БАРСЕЛОНА – DNSSEC для всех: Руководство для начинающих
Воскресенье, 21 октября 2018 года – 15:15 – 16:45 по CEST
ICANN63 | Барселона, Испания

УЭС ХАРДЕЙКЕР (WES HARDAKER): Сделает весь мир безопасным, если вы используете и включите его. Мы собираемся изложить материал в форме рассказа. Давайте начнем с возникновения DNSSEC в 5000 году до н.э., что было довольно-таки давно. Начало DNSSEC уже было положено даже до появления интернета.

Позвольте представить вам Угвину. Она живет на краю Большого Каньона. Для тех, кто не знаком с Большим Каньоном, это гигантская пропасть посередине Соединенных Штатов.

Это Ог. Он живет в пещере на другой стороне Большого Каньона. Путь вниз и путь вокруг очень длинный, поэтому они редко могут поговорить друг с другом. Я проделал этот путь. Подъем с одной стороны на другую занимает два или три дня.

Во время одного из редких визитов они обратили внимание на дым, идущий от костра Ога. Вскоре они регулярно переговаривались при помощи дымовых сигналов по протоколу UDP. Так продолжалось до тех пор, пока однажды подлый пещерный человек Каминский не перебрался поближе к жилищу Ога и не начал тоже посылать дымовые сигналы. Для тех, кто не знает, Каминский — это фамилия человека, который

на самом деле обнаружил весьма серьезную уязвимость в DNS.

Теперь Угвина пребывает в полном замешательстве. Она не знает, каким дымовым сигналам можно доверять. Какие из них, приходящие с действительно большого расстояния, она должна читать, не имея бинокля, чтобы идентифицировать того, кто их посылает?

Поэтому Угвина спустилась в каньон, чтобы попытаться разобраться во всем этом беспорядке. Угвина и Ог обратились за помощью к мудрым старцам деревни. Пещерный человек Диффи подумал, что, возможно, у него есть хитрая идея. Для тех, кто не знает, Диффи был одним из тех, кто создал шифрование с открытым ключом, ставшее сегодня основой большинства криптографических систем интернета.

В мгновение ока пещерный человек Диффи вскочил и бросился бегом в пещеру Ога. В самом дальнем углу он нашел кучу песка странного цвета, которую нигде нельзя было найти, кроме пещеры Ога. Схватив горстку, он выскочил наружу и бросил немного волшебного песка в огонь, который превратился в изумительный голубой дым.

Теперь Угвина и Ог были снова счастливы и болтали в безопасности, зная, что никто не сможет вмешиваться в их разговоры, поскольку только у Ога был волшебный песок.

Таково введение в DNSSEC в форме забавной схемы. Давайте вернемся немного к DNS, поскольку эта система работает, в известной мере, аналогично дымовым сигналам.

В системе DNS существует три структуры, или, как некоторым людям нравится их называть, иерархии. На верхнем уровне находится корень. Затем на уровне ниже находятся все TLD. Это включает ccTLD, gTLD и новые TLD. Затем уровнем ниже каждого из них находятся точки регистрации, где происходят различные вещи.

Теперь я собираюсь обратить ваше внимание на место посередине внизу, где находится «bigbank.com». Мы будем возвращаться к этому несколько раз. Корень делегирует информацию «com» серверам «com», а сервера «com» делегируют «bigbank» их серверам.

Резолвер не знает все дерево целиком, когда он пытается ответить на ваш запрос, где, возможно находится www.bigbank.com. Он должен начать с верхнего уровня. Но он знает, где находится корневая зона, и он может пройти по иерархии DNS, чтобы ее найти.

Каждый уровень в этой иерархии, как я сказал, ссылается на следующий резолвер. Резолвер может просто следовать по всей цепочке вниз до конца, пока не будет получен ответ на вопрос.

Резолвер сохраняет в кэш всю информацию для будущего использования. Поэтому, если он действительно знает эту информацию, он может ответить вам намного быстрее, поскольку он, по возможности, сохраняет информацию в кэше.

Однако в DNS имеется проблема. Она создана без использования какого-либо средства безопасности. Подобно

дымовым сигналам, DNS не содержит в себе системы безопасности. По наивности она предполагает, что все всегда правильно. Имена можно легко подделать, и поскольку информация в кэше хранится длительное время, если в кэш попадает неправильный ответ, он запоминает надолго также этот неправильный ответ.

Но поскольку забавные схемы недостаточно забавны, нам необходимо разыграть сценку. Это будет очень забавно. Кто из вас видел эту сценку?

Пара человек. Ладно. Остальным из вас будет на что посмотреть. Тем из вас, кто видел ее раньше, придется потерпеть и посмотреть ее снова.

Хорошо. Если есть добровольные актеры, пожалуйста, встаньте.

Итак, у нас есть несколько актеров. У нас есть обычный пользователь, пользователь Джо. Поднимите руки, пожалуйста. Он будет пользователем в этом сценарии, и он собирается сегодня осуществить некоторую банковскую операцию. У нас есть корневой представитель, который представляет корень дерева DNS. У нас есть интернет-провайдер, который знает, где находится корень. У нас есть «.com», и у нас есть «bigbank.com». Фред, на самом деле, лучше прямо здесь. Итак, пусть они берутся за дело и начинают. Прошу вас.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: [Когда] включится свет, алло, алло.

УЭС ХАРДЕЙКЕР: Да, вот так. Хорошо, оба работают. Здесь, Тим. У Расса есть вопросы.

ТИМ: Класс! У меня много денег. Я хочу положить их на депозит в банке. Мне нужно зайти на www.bigbank.com, чтобы положить деньги на депозит в банке.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Что ж, я не знаю где это, поэтому я собираюсь найти это для вас. Итак, я начну с корня. Привет, вы знаете, где находится www.bigbank.com?

ФРЕД БЕЙКЕР (FRED BAKER): Вот это да. Не имею понятия. Однако, у меня к вам предложение! Спросите «.com», он может знать. Он находится по адресу 1.1.1.

ТИМ: Отлично. Я попробую спросить там.

УЭС ХАРДЕЙКЕР: [Неразборчиво]. Ну вот. Извините.

ТИМ: Мне сказали спросить у вас. Вы знаете, где находится www.bigbank.com?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Отличный вопрос. Я «.com». Я нахожусь по адресу 1.1.1. Спасибо, что посетили меня. Я могу сказать вам, где находится «bigbank». Ага, вот. «Bigbank» находится по адресу 2.2.2. Хотите перейти туда?

ТИМ: Спасибо. Я должен знать, где находится www.bigbank.com.

РАСС МАНДИ (RUSS MUNDY): Спасибо, что спросили, мистер интернет-провайдер. Я в самом деле могу сказать, где именно находится www.bigbank.com. Он находится по адресу 2.2.2.3.

ТИМ: Спасибо. «Bigbank.com» находится по адресу 2.2.2.3. Замечательно! Теперь я пойду и положу свои деньги в банк! Спасибо, «Bigbank»!

ФРЕД БЕЙКЕР: Не знаю. Он должен поблагодарить вас.

УЭС ХАРДЕЙКЕР: Хорошо. Всем спасибо. Не расходитесь, через минуту вы опять нам понадобитесь.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Не бросайте основную работу!

УЭС ХАРДЕЙКЕР: Это их основная работа. Итак, Угвина, резолвер, разговаривает с Огом, сервером, аналогично тому, что вы только что видели. Они общались между собой при помощи дымовых сигналов. Проблемы не было. Никто не вмешивался.

Далее мы собираемся посмотреть, что случится, возможно, если что-то пойдет не так. Можно повторить представление?

ТИМ: Класс! Теперь у меня есть один миллион долларов, и мне нужно открыть депозит в банке. Мне нужно перейти на www.bigbank.com, поэтому я собираюсь пойти к моему интернет-провайдеру и спросить: «Как мне попасть наwww.bigbank.com?»

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Я не знаю, но попробую. Здравствуйте. Вы знаете, где находится www.bigbank.com?

ФРЕД БЕЙКЕР: Что ж, я корень, и я действительно не знаю об этом. Но вы можете спросить у «.com». Он может знать. Он находится по адресу 1.1.1.1.

ТИМ: Хорошо. Спасибо. Здравствуйте, «.com». Вы знаете, где находится www.bigbank.com?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Добро пожаловать! Я «.com». Я скажу вам, где находится «bigbank». «Bigbank.com» находится по адресу 2.2.2.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: .2.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: .2.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: IPv3?

ТИМ: Спасибо. Здравствуйте

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Здравствуйте.

ТИМ: Здравствуйте. Вы знаете, где находится www.bigbank.com?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Конечно. Он находится по адресу 6.6.6.6.

ТИМ: Отлично. Спасибо. [Неразборчиво]

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Ну вот. www.bigbank.com находится по адресу 6.6.6.6.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: О, Боже! Спасибо! Хочу положить свои деньги в банк!

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Спасибо.

УЭС ХАРДЕЙКЕР: Хорошо. Еще раз спасибо. Итак, главный вопрос в том, как избавиться от такого ужасного сеанса с Доктором Зло, контролирующим каждый банк.

Поэтому резолвер Угвина находится в замешательстве. Вы только что видели эту ситуацию. Есть два сигнала. Она не знает, какому из них можно доверять. Фактически в DNS вы доверяете тому из них, который вернулся первым, или так было, по крайней мере, до тех пор, пока не появились DNSSEC.

Итак, давайте вернемся назад к той же схеме, если два разных сервера дают вам два разных ответа, вы можете получить ответ о «bigbank.com» из двух разных мест, и вы не знаете, какому из них доверять. Так на схеме вверху есть один голубой и один красный. Вам остается только гадать, какой из ответов является правильным.

Но DNSSEC фактически добавляют безопасность в DNS и используют для этого цифровые подписи. Это обеспечивает вам две базовые вещи: что информация не была искажена, и что она поступила из правильного места. Поэтому не имеет значения, в скольких местах она была сохранена, не имеет значения, что она находится в кэше; она не была искажена, и вы знаете, откуда она поступила.

Сами ключи и подписи также хранятся в DNS. Поскольку DNS имеет систему поиска, ключи могут быть легко найдены, также как и подписи, в любой другой день, пока у вас есть место, с которого начать.

Таким образом, на высоком уровне концепция DNSSEC состоит в том, чтобы резолвер знал не просто, где находится корневой сервер, но также знал ключ корневого сервера. До тех пор, пока он знает эти два элемента начальной информации, он может проверить все остальное дерево.

Это делается путем построения цепочки доверия. Каждый уровень подписывает следующий и данные, находящиеся на его собственном уровне, до тех пор, пока не будет выстроена вся цепочка вниз до необходимого вам ответа.

Таким образом, наконец, резолвер интернет-провайдера может фактически определить, какая из этих двух записей нижнего уровня о «bigbank» является правильной, правильная — это голубая, а знаком X обозначена неправильная.

Итак, давайте посмотрим, что фактически происходит, когда в игру вступает DNSSEC. Есть несколько моментов, о которых мы хотели бы сегодня рассказать. Сейчас вы видите,что у нас есть эти маленькие знаки отличия. Они обозначают цифровые подписи. Каждый из этих трех серверов DNS должен иметь такой знак отличия, а затем интернет-провайдер должен иметь совпадающий знак отличия, чтобы убедиться, что он может проверить, что говорит с правильным субъектом. Берите это в свои руки.

ТИМ: Класс! Я хочу сделать другой вклад в банке. Мне нужно зайти на www.bigbank.com, чтобы сделать этот вклад в банке.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Хорошо. Я поищу его для вас.

Привет, корень. Вы можете сказать мне, где находится www.bigbank.com?

ФРЕД БЕЙКЕР: Что ж, хорошо. Я корень, и я могу доказать подлинность моих заявлений. Но я не имею понятия, где находится «bigbank». Вы можете спросить «.com». Он находится по адресу 1.1.1.1.

ТИМ: Спасибо. Здравствуйте, «.com». Вы можете сказать мне, где находится www.bigbank.com?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Привет, интернет-провайдер. Я «.com». Проверь, что я «.com». Точно! Это я! Отлично. Позвольте просто сказать вам, где находится «bigbank». «Bigbank» находится по адресу 2.2.2.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: .2.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: .2.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Привет, «bigbank». Вы можете сказать мне, где находится www.bigbank.com?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Разумеется. Но у меня нет подписи, поэтому вы должны отклонить меня.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: О, нет! До свидания. Привет, «bigbank». Вы можете сказать мне, где находится www.bigbank.com?

РАСС МАНДИ: На самом деле www.bigbank.com находится по адресу 2.2.2.3.

ТИМ: Спасибо. Могу я проверить вашу подпись?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Дзинь!

НЕПРЕДСТАВИВШИЙСЯ МУЖЧИНА: www.bigbank.com находится по адресу 2.2.2.3 и он подписан.

ТИМ: Отлично! Теперь я пойду и положу свои деньги в банк безопасно.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Деньгиии!

УЭС ХАРДЕЙКЕР: Хорошо. Прошу аплодисменты для заключительного действия нашей состоящей из трех частей пьесы. Я знаю, что нам необходим маленький мало что знающий человек, чтобы

проверить эти вещи, когда они зазвучат вместе в будущем. Это было бы замечательно.

Хорошо. Что ж, как бы это не было забавно, это действительно то, что происходит в системе DNS и уже произошло с DNSSEC. Конечно, это немного сложнее. Но в реальности резолверы на самом деле образуют цепочку до самого низкого уровня от корня. Они проходят через следующий TLD, каким бы он не был, и через множество уровней, чтобы получить окончательный ответ.

И иногда эти уровни могут уходить совсем глубоко, но до тех пор, пока DNSSEC защищают эту цепочку вплоть до самого нижнего уровня, вы в конце концов получаете защищенный ответ, точно так же, как голубой дым защищает резолвер посредством проверки, что Ог на самом деле отправил реальное сообщение.

А сейчас я передаю слово моему коллеге Рассу Манди. Позвольте сначала представиться самому. Итак, я – Уэс Хардейкер из университета Южной Калифорнии, институт информатики. Расс Манди из компании Parsons, и он более подробно объяснит, почему вам необходимы DNSSEC.

РАСС МАНДИ: Спасибо, Уэс. Также спасибо большое нашим другим актерам, которые были с нами сегодня. Это было очень здорово делать с новым составом участников, поскольку это был свежий состав. Спасибо всем за то, что присоединились к нам. Спасибо вам за это, еще раз.

Итак, вот аспект заседания «DNSSEC для всех», цель которого — помочь людям подумать о внутренних причинах, почему любой, будь то конечный пользователