу больше историй, разговаривать гораздо чаще.

Но однажды некий другой пещерный человек, живущий неподалеку, назовем его Камински, встает рядом с Огом и начинает посылать свои собственные дымовые сигналы. Внезапно, Угвина на другой стороне перестает понимать, какой из сигналов правильный; она не знает. «Кому мне следует...? Какие сигналы я должна считать правильными?» Она отправляется в путь, чтобы выяснить: «Что мы можем сделать? Как все исправить, чтобы я понимала, кто там?»

Они обращаются за помощью к мудрым старейшинам деревни. И у пещерного человека Диффи возникла идея. Он встает, бежит в пещеру Ога и идет к ее задней стене, где видит кучу голубого песка. Этот песок необычного цвета есть только в пещере Ога. Он берет немного этого песка, выбегает и бросает его в огонь. Пламя окрашивается в великолепный синий цвет, и теперь Угвина и Ог могут общаться, потому что теперь она знает, какие сигналы посылает Ог. Никто не может помешать, потому что они точно

знают, что голубой дым исходит от костра Ога, а не от какого-то другого.

Забавно, но в этом вся суть DNSSEC. Речь идет о том, чтобы вы получали правильную информацию от отправителя. Данные обрабатываются особым образом, чтобы можно было распознать, какая уникальная информация поступает от этого человека. Мы остановимся на этом немного подробнее, разберем технические аспекты.

На высоком уровне DNS часто изображается именно так. В конечном итоге, есть корень DNS, все эти домены верхнего уровня, TLD, которые показаны здесь, всевозможные разновидности. Кроме того, есть домены второго, более низкого уровня. И все это работает. Резолвер, DNS-резолвер, знает, как добраться до корня, он знает, как пройти по иерархии и определить ее, и на каждом уровне этого пути резолвер получает команду: «Иди, поговори с кем-нибудь еще».

DNS — это распределенная база данных. Он идет и выясняет, как получить информацию от каждого резолвера, по пути кешируя ее. Но этот протокол не обеспечивает безопасности, как в нашей маленькой истории, кто-то другой может прийти и подделать, дать другие ответы другим способом. Можно отравить кэш резолверов, потому что после запоминания эти данные могут храниться в течение некоторого срока.

И мы разыграем сценку. Труппа готова? Поднимайтесь. Мы собираемся показать вам немного подробнее, как это работает. Итак, вы видите, что здесь присутствуют персонажи, которые будут играть роль пользователя, который хочет найти информацию, хочет подключиться к bigbank.com. Итак, наши актеры занимают свои места. Ладно. Подождите. Хорошо. Вот. Хорошо. Таким образом, Уэс Хардейкер (Wes Hardaker) будет пользователем, который обменивается данными с интернет-провайдером, резолвером, а этот резолвер будет взаимодействовать с перестраиваемой иерархией DNS.

УЭС ХАРДЕЙКЕР: Проверка, проверка, проверка.

ФРЕД БЕЙКЕР (FRED BAKER): Первая проблема, нам нужно электричество.

ДЭН ЙОРК: Звук. Вы можете принести этот микрофон?

УЭС ХАРДЕЙКЕР: Готово. Пожалуй, я хочу купить яхту. Мне всегда хотелось купить яхту. Это огромные лодки, а мне нравятся огромные лодки. Я проверю свой банковский счет в www.bigbank.com и выясню, сколько у меня денег. Не подскажете мне адрес www.bigbank.com, чтобы я мог поговорить?

УОРРЕН КУМАРИ (WARREN KUMARI): Конечно, ведь вы такой клиент, которого мне не хотелось бы огорчать. Сейчас я это выясню для вас. Здравствуйте, корень! Один из моих пользователей хочет попасть на www.bigbank.com. Вы не подскажете, где это?

ФРЕД БЕЙКЕР (FRED BAKER): Ну, мне бы хотелось вам помочь, но есть проблема. На самом деле я этого не знаю. Я знаю, где найти .com, вы можете спросить у .com.

УОРРЕН КУМАРИ: Хорошо, спасибо, я попробую. Здравствуйте, .com. Один из моих пользователей хочет попасть на www.bigbank.com. Вы не подскажете, где это?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Ну, я не уверен насчет www., но знаю, что bigbank.com вон там.

УОРРЕН КУМАРИ: Прекрасно, пойду и спрошу у него. Здравствуйте, bigbank. Не могли бы вы сказать мне, где находится www.bigbank.com?

РАСС МАНДИ (RUSS MUNDY): Здравствуйте, господин ISP. Я могу сказать вам, где находится www.bigbank.com. Его адрес 2.2.2.3.

УОРРЕН КУМАРИ: Ура! Наконец-то я получил ответ. Здравствуйте, господин пользователь, www.bigbank.com находится по адресу 2.2.2.3. Вы прокатите меня когда-нибудь на своей яхте?

УЭС ХАРДЕЙКЕР: Боюсь, моя яхта не позволяет катать рекурсивные резолверы, но ладно. Хорошо, я могу проверить свой счет. Класс! У меня море наличных.

ДЭН ЙОРК: Давайте им поаплодируем за эту сценку. Вот так работает DNS. Именно это постоянно происходит при выполнении бессчетного множества маленьких DNS-запросов. Но мы хотим рассказать немного больше о том, как это может работать. И мы собираемся показать вам еще один обмен информацией. Мы сделаем это снова, но на этот раз вы увидите, что происходит, когда вмешивается злоумышленник.

УЭС ХАРДЕЙКЕР: Итак, поехали. Настал тот день, когда я собираюсь купить свою лодку, свою огромную яхту. Мне нужно снова зайти на bigbank.com, чтобы перевести деньги. Скажите еще раз, где он, потому что я забыл?

УОРРЕН КУМАРИ: Да, к сожалению, и я забыл. Но я сейчас выясню это для вас. Здравствуйте, корень. Один из моих пользователей хочет попасть на www.bigbank.com. Вы не подскажете, где это?

ФРЕД БЕЙКЕР: Если бы я только знал ответ. Хотя я знаю, где находится .com. Это поможет?

УОРРЕН КУМАРИ: Ну, да. Корень в общем-то бесполезен, так что пойду и спрошу у .com. Здравствуйте, .com. Один из моих пользователей хочет попасть на www.bigbank.com. Вы не подскажете, где это?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Ну, я все еще сомневаюсь насчет www., но знаю, что bigbank.com находится по адресу 2.2.2.2.

УОРРЕН КУМАРИ: Пойду и спрошу. Здравствуйте...

ЭНДРЮ МАККОНАХИ (ANDREW MCCONACHIE): На самом деле нет, потому что bigbank.com находится по адресу 6.6.6.6.

УОРРЕН КУМАРИ: Конечно. Разумеется. Здравствуйте, господин пользователь.

УЭС ХАРДЕЙКЕР: О, 6.6.6.6, теперь я знаю, куда обратиться... я могу отдать все свои деньги 6.6.6.6, спасибо. Где моя лодка?

ЭНДРЮ МАККОНАХИ: Спасибо. Ха-ха-ха!

УЭС ХАРДЕЙКЕР: Моя лодка?

ДЭН ЙОРК: Ладно. Давайте еще раз им поаплодируем. Итак, именно так DNS, о которой мы все здесь говорим, DNS может быть отравлена. Злоумышленник может это сделать. По сути, кто первый ответит резолверу, тот и побеждает. Вы знаете, скорость — решающий фактор в плане того, кто сможет передать свои данные.

И в данном случае доктор Зло сумел опередить бедного Расса и ответить раньше него. Так вот, опасность также и в том, что теперь Уоррен, наш ISP, в течение некоторого времени будет хранить этот ответ. Таким образом, все, кто запрашивает адрес www.bigbank.com, будут по-прежнему получать неправильный...

ЭНДРЮ МАККОНАХИ: 6.6.6.6.

ДЭН ЙОРК: Именно так. Будут по-прежнему получать неправильный ответ, неоднократно, пока не истечет временной интервал. Это атаки на DNS. Это отравление кэша. Все происходит именно так. Итак, опять же, сейчас мы рассматриваем DNS. С помощью DNSSEC мы добавляем концепцию цифровых подписей, и вы видите, что наша труппа все еще не уходит, потому что собирается еще раз разыграть эту сценку.

Что происходит, если у вас есть ключи и подписи, которые хранятся в DNS, чтобы можно было проверить, действительно ли информация поступила из первоисточника? Это действительно тот, кто должен передавать информацию о bigbank.com? Чтобы все это работало, резолверу известно, где находится ключ корневой зоны, или известно, как его получить. Кто из вас слышал о смене ключей корневой зоны в прошлом году? Да, хорошо. Люди этим интересуются.

Суть была в том, чтобы создать цепочку доверия от корня DNS вплоть до разных людей, разных авторитативных серверов, предоставляющих эту информацию. Все это связано, чтобы защитить целостность хранящихся там данных. Итак, мы хотим сделать так, чтобы только DNS-сервер bigbank мог передавать информацию ISP, а не кто-то другой. Давайте попросим наших актеров разыграть эту сценку еще раз, теперь с DNSSEC.

УЭС ХАРДЕЙКЕР: Вас порадует, что это в последний раз.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Прежде всего, нам нужны подписи.

ДЭН ЙОРК: О! О, да. Это необходимо сделать в первую очередь. Давайте, парни. Что мы здесь делаем? Корень подписывает. Разве IANA не понравилось бы, если бы все было так просто, верно? Итак, вы заметите, что корень их подписал: .com подписан, bigbank подписан, все подписаны. Все в порядке. И теперь...

УЭС ХАРДЕЙКЕР: Хорошо, давайте представим, что этого не произошло. У меня есть деньги еще на одну яхту. Я собираюсь пойти и купить другую лодку, на этот раз по-настоящему. Вы можете мне сказать на этот раз, где находится bigbank.com, и сообщить правильный адрес?

УОРРЕН КУМАРИ: Да, я попробую. Позвольте мне спросить у корня. Здравствуйте, корень, один из моих пользователей хочет выяснить, где находится www.bigbank.com. Не могли бы вы подсказать?

ФРЕД БЕЙКЕР: Нет, не могу. Но могу сказать вам, где найти .com, и .com сможет вам это сказать. И я подписан.

УОРРЕН КУМАРИ: Позвольте мне быстренько проверить эту подпись. Да, все в порядке, похоже она подлинная. Я пойду дальше и выясню у .com. Здравствуйте, .com, один из моих пользователей все еще хочет купить яхту. Ему нужно узнать, где находится www.bigbank.com. Не могли бы вы мне сказать?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Я до сих пор не знаю насчет www., но могу сказать, что bigbank.com находится по адресу 2.2.2.2, и я готов подписать этот ответ.

УОРРЕН КУМАРИ: Позвольте мне проверить эту подпись. Да, все в порядке, я пойду и спрошу. Здравствуйте, www.bigbank.com.

ЭНДРЮ МАККОНАХИ: Привет.

УОРРЕН КУМАРИ: Привет, как дела?

ЭНДРЮ МАККОНАХИ: 6.6.6.6.

УОРРЕН КУМАРИ: Где подпись? Я не вижу подписи [ПОМЕХИ] bigbank.com. Вы можете подсказать, где находится www.bigbank.com?

РАСС МАНДИ: Ну конечно могу. www.bigbank.com находится по адресу 2.2.2.3 и эти данные подписаны.

УОРРЕН КУМАРИ: Позвольте проверить, и я будут проверять тщательно. Да, все в порядке. Вот, пользователь, адрес www.bigbank.com 2.2.2.3, и я его проверил, можете ему доверять.

УЭС ХАРДЕЙКЕР: Спасибо. Господин Банк, вы можете перевести все мои деньги Дэну Йорку? Я покупаю у него подержанную лодку.

ДЭН ЙОРК: Ба! Спасибо, Уэс. Пожалуйста, поаплодируйте этим людям. Вот так мы это делаем и в этом суть DNSSEC. Есть подписи, которые гарантируют, что никто не сможет вмешаться в этот процесс.

Вот что происходит. И это все, что делается, важная часть. Это просто гарантирует целостность информации: пользователь получает именно те данные, которые размещены в DNS. Речь идет не о конфиденциальности, не о защите этих данных, а о проверке того, что данные именно те, что ввел пользователь. Теперь, чтобы немного подробнее обсудить это и привести пример, мы позовем сюда Расса Манди. И я верну деньги Уэсу.

РАСС МАНДИ: Спасибо, Дэн. И спасибо всем, кто сегодня к нам присоединился. Ой, какие яркие огни. Итак, вот о чем я хочу немного рассказать... Ага, пульт, хорошо. Это примеры и описания того, о чем нужно подумать людям, внедряющим DNSSEC. Частично ответ на вопрос «Зачем это делать?» кроется в ответе на вопрос «Почему вообще мы беспокоимся о DNSSEC?» И мы уже поговорили об этом с точки зрения DNS и того, как можно подменить данные DNS, особенно если у вас нет DNSSEC.

Но зачем люди пытаются взломать DNS? DNS сама по себе не представляет большого интереса. Когда люди пытаются вмешаться в работу DNS, почти во всех случаях их цель в том, чтобы что-то сделать с приложениями, которые отправляют DNS-запросы. Как вы уже видели, когда Уэс хотел перевести деньги, это была попытка украсть деньги. Поэтому очень важно, чтобы приложения, которые используют DNS, функционировали правильно. Если приложение не попадет в правильное место, кто знает, что произойдет.

У нас было несколько примеров такого рода в реальном мире и просто... некоторые из них перечислены на экране, и это любое приложение, которое сегодня работает в интернете. Есть чрезвычайно высокая вероятность того, что в основе оно использует DNS, и по большей части пользователи приложений не знают о существовании DNS и, честно говоря, она их не волнует, хотя для них важно, чтобы приложения функционировали должным образом.

Одна из вещей, которую я обнаружил несколько лет назад, и я вернулся и снова посмотрел, но, к сожалению, не сохранил конкретных данных о том, что нашел тогда. Но был один профессор университета, который в курсе по программированию требовал, чтобы его студенты написали программу для взлома DNS.

И я просмотрел все требования и программу курса, но не увидел ни единого упоминания об этике или о том, почему нельзя этого делать. Было сказано только: «Эй, студенты. Напишите-ка программу для взлома DNS», — и это было действительно жутко, потому что есть те, кто уже давно пытается не допустить ее взлома.

К счастью, такое больше мне не встречалось в течение последних пяти лет, так что, возможно, это кануло в прошлое. Итак, как сказал Дэн, очень важно иметь возможность добраться до нужного места, а когда вы доберетесь до нужного места, суметь убедиться, что полученная информация достоверна.

Таким образом, основополагающим техническим механизмом является криптография открытого ключа, встроенная для обеспечения работоспособности DNSSEC. Так вот, в рамках нашей предыдущей деятельности мы на конференциях ICANN действительно занимались реальным взломом. Это всего лишь серия слайдов, наглядно иллюстрирующих ту же идею, что вы видели на сцене.

Одна из причин, по которой мы перестали делать это по-настоящему, заключается в том, что на одной из конференций нам удалось вместо того, чтобы взломать DNS в конкретном зале заседаний, ну, конфигурация сети оказалась не совсем такой, как ожидалось, и мы взломали DNS всей конференции ICANN. Это было довольно смешно, когда все закончилось, но тогда нам было не до смеха. И теперь мы просто показываем слайды. Как видите, пользователь Джо в левом нижнем углу хочет попасть на свой веб-сервер вон там.

И вы можете видеть на картинке, что он отправляет запрос. Этот запрос поступает на его рекурсивный сервер. Рекурсивный сервер сохраняет и отправляет запрос на авторитативный DNS-сервер, связанный с сетью. Его веб-сервер, на который он хочет перейти, возвращает ответ на рекурсивный сервер. И затем рекурсивный сервер возвращает данные пользователю. Как раз это вы видели, когда мы ходили взад и вперед, бегали по сцене.

Теперь, после подключения, он действительно может провести свою транзакцию. Таким образом, когда мы заходим на реальные сайты, особая конфигурация обеспечивает показ изображения на самом сайте, которое сообщает об использовании DNSSEC.

Нет стандартного изображения, обозначающего наличие DNSSEC, но становится намного проще, если установить его на сайте для показа пользователям. И когда вы заходите на тот же сайт, не используя механизм валидации DNSSEC, отображается другой

символ. Вы видите, что вверху изображена галочка, а внизу треугольник, который сообщает: «О, режим DNSSEC отключен».

Когда мы делаем то же самое, что показывали на сцене; пользователь Джо отправляет запрос, но на этот раз в сети находится доктор Зло. Итак, запрос попадает в сеть, и в реальном мире доктор Зло видит этот запрос и отвечает на него. Хотя запрос еще продолжает блуждать по сети, пользователь Джо уже отправлен на подложный сайт.

И вы видите, что другие запросы прошли через сеть и вернулись с ответом, однако пользователь Джо его не получил, поскольку его резолвер взял первый ответ и перешел на неправильный сайт. Так что он уже не мог вернуться, если не использовал DNSSEC. Если он использовал DNSSEC, это препятствовало принятию неправильного ответа резолвером, а затем, после получения правильного ответа, он перешел на правильный сайт и вел свои дела без помех.

Итак, мы настроили сайт для демонстрации того, что можно сделать. В частности, на сайте был создан раздел, который показывал место, уязвимое для взлома. И затем против веб-браузера, не выполнявшего валидацию DNSSEC, была проведена атака. Мы фактически вставили информацию, фиктивную статью: «Стив Крокер признает, что DNSSEC не решит проблему голода в мире».

Довольно очевидная юмористическая иллюстрация, как и было задумано, но вы видите спереди изображение «DNSSEC выкл.», и

ниже статью о том, «Домен .org делится рекомендациями Comcast по DNSSEC для ISP», в то время как вверху страницы это было основной новостью. То есть, по сути, после взлома мы добавили на страницу информацию. Хотя она отображалась в браузерах на той же странице, это была другая информация, разумеется, ложная.

Сколько запросов поступает с пустого DNS-сервера, где нет кэшированных данных, для отображения единственной веб-страницы. Это CNN.com, вероятно, шесть или семь лет назад, и где-то около 75–100 запросов и ответов только для того, чтобы заполнить одну страницу. Таким образом, может быть взломан любой из них или значительная их часть.

Улучшилась ли ситуация? Нет, в некоторых отношениях да, а в некоторых нет. Для заполнения страницы коммерческого сайта требуется больше запросов, чем раньше. Эти конкретные измерения показывают, что некоторые из них уже подписаны с помощью DNSSEC, но количество, необходимое для заполнения сайта, почти удвоилось за четыре-пять лет. И основная вещь, о которой люди часто беспокоятся и думают, когда идет речь о DNSSEC: «О, боже мой, здесь используются криптографические ключи. Что нам делать? Это так важно следить за криптографическими ключами».

Да, все верно, но самое важное — это данные вашей зоны DNS. Таким образом, необходимо уделять как минимум столько же внимания точности и правильности данных своей зоны DNS, как и

любым криптографическим ключам, потому что смысл связывания DNSSEC с любой зоной заключается в том, что пользователь, получающий эту информацию, знает, что данные DNS верны. И поэтому, если вы будете больше заботиться о своих криптографических ключах, чем о данных своей зоны, и кто-то захочет атаковать вашу зону, они нападут на ту часть вашей системы, которая обеспечивает ввод данных в систему.

И если вы подпишете такие данные, получатели скажут: «Ну, эти данные наверняка правильные, ведь они подписаны». Однако, если кто-то успешно атакует то, что часто называют «системой подготовки» вашей информации, вашей части DNS, и поместит туда недостоверную информацию, то в некотором смысле ситуация станет хуже, чем была тогда, когда вы не использовали DNSSEC, потому что вы, как оператор, подтверждаете с помощью криптографии правильность этой информации, а если она недостоверна, то на вас ложится ответственность за неправильную и ненадлежащую обработку своих данных.

Вот еще один пример работы DNS без DNSSEC. Зона, это относится к данным зоны, когда вы размещаете информацию на своем авторитативном DNS-сервере. Эти данные поступают на авторитативный DNS-сервер, который находится в интернете, работает и содержит их. Он получает запрос от рекурсивного DNS-сервера, который, в свою очередь, получил запрос от клиента и отвечает на этот запрос.

Итак, если вы включаете DNS в состав своей системы вместо аутсорсинга или получения этих услуг от сторонней регистратуры, если DNS достаточно важна для работы того, что находится под вашим управлением, органически вписывается в деятельность вашей организации, то у вас, вероятно, есть персонал, который разбирается в DNS. И вы, наверное, захотите использовать DNSSEC как часть, как расширение того, что вы уже делаете для управления DNS.

Таким образом, крупные компании, опирающиеся в работе на собственные DNS, в частности те, для которых DNS особенно важна, вероятно, захотят самостоятельно обеспечить реализацию и функционирование DNSSEC. Например, вы — организация, зарегистрировавшая TLD, или крупное предприятие: hp.com всегда служил отличным примером; verisign.com, их бизнес связан с DNS. Это значимые организации с точки зрения DNS и поэтому, наверное, они будут заниматься этой системой самостоятельно.

Если ваши зоны DNS не настолько важны, ни для Интернета, ни для экономической жизнеспособности организации. То есть, если вы, здесь я приведу в качестве примера net-snmp.org — домен, который, по-моему, принадлежит мне. Он на самом деле ничего не делает. О, вы им сейчас владеете? Да, хорошо. Я передал его Уэсу. Хорошо.

Но суть дела в том, что его работа не является критически важной для DNS. Хорошо, если он правильно функционирует, но это не критично для интернета, для ведения вашего бизнеса. Кроме

того, все, кто здесь присутствует, все мы используем DNS и нам нужно использовать DNSSEC всегда, когда это возможно. Опять-таки, важно защитить данные зоны DNS. Так вот, мы видели предыдущий пример: загрузка зоны на авторитативный сервер, запрос данных и получение ответа.

Это хорошая простая иллюстрация тех мест, где нужно принять несколько дополнительных мер. Вы должны подписать данные своей зоны перед загрузкой на авторитативные серверы этой зоны. У рекурсивного сервера или конечного приложения, — надеемся, что когда-нибудь это произойдет, — но у самого рекурсивного сервера должен быть корневой ключ для валидации, чтобы при выполнении запросов и возврате ответов вы действительно могли выполнить валидацию самостоятельно. А для большинства валидирующих DNS-серверов, конечно же, продуктов с открытым исходным кодом, его можно включить, просто правильно настроив один переключатель конфигурации. Вот и все, что для этого нужно.

Теперь, в заключение, общий план действий для тех, кто запускает собственные DNS, для кого DNS очень важна. Они захотят самостоятельно внедрить DNSSEC и обеспечить работу DNSSEC, чтобы убедиться, что эта система работает так же хорошо и точно, как и их DNS. Если кто-то передал управление своей DNS на аутсорсинг, он, вероятно, также захочет поручить внешнему подрядчику деятельность, связанную с DNSSEC. И в некоторых случаях эта задача все более упрощается.

Многие провайдеры внешней службы DNS в прошлом не предлагали DNSSEC. И я настоятельно рекомендую тем, кто нашел поставщика услуг и привлек в качестве внешнего подрядчика, не заниматься DNSSEC самостоятельно, а попросить об этом их. И если они не согласятся, я... немногие так поступят, но некоторые из нас, в том числе я, это сделали... если они не найдут сервер, сменить того, кому вы платите за предоставление службы DNS, на того, кто внедрил DNSSEC.

И вот наш сводный слайд. Организации-спонсоры этого мероприятия, этого сегодняшнего дневного собрания. Возвращайтесь, Дэн. А в остальное время мы открыты для обсуждения, вопросов, ответов. И, пожалуйста, приходите и мы ответим на некоторые вопросы, я надеюсь.

ДЭН ЙОРК: Ага, да. Если вы, друзья, хотите подойти и взять здесь микрофон, у нас есть такие, которые должны быть... да, они должны быть... давайте. Итак, у кого есть вопросы? Вы все это посмотрели. Кто-нибудь? Давайте, кто-то должен.

Кэти здесь, о, Эндрю собирается прогуляться, доктор Зло. Кто-нибудь должен задать вопрос доктору Зло. Ага, хорошо, здесь кто-то есть. Я боялся, что мне придется начать шутить, а это может причинить боль. Взгляните на Уоррена. Хорошо, давайте.

РОСИО ДЕ ЛА ФУЭНТЕ (ROCIO DE LA FUENTE): Большое спасибо за выступление и за презентацию тоже. Я Росио де ла Фуэнте, участница программы Fellowship на ICANN66, и я просто хочу уточнить, правильно ли я поняла: подпись — это ключ DNS, поэтому, если TLD не подписан, у домена, который я регистрирую, не будет подписи, не будет DNSSEC, верно?

ДЭН ЙОРК: Да. Один из вас...? Хорошо, ответ следующий. Вы могли бы подписать свой домен, с ним можно так поступить, но он не попадет в цепочку доверия. Поэтому TLD, поэтому любой, кто будет подтверждать его достоверность, не сможет проверить весь путь до корня. Так что да, как правило, для работы DNSSEC необходим подписанный TLD.

УЭС ХАРДЕЙКЕР: И в идеале действительно нужно, чтобы было подписано все. Таким образом, DNSSEC защитит вас, начиная с корня, насколько ниже что-то подписано. Большинство TLD сегодня подписаны, и я думаю, что на семинаре по DNSSEC будут представлены графики, которые это продемонстрируют.

Есть более 10 миллионов подписанных доменов, знаете ли, например, конечных доменов, таких как bigbank.com, который, возможно, действительно существует и, возможно, не подписан. Но вы должны суметь проверить все дерево. С другой стороны,

даже если вы не можете, даже валидация до .com лучше, чем ничего, если сам bigbank, если нет связи ниже этого уровня.

ДЭН ЙОРК: Что касается замечания Уэса о семинаре по DNSSEC в среду, если вы на него придете, то увидите пару подготовленных нами диаграмм, где показаны некоторые из областей, и мы создадим несколько карт и во многих частях, но я пока не знаю, какие. Из какой вы страны? Аргентина? Хорошо. Это ведь домен .ar? Да, он проверяет. Давайте, там сзади.

ЯЗИД АКАНХО (YAZID AKANHO): Привет, меня зовут Язид Аканхо. Я из Бенина, участник программы Fellowship на ICANN66. Спасибо за презентацию, а также за фильм. Это помогает нам по-настоящему понять. У меня на самом деле два вопроса. Во-первых, почему внедрение DNSSEC... я не знаю, какое слово использовать, но внедрение идет довольно медленно. Почему? Есть технические причины? Политические? Просто, почему?

Второй вопрос. Мне рассказали о программе выездных презентаций DNSSEC, она умерла или…? Каков следующий этап программы выездных презентаций DNSSEC?

И мой последний вопрос. Расскажите подробнее об инфраструктуре генерации ключей для DNSSEC. Мне также рассказали, что есть отдельная инфраструктура, которая должна храниться в тайне. Можете объяснить немного подробнее? Спасибо.

ДЭН ЙОРК: Разумеется. Итак, проблемы с внедрением, выездная презентация DNSSEC, информация о процедуре подписания и так далее. Я правильно понял? Хорошо. Кто хочет ответить? Ответите на один из них?

УОРРЕН КУМАРИ: Я отвечу на некоторые. Итак, я быстро проверил, .ar подписан, поэтому Аргентина... Да, здорово. А что касается внедрения, да, DNSSEC внедряются не так быстро, как могли бы. Но некоторые интересные статистические данные. Сейчас мы в Канаде, и в Канаде проверяется 13,3% запросов, в США 25%, в Гренландии 19%, в России 14%.

Таким образом, как видите, это внедрено не так уж широко, не повсеместно, но темпы внедрения на самом деле набирают обороты, и сейчас проверяется большинство... не большинство, но значительное количество запросов, и подписано подавляющее большинство TLD. В соглашении об администрировании нового gTLD есть требование, чтобы все новые gTLD были подписаны, и на данном этапе также подписано большинство ccTLD.

ДЭН ЙОРК: Вам слово, Расс.

УЭС ХАРДЕЙКЕР: Если вы хотите отслеживать, знаете ли, ситуацию практически ежедневно, мой коллега... Виктор, спасибо, я запамятовал его

имя, у нас с ним есть сайт, который мы обновляем ежедневно — stats.dnssec-tools.org. На нем вы увидите, если посмотрите на график, вы увидите, что внедрение неуклонно расширяется с 2011 года. Иногда, вы знаете, бывают гигантские скачки.

Один фактически произошел всего за день, поскольку провайдер one.com неожиданно подписал множество имен в домене .dk. Так что бывают огромные скачки, и на самом деле для внедрения нам нужно, чтобы их стало больше. Нам нужны гигантские компании, чтобы это использовалось просто по умолчанию, потому что большая часть доменов в мире не находится под управлением отдельных людей, ими управляют, знаете ли, компании, предоставляющие услуги DNS-хостинга.

И на протяжении нескольких лет произошло много больших скачков. Швеция стала одной из первых стран, и в Чешской Республике также были гигантские стимулы, подталкивающие людей к подписанию. Финансовые стимулы, фактически, удешевляющие регистрацию, на самом деле сильно подтолкнули к подписанию в отдельных национальных доменах. Например, для роста.

ДЭН ЙОРК: Расс, вы хотели выступить?

РАСС МАНДИ: Да, я хотел бы просто, может быть, дополнить то, что сейчас сказал Уэс. Существует множество различных стимулов, которые использовались различными организациями, чтобы подтолкнуть людей к использованию DNSSEC. Одной из важных составляющих, которая очень помогла, является то, что большая часть общедоступных резолверов DNS, с четырьмя одинаковыми числами, довольно распространенная вещь. Большинство из них сейчас выполняет валидацию DNSSEC.

Одна из вещей, которой некоторые из нас, работавшие в этой области, уже давно занялись, это то, что мы хотим переместить валидацию в конечное приложение. И в примере, который включен в эту презентацию, когда Стив Крокер сказал: «DNSSEC не решит проблему голода в мире», валидация выполнялась в самом браузере.

Поэтому, когда будете общаться и обсуждать это с другими, помните о том, что чем ближе к конечному пользователю проводится валидация ваших DNS-данных, тем выше уровень безопасности системы. Предлагайте людям задуматься о том, чтобы выйти за пределы пусть даже крупных кеширующих общедоступных резолверов и реализовать это в приложениях. Это был еще один вопрос. Да.

ДЭН ЙОРК: Позвольте мне отметить, что эта конкретная проблема внедрения также связана с тем, как показано на этом рисунке, что на самом

деле есть две части, верно? Все, кто подписывает, у кого есть домен, который нужно подписать. И это одна часть. Это подписывающая сторона. И кое-что из этого, как сказал Расс, можно автоматизировать; у нас есть немало инструментов. И если пойти и поговорить с провайдерами DNS-хостинга, некоторые из них могут сделать это без всякого труда.

У некоторых есть флажок, знаете ли. Бум! И ваш домен подписан. Отчасти это легко. Однако, с другой стороны, вам нужно проверять, выполнять валидацию. И, как упомянул Расс, иногда это просто снятие галочки или удаление значка комментария у строки в файле конфигурации, после чего сразу можно начать валидацию.

Но отчасти в течение долгого времени у нас была проблема типа «курица и яйцо», как сказали бы в США, с точки зрения... Некоторые сетевые операторы, интернет-провайдеры, которых играл Уоррен, выполняющие валидацию DNSSEC, говорили: «Мы не собираемся включать эту валидацию, потому что недостаточно подписанных доменов».

Таким образом, операторы говорили: «Эй, мы не собираемся этого делать, потому что мало подписанных доменов». А некоторые из крупных хостинг-провайдеров говорили: «Ну, мы не собираемся подписывать свои домены, потому что мало кто выполняет такую валидацию». То есть были те, кто приостанавливал процесс и говорил такие слова.

Сегодня многое из этого уже преодолено, потому что, как сказал Уэс, есть реальные случаи внедрения, знаете ли, очень много тех, кто занимается рекурсивным разрешением. И если посмотреть на некоторые крупные общедоступные DNS-серверы, такие как Google Public DNS, Cloudflare, Quad Nine, все они выполняют валидацию DNSSEC.

Итак, это делают крупные резолверы, это делают крупные ISP, Comcast здесь, в Северной Америке, с его 20 миллионами клиентов, которые... все делается с использованием валидации DNSSEC. Так что это препятствие, некоторое время замедлявшее внедрение, теперь преодолено, хотя еще не до конца. Я знаю, что вы можете рассказать еще о двух составляющих, Фред. Хотите...? Да, он включен.

ФРЕД БЕЙКЕР: Я хотел задать Рассу вопрос. Вы можете назвать конкретные браузеры, поддерживающие валидацию DNSSEC? Какой браузер... на моем ноутбуке только четыре браузера. Какой мне следует использовать?

РАСС МАНДИ: Ну, к сожалению, нет доступного браузера со встроенной валидацией DNSSEC. Уоррен, вам о таком известно? У нас был один и он поддерживался некоторое время, но больше не поддерживается.

УОРРЕН КУМАРИ: Фактически, подождите секундочку. По-моему, тот, о котором вы говорите, выполняет валидацию DANE.

ДЭН ЙОРК: Нет, нет.

УОРРЕН КУМАРИ: Я хочу сказать, что все браузеры полагаются на системный резолвер. Если компьютер выполняет валидацию DNSSEC. Резолвер в браузере во многом зависит от того, что делает системный резолвер. Таким образом, если включена валидация DNSSEC на любом резолвере, на который указывает ваш компьютер, вы получите валидацию DNSSEC за чужой счет. И думаю, что Уэс сейчас начнет кричать на меня.

УЭС ХАРДЕЙКЕР: Вовсе нет. Я никогда не стал бы на вас кричать.

ФРЕД БЕЙКЕР: Хорошо. Вы только что сказали мне, как пользователю, что мне нужно что-то сделать на своем компьютере, где установлена система Mac, Windows или Linux.

УЭС ХАРДЕЙКЕР: Это сложно описать, и мы углубимся в технические нюансы, но есть элементы, где может выполняться валидация. Прямо сейчас,

сегодня, приложения, к которым относятся браузеры и программы для чтения электронной почты, а также все остальное, что подключено к сети, обычно не выполняют проверку самостоятельно. Как и в сценке, где минуту назад я, пользователь Джо, на самом деле не сам проверял эти сертификаты, а доверил эту задачу своему ISP. И это действительно...

ФРЕД БЕЙКЕР: Пользователь Джо, вы ужасный человек.

УЭС ХАРДЕЙКЕР: Я ужасный человек. Итак, я на самом деле вложил код валидации в... Фактически, в пакет net-snmp, о котором недавно говорил Расс. На самом деле код валидации есть в этом пакете с открытым исходным кодом, что позволяет выполнять валидацию в приложении. Но ее выполняют очень немногие приложения. Есть одна, одна из самых важных, если открыть страницу статистики, о которой я уже упоминал.

Одной из самых важных причин для внедрения и использования подписей является то, что это один из немногих способов... это действительно лучший способ защитить электронную почту при передаче между серверами. Так что, на самом деле, его использование очень быстро расширяется. Не все это DNSSEC, но если посмотреть на использование DANE, технологии, где подписи применяются при обмене электронной почтой между

серверами, то оно довольно быстро расширяется, и это происходит по крайней мере рядом с приложением, если не в нем.

ДЭН ЙОРК: Хорошо, Уоррен. У вас был...

УОРРЕН КУМАРИ: Фред, вы сказали, что как пользователь услышали о необходимости что-то сделать. Как пользователь вы должны убедиться, что резолверы вашего ISP выполняют валидацию. Вы можете его об этом попросить. Или воспользуйтесь одним из... знаете ли, если нет, вы можете выбрать один из крупных общедоступных резолверов, 111199998888, один из них, потому что все они выполняют такую валидацию.

Таким образом, если вы хотите получить защиту DNSSEC, воспользуйтесь соответствующей услугой своего ISP, а если он ее не оказывает, обратитесь к кому-то другому. Есть сайт, internet.nl. Если на него перейти, то можно проверить, выполняют ли валидацию используемые вами рекурсивные резолверы. И вы сможете понять, делает ли это ваш ISP.

ДЭН ЙОРК: Я хочу вернуться к вопросу Язида, но, я бы сказал, Фред, что касается браузеров, мы рискуем углубиться еще сильнее, но давайте просто оставим это на среду. Но есть вещи, которые начинает выполнять DNS по HTTPS, как это делают браузеры. И

многие другие конечные точки, являющиеся серверами DOH, также выполняют проверку DNSSEC. Таким образом, ваш браузер действительно может делать это, если пойти по этому пути, но давайте не будем сейчас рассматривать DOH.

Давайте вернемся к вопросу Язида, потому что он очень терпеливо стоит, и извините, если я неправильно произнес ваше имя.

ЯЗИД АКАНХО: Меня зовут Язид. Хорошо, спасибо. Спасибо, что пояснили валидацию в резолверах и подпись зоны. Как я понимаю, это две разные вещи. Два года назад в моей стране, в Бенине, мы удивились, когда заметили, что резолверы выполняют валидацию 80% запросов DNSSEC. Почему? Потому что некоторые интернет-провайдеры использовали публичные резолверы.

ДЭН ЙОРК: Да.

ЯЗИД АКАНХО: И это не имеет ничего общего с подписанием зоны, поэтому я и спросил. Куда делась программа выездных презентаций DNSSEC?

ДЭН ЙОРК: Да. Итак, вы абсолютно правы, и это... по некоторым статистическим данным, может быть вашим, Уэс, но я знаю, что статистические данные APNIC Джеффа Хьюстона говорят о том,

что в некоторых странах сейчас чрезвычайно высокие уровни валидации DNSSEC. И если их изучить, то окажется, что некоторые из этих ISP в своей стране ушли и просто используют публичные DNS-серверы. У них нет собственных резолверов, они используют, знаете, 8.8.8, 1.1, 9.9, что угодно, один из существующих публичных резолверов.

Что касается выездных презентаций ICANN, я не знаю. На этот вопрос мы ответим вам позже, поскольку не участвуем напрямую в этой программе. Поэтому мы позже передадим вам ответ. Так что, Язид, просто сообщите одному из нас свое имя, и потом мы с вами свяжемся.

Что касается вопроса о документации, я также могу... Найдите меня... Можете сказать свой номер? Общество интернета опубликовало на нашем сайте информацию о нашей части Deploy 360, ICANN опубликовала некоторую информацию, есть ряд ресурсов, где представлены подробности. И многие компании, имеющие авторитативные серверы, ISC, nlnet labs, некоторые другие, прошли через это и подготовили собственную документацию о том, как это сделать. Так что есть несколько полезных ссылок. Другие вопросы? Да, вон тот господин.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Спасибо. Рискую немного отклониться от темы, но мне интересно, какое отношение имеет DNSSEC к разделу псевдо-записи SIG(0) в ответе.

УЭС ХАРДЕЙКЕР: На самом деле никакого. Это разные вещи. DNSSEC призваны защитить набор данных и обеспечить возможность его валидации, чтобы независимо от того, как они к вам попали, в них можно было разобраться. SIG(0) и TSIG — это еще одна технология в DNS, предназначенная для защиты. Но она защищает только соединение, а не сами данные, независимо от маршрута их передачи. Это разные технологии.

ДЭН ЙОРК: Да, прошу вас.

УОРРЕН КУМАРИ: В некотором смысле из этого следует вот что. Уэс сказал, что DNSSEC позволяет вам выполнять валидацию информации независимо от того, как она получена. Одним из приятных следствий является то, что многие на самом деле просто загружают всю корневую зону в свой резолвер, потому что все данные подписаны.

И можно просто выполнять валидацию в своем резолвере; не нужно отправлять запросы в корень. Это один из приятных моментов, связанных с наличием подписанной зоны. В определенных ситуациях вы можете не заниматься получением ответов на запросы, а просто скачать весь файл зоны или позволить кому-то другому сделать это.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Это относится к запросу на перенос, или вы получаете весь файл зоны?

УОРРЕН КУМАРИ: Итак, многие корневые серверы, в том числе обозначенные буквами B и F, и я не могу вспомнить, какие еще, позволяют просто выполнить запрос на перенос, AXFR. Если вы узнать больше, это называется «локальный корень» — это одно из названий, и в RFC 7706 есть информация о нем, а скоро выйдет новая версия этого стандарта. Но, да, локальный корень или гиперлокальный корень...

ДЭН ЙОРК: Гиперлокальный корень, да.

УОРРЕН КУМАРИ: ...есть проект, который позволяет вам сделать это через веб-страницу.

УЭС ХАРДЕЙКЕР: Да. Мой фактически называется локальным корнем, и это localroot.isi.edu, он дает конфигурацию, необходимую для превращения резолвера в корневой кеширующий резолвер, чтобы все предварительно кэшировалось. Есть много информации об этом, и, надеюсь, вам будет довольно легко в ней разобраться, если вы квалифицированный администратор, а не конечный пользователь.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Вы позволите мне задать еще один, еще один вопрос на тему DNSSEC? Если взглянуть, например, на домен .com, у него может быть десяток DNS-серверов. Получает ли каждый из них уникальный ключ DNSSEC для каждого отдельного зеркала, компьютера, или ключ один для всего TLD?

УОРРЕН КУМАРИ: На самом деле подписывается зона. Поэтому, когда зона подписана, ее можно поместить на любой DNS-сервер. Это особенно приятно, если вы используете собственный DNS-сервер, а затем привлекаете стороннюю организацию, у которой будет своего рода ведомый или вторичный сервер. Вы подписываете свою зону, передаете им зону и другие ключи не нужны. Очевидно, что вам не придется опасаться того, что они смогут воспользоваться ей в злонамеренных целях, или чего-то в этом роде.

ДЭН ЙОРК: Да, в этом вся прелесть такого алгоритма работы, потому что, как сказал Уоррен, как только вы все это подписали, вы можете просто остановить это где угодно. Это открытый ключ, закрытый ключ, криптография. Другие вопросы? Они могут быть общими, они могут быть глупыми. Вы можете спросить... почему в DNSSEC есть аббревиатура SEC или что-то еще? Я не знаю. Да, снова вы, Язид.

ЯЗИД АКАНХО: Еще один вопрос. Я слышал, что изучается или анализируется возможность изменить протокол создания открытых и закрытых ключей корневой зоны. Где это обсуждается и каковы дальнейшие шаги?

ДЭН ЙОРК: Ну, по-моему, некоторые из моих коллег, сидящих за этим столом, могли бы рассказать об этом, только вкратце. Вы совершенно правы. Итак, при подписании, когда у вас есть подпись, на подписывающем сервере используется определенный криптографический алгоритм. Будь то RSA или криптография на основе эллиптических кривых. Есть множество разных криптографических алгоритмов, каждый из которых обладает своими свойствами, более или менее защищен, более или менее подвержен взлому. Видите ли, некоторые из первоначальных протоколов уже взламывались различными способами, так что некоторые могут это сделать.

Поэтому люди переходили на более безопасный алгоритм. Теперь мы с разных сторон изучаем 2048-битные ключи RSA. Мы изучаем эллиптические кривые, которые к тому же меньше. Так что да, существуют разные алгоритмы. Что касается состояния корня, Уоррен, похоже, что вы хотите нажать кнопку. Нет? Хорошо.

УОРРЕН КУМАРИ: Пожалуй, у меня будет несколько общих комментариев.

ДЭН ЙОРК: Вы нажимали кнопку; ваша рука лежала на ней. Поэтому я думаю...

УОРРЕН КУМАРИ: Я просто ее потрогал. Итак. Существует много религиозных течений, у каждого из которых свой лучший криптографический протокол, и если закрыть в одной комнате трех криптографов, живым оттуда выйдет только один, который зарежет всех остальных. Знаете, какой ожесточенный спор идет о том, что лучше: RSA, эллиптическая кривая, ED 25519 или что-то еще. В настоящее время произошел определенный переход от RSA к более новым протоколам, но одна из вещей, которую некоторые начинают обсуждать, это протоколы, обеспечивающие безопасность в мире квантовых вычислений.

Некоторые специалисты по криптографии обеспокоены тем, что квантовые компьютеры сделают существующие криптографические алгоритмы бесполезными. Есть множество других, кто считает эту проблему сильно раздутой. Но на это начинают обращать внимание, и в какой-то момент, знаете ли, может начаться внедрение протоколов квантовой безопасности.

ДЭН ЙОРК: Думаю, что ответ следующий. Те, кто занимается корневой зоной, не планируют срочно менять протокол. О, Расс, вы хотите его изменить?

РАСС МАНДИ: Ну, мы не собираемся его менять, но я снова хотел прорекламировать наш семинар в среду. Одним из пунктов повестки дня является презентация Кима Дейвиса (Kim Davies) о планах очередного обновления ключа KSK. Таким образом, если вам нужна дополнительная информация о сроках и процедуре, и вы хотите понять, как были учтены все полученные от сообщества комментарии, на семинаре DNSSEC в среду днем, по-моему, состоится 20- или 25-минутное заседание, где Ким, президент PTI, который управляет IANA, проведет презентацию недавно, в пятницу или в субботу, опубликованного проекта плана.

ДЭН ЙОРК: Только что доставленного из типографии. Кстати, этот семинар будет проходить в 13:30 по соседству в зале 517C. Несколько часов обсуждения различных аспектов DNSSEC, всего спектра вопросов. Некоторые вопросы высокого уровня, некоторые глубинные, а некоторые между ними, весь спектр. И вы увидите там многих из нас. Еще вопросы?

Эндрю стоит там и машет рукой. Кто-то должен ему помочь. Кто-нибудь? Есть желающие? У вас есть возможность получить бесплатный совета или что-то еще, иначе мы попросим Уоррена снова начать шутить. Да, хорошо. Смотрите. Отлично. Угроза подействовала.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Может быть это немного глупый вопрос, но я просто хотел кое-что уяснить. Фактически, это своего рода продолжение вопроса, который ранее задал Фред. Итак, если у меня нет браузера, который поддерживает DNSSEC, или, например, Outlook или чего-то еще, значит ли это, что сегмент между моим DNS-резолвером и клиентом технически незащищен?

ДЭН ЙОРК: Да. Но вам также следует четко понимать, как сказал Уоррен, что все приложения на вашем устройстве исторически всегда передавали задачу разрешения DNS небольшому куску кода, stub-резолверу в операционной системе, который затем отправлял внешние запросы резолверу ISP и все выполнялось там.

Поэтому, если ваша операционная система не поддерживает валидацию DNSSEC, проверку подписей, да, есть риск того, что злоумышленник, доктор Зло, подсунет вам ложную информацию и перенаправит на другой сайт. Традиционно было именно так, за исключением нескольких ситуаций, например, когда люди встраивали, знаете ли, валидацию DNSSEC в определенные браузеры, в большей степени для тестирования.

Сейчас это немного меняется. Есть целая группа в составе Инженерной проектной группы интернета, IETF, которая изучает тот факт, что все больше и больше приложений выполняют валидацию DNSSEC. Мы слышим о некоторых более важных вещах, в том числе о DOH и браузерах, но и другие приложения

тоже расширяют использование валидации DNS и не только, что немного меняет архитектуру DNS и интернета. Уоррен смотрит на меня так, будто хочет что-то сказать.

УОРРЕН КУМАРИ: Да. Уоррен считает, что на самом деле вы, или все мы могли бы «перепродать» защиту, которая здесь есть. Итак, что на самом деле происходит, если вы заметили это в сценке, ISP пошел и выполнил всю валидацию, в конце концов вернулся к пользователю и сказал: «Я проверил. Не волнуйтесь, все в порядке».

На самом деле DNSSEC работает так: валидирующий резолвер, ISP, публичный DNS-сервер или другое устройство выполняет проверку, а затем сообщает клиенту, что он это сделал, и этим данным следует доверять. По сути, он сообщает: «Да, все в порядке», — и все счастливы. Это означает, что, если пакет на обратном пути от резолвера к клиенту будет перехвачен, кто-то сможет сделать что-нибудь плохое.

В конце концов, было бы неплохо, если бы ваш компьютер сам выполнял проверку, а не доверял ISP, если бы он сам выполнял всю криптографическую работу. И некоторые операционные системы можно заставить это делать. Linux, к примеру, многие версии Debian сейчас поставляются с функцией, которая позволяет нажать кнопку, и операционная система сама выполнит проверку.

Некоторые поставляют программное обеспечение, которое можно просто установить на компьютер. Есть программа под названием Stubby, выполняющая валидацию. Но в целом вы в значительной степени верите своему ISP или резолверу, что он сделал все правильно и не солгал, а также не изменил какие-то данные на обратном пути.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Да, я был... о, да, позвольте мне дополнить свой вопрос. Я думал скорее о том, когда кто-то в локальной сети, возможно, просто отравил все данные, и фильтрует, просто отвечает на DNS-запрос быстрее.

ДЭН ЙОРК: Правильно, и это именно тот вектор атаки, который возможен, и именно поэтому вы видите большую работу, связанную с конфиденциальностью данных DNS, DNS по TLS, DNS по HTTPS, DOH, и так далее, чтобы изучить механизм шифрования данных в канале связи от вашего локального устройства до рекурсивного резолвера, чтобы создать там защищенное соединение, чтобы в вашей локальной сети не было такого человека, отправляющего пакеты. Это еще один элемент уровней глубокой защиты и уровней защиты DNS.

УОРРЕН КУМАРИ: Да, из этого следует возможность двух разных атак. В вашей сети есть тот, кто отравляет данные и затем посылает вам неправильные ответы, чтобы заставить вас пойти не туда. Но не менее страшно, когда кто-то в сети просто наблюдает за вашими пакетами, и, видите ли, не очень поможет, если весь контент зашифрован, когда вы заходите на https://alcoholicsanonymous.org.

Если люди увидят, что вы искали имя alcoholicsanonymous.org (сайт анонимных алкоголиков) или gayrights.org (права геев) или humanrightswatch (защита прав человека), сам факт разрешения определенных имен, то факт, что это не зашифровано, способен нанести такой же ущерб, как и доступ к просматриваемому вами контенту.

ДЭН ЙОРК: Расс.

РАСС МАНДИ: То, что сейчас описал Уоррен, иногда называют атакой в кафе, когда вы заходите в свою любимую местную кофейню, сеть Wi-Fi там может быть зашифрована, но... общедоступна, и любой посетитель кафе может подключиться к этой сети Wi-Fi, копировать или фальсифицировать ответы на ваши DNS-запросы.

И поэтому, если у вас есть, если у вас есть средства защиты на компьютере, подтверждающие достоверность данных, вы будете менее уязвимы для атак. И я точно знаю, что это осуществимо и в

интернете доступно для скачивания программное обеспечение, которое позволит это сделать.

ДЭН ЙОРК: И, чтобы внести ясность, опять же, DNSSEC просто гарантирует получение правильных ответов. Речь идет исключительно о целостности. Мы говорим о дополнительных уровнях повышения конфиденциальности, и некоторые из них обсудим в среду на нашем заседании в 1:30. Там будут рассматриваться некоторые составляющие этого. Вы удовлетворены? У вас что-то еще?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Да, да, я удовлетворен. Большое спасибо.

ДЭН ЙОРК: Хорошо, спасибо. Кати говорит мне, что получено что-то от удаленного участника.

КАТИ ШНИТТ (KATHY SCHNITT): Вопрос задает Коси. Можете ли вы пояснить суть сделки между Firefox и Cloudflare относительно резолвера DNSSEC, о которой говорилось на предыдущей презентации.

ДЭН ЙОРК: Хорошо, DOH. Я не знаю... насколько сильно мы хотим в это углубиться?

УЭС ХАРДЕЙКЕР: Я могу рассказать об этом в общих чертах с нейтральной точки зрения.

ДЭН ЙОРК: Давайте, расскажите в общих чертах с нейтральной точки зрения.

УОРРЕН КУМАРИ: О, это подразумевает, что я не могу.

УЭС ХАРДЕЙКЕР: Проблема в том, что именно я отвечал во время предыдущего разговора и предлагаю вам поправить меня, если я ошибусь. Согласны? Итак, есть два... позвольте сначала вернуться и ответить на предыдущий вопрос, опять же, очень кратко.

Есть несколько способов защитить обмен данными между вами и резолвером. Хорошо, доктор Зло. Есть несколько способов защитить вас от резолвера, и мир все еще работает над этим. Кроме того, через две недели Инженерная проектная группа интернета будет дополнительно обсуждать эту тему. Можно использовать DNSSEC на стороне клиента, можно использовать что-то вроде DOH, можно использовать что-то вроде DOT, есть несколько способов, и мы пытаемся выяснить, как обеспечить защиту. Все они работают по-разному.

Что касается браузеров, разработчики браузеры решили, поскольку они уже очень хорошо разбираются в HTTPS,

понимают этот протокол, понимают, как его использовать, у них есть действительно быстрые библиотеки, которые знают, как его использовать. Они решили, что хотят использовать DNS по HTTPS и заинтересованы в этом. Они внедряют это по-разному.

Двое, о ком я знаю, это Chrome и Firefox. Планы других мне неизвестны. Начну с Firefox, потому что его разработчики вроде бы объявили об этом первыми. Разработчики Firefox решили наладить сотрудничество с компанией Cloudflare, у которой есть сетевые прокси-серверы и широкие функциональные возможности, и которая также входит в число тех, кто создал общемировой валидирующий резолвер DNSSEC.

Они сотрудничают с Cloudflare, чтобы отправлять все ваши веб-запросы DNS в Cloudflare, если вы используете Firefox. Это происходит прямо сейчас, если вы используете... если вы находитесь в Соединенных Штатах. Их дальнейшие планы пока неясны, но в этом месяце они вернулись к обычному тестированию в Соединенных Штатах, и на данный момент сотрудничают только с Cloudflare, хотя у них будет раскрывающийся список, который позволит выбирать других поставщиков.

Google, с другой стороны, и именно здесь Уоррен поправит меня, если я ошибусь, Google, с другой стороны, на самом деле собирается проверять вашего ISP, смотреть, предоставляет ли ваш ISP сервис HTTP или HTTPS для DNS. И если предоставляет, и если он есть в списке доверенных провайдеров, то для обмена данными с таким ISP будет использоваться DOH. Если один из

этих критериев не выполняется, будет использоваться обычная DNS. Они не собираются отправлять ваш трафик третьей стороне, если только не изменили недавно свое решение.

УОРРЕН КУМАРИ: Хотя мне больно это говорить, в принципе все правильно. Я имею в виду, что хотел бы добавить что-нибудь о подходе Chrome. Google считает, знаете ли, что вам нужно продолжать, в настоящее время вам нужно продолжать обмен данными с текущим резолвером, потому что он может защитить вас от вредоносного ПО. Если вы обмениваетесь данными со своей текущей группой резолверов, если они не меняют ваш резолвер, это позволяет вам использовать все текущие механизмы защиты, позволяет вам искать внутренние доменные имена и тому подобное. Таков в общем-то подход Google.

ДЭН ЙОРК: И я думаю, что удаленному слушателю, задавшему этот вопрос, важно также понимать, что есть протокол, DOH, DNS по HTTPS, который был определен IETF в RFC 8484. Это протокол, который определяет алгоритм использования DNS через соединение HTTPS. Существует протокол под названием DOH, и клиент DOH, который может быть браузером, — пока это основной вид приложений, — и обмениваться данными с любым сервером DOH. И это способ создания зашифрованного, безопасного частного соединения между приложением и резолвером DNS. Итак, это шифрует подключение. DOH — соответствующий протокол.

Так вот, на этих ранних этапах внедрения DOH возникли разногласия из-за различных механизмов и разных предложенных способов. Так что, по-моему, важно просто понимать, что есть протокол, который работает на этом уровне конфиденциальности, чтобы гарантировать, что ни один из посетителей кафе не сможет перехватить все ваши метаданные обо всех местах, которые вы хотите посетить.

И именно для этого предназначен DOH и еще один протокол под названием DNS по TLS, DOT. Эти два протокола предназначены для защиты конфиденциальности. То есть они повышают уровень конфиденциальности в подобных ситуациях. При этом возникают споры, в том числе из-за разных подходов к реализации на текущем начальном этапе. Расс, вы что-то хотите сказать или... подождите. Уоррен?

УОРРЕН КУМАРИ: Уэс указал на то, о чем я забыл. Полное раскрытие, я работаю в компании Google, знаете ли, которая разрабатывает Chrome. Я хотел сообщить об этом, но забыл.

РАСС МАНДИ: Скажу тем, кто хочет увидеть немного больше, услышать немного больше об этом обсуждении, что, по-моему, на ICANN64 состоялось специальное заседание для обсуждения темы, представляющей особый интерес, примерно полуторачасовое или двухчасовое, где упоминались DOH и DOT. Это довольно

длинное заседание, оно было записано, и я уверен, что запись доступна на сайте архива ICANN64, так что можете посмотреть там пару часов соответствующей дискуссии в ICANN.

ДЭН ЙОРК: Еще вопросы? Эндрю.

ЭНДРЮ МАККОНАХИ: По-моему, на самом деле это произошло на ICANN65. Разве не там в последний раз проводилось заседание на тему DOH?

УЭС ХАРДЕЙКЕР: В Марракеше, да.

ЭНДРЮ МАККОНАХИ: Да. Да. Да.

ДЭН ЙОРК: Хорошо, еще вопросы?

УЭС ХАРДЕЙКЕР: И я должен по крайней мере упомянуть, что работаю в Университете Южной Калифорнии, чтобы сообщить, откуда я.

УОРРЕН КУМАРИ: И, наверное, о DOH, DOT и подобных вещах будет представлено немного больше информации, хотя я это не проверял, на семинаре DNSSEC.

УЭС ХАРДЕЙКЕР: Да, мы проводим в среду заседание, посвященное DOH.

ДЭН ЙОРК: Еще вопросы? Да, участник в передней части зала, вон там. А потом вы, вас я тоже заметил.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Я Гай из США. Существует ли способ отправки частных DNS-запросов, которые нельзя перехватить в кафе, которые невозможно отследить, потому что сам DNS-запрос каким-то образом зашифрован?

ДЭН ЙОРК: Да. И, опять же, это позволяют сделать технологии DOH или DOT. Вы можете подключиться со своего... ну, если вы хотите использовать их напрямую, это можно сделать с помощью браузера. Если настроить Chrome или Firefox на использование DOH. Это можно сделать сейчас и указать, к какому серверу подключаться. Это можно сделать прямо сейчас.

Вы также можете перейти на dnsprivacy.org, верно? На сайт dnsprivacy.org, где есть целый ряд других программ, которые

можно установить. Вы можете установить в своей локальной системе программу Stubby, которая будет шифровать все ваши запросы на определенных серверах DOT. Так что вы можете это сделать. Вы также можете запустить свой собственный сервер DOH или DOT, если хотите. Вы можете запустить его самостоятельно, где захотите, и настроить соответствующим образом. Это можно сделать.

УОРРЕН КУМАРИ: И вы также можете создать VPN, если прямо сейчас хотите получить быстрое и простое универсальное решение.

ДЭН ЙОРК: Да. Да, вы. Еще вопросы? Да, сзади.

РОСИО ДЕ ЛА ФУЭНТЕ: Мой вопрос относится к компьютерной грамотности. Когда мы говорим об обучении пользователей или владельцев доменов, должны ли мы разъяснять им важность DNSSEC при регистрации доменов? Потому что, когда мы говорим об ISP, регистратуре, регистраторах... не регистратор регистрирует, верно? И если рассказывать об этом, поспособствует ли это внедрению DNSSEC? Как вы считаете?

ДЭН ЙОРК: Ну, по-моему, все четверо сидящих здесь людей и не только они сказали бы: «Совершенно верно». Мы, конечно, призываем людей включать это в состав... просто говорить о том, что при получении и настройке домена, его следует подписать.

Опять-таки, некоторые регистраторы, и я не знаю, как обстоят дела в Аргентине, но некоторые регистраторы достигли такого уровня, регистраторы и провайдеры DNS-хостинга достигли такого уровня, когда DNSSEC можно включить, установив флажок или нажав кнопку, к примеру.

И в идеале именно к этому мы стремимся в том, что касается подписания, чтобы этот процесс стал очень простым и легким, чтобы конечному пользователю даже не приходилось каким-то образом вмешиваться. Но мы призываем людей подписывать домены, потому что это гарантия сохранения репутации бренда, гарантия того, что люди попадут на сайты, которые вы разместили в DNS.

УОРРЕН КУМАРИ: Позвольте не согласиться?

ДЭН ЙОРК: Уоррен может не согласиться, конечно.

УОРРЕН КУМАРИ: Уоррен может не согласиться ни с чем, потому что любит спорить. Я хочу сказать, что все зависит от того, на каком этапе процесса повышения компьютерной грамотности это происходит. По-моему, мы все сказали бы, что DNSSEC — хорошая вещь, но разве она важнее всего для нового интернет-пользователя? Пожалуй, нет. Разве это самое важное при регистрации домена? Так могло бы быть, но хочу сказать, что есть много других вещей, связанных с безопасностью, которые тоже очень важны, и вам нужно разобраться в них. Так что это вписывается в целый спектр.

ДЭН ЙОРК: Ладно, Уоррен. Это был хороший спектр разногласий. Прошу вас.

РОСИО ДЕ ЛА ФУЭНТЕ: Вот почему я тоже об этом думала. Потому что, если размышлять с точки зрения стимулов и, что касается нас, мы отчасти участвуем в работе ICANN и управлении интернетом. Если у вас нет технического образования, вам придется потратить время и силы на осмысление важности DNSSEC. Владелец домена или пользователь думает о своей компании или о чем-то еще. Например, как вести пропаганду, что-нибудь вроде: «Хорошо, это важно. Может быть, домен обойдется вам немного дороже, но в интернете он будет в безопасности», — верно?

ДЭН ЙОРК: Да. Это часть проблемы, и, честно говоря, именно поэтому во многих местах мы сотрудничаем с провайдерами DNS, поставщиками DNS-хостинга или регистраторами, которые зачастую бывают в одном лице, и стараемся уговорить их сделать это, подписать все, как это делает часть провайдеров DNS-хостинга, которые просто подписывают домен по умолчанию. Или, чтобы людям было легче понять и сделать это. И в идеале, сделать это без затрат, хотя, знаете ли, бизнес-модели варьируются в разных местах.

Поскольку, что касается вашего мнения Уоррен, и я согласен с Уорреном, что в общем плане того, как кто-то выходит в интернет на новом месте, это одна из многих вещей в его списке. Но она может не попасть в этот список, в зависимости от уровня смекалки и умения с этим работать, она может не подняться на верхние строчки.

Но по этой причине, в идеале, это просто должно быть встроено в инфраструктуру. Чтобы это происходило, чтобы этой работой занимались на тех уровнях. Вы по-прежнему не согласны со мной, Уоррен? Нет? Ладно, хорошо. Он вам покажет. Другие вопросы? У нас есть время для еще одного или двух. Нет? Ага, господин Левин здесь. Я так говорю, потому что хорошо знаю Джона.

ДЖОН ЛЕВИН: Нет, на самом деле это просто реклама.

ДЭН ЙОРК: Реклама?

ДЖОН ЛЕВИН: Да. Чуть раньше некоторые из вас упомянули, что может дать квантовая криптография... какое влияние она может оказать на DNSSEC, и по удивительному стечению обстоятельств именно об этом пойдет речь на последнем заседании завтра в Технический день.

ДЭН ЙОРК: Отлично.

ДЖОН ЛЕВИН: Да. Плохая новость в том, что этот парень произносит высокопарные речи, но тут уж ничего не поделаешь.

ДЭН ЙОРК: Ладно, ладно, спасибо, Джон.

УЭС ХАРДЕЙКЕР: Мы полагаем, что это ты, Джон, значит все в порядке.

ДЭН ЙОРК: Ага, хорошо. Хорошо. Итак, Джон выступит завтра с докладом в конце Технического дня. Кстати, если вы новичок, и я вижу несколько участников программы Fellowship, которые сказали, что они новички, завтра будет проведен Технический день, в

рамках которого состоится ряд различных заседаний в одном из этих залов.

Я не знаю, в каком именно, но если вы заглянете в график Технического дня, то найдете там много разных тем, по-моему, от квантовой криптографии до DDoS-атак и других вещей. Я не изучал график на эту неделю, поэтому не знаю. Но в любом случае состоится много полезных заседаний.

УОРРЕН КУМАРИ: В зале 516C.

ДЭН ЙОРК: О, слушайте. Отлично. Мы это выяснили. Мероприятие начнется в 10:30 завтра. Что-то еще? Хорошо. Если нет, благодарю вас за внимание, а также, если вас интересует что-то еще, можете подойти и поговорить с любым из нас, мы будем поблизости еще несколько минут.

Еще раз напомню, что среду в соседнем зале 517C в 1:30 начнется семинар по DNSSEC, на котором мы рассмотрим ряд тем. Вы можете ознакомиться с его повесткой дня, если откроете календарь на сайте и посмотрите там. Так что большое спасибо, и желаю вам с пользой провести эту неделю в ICANN.

[КОНЕЦ СТЕНОГРАММЫ]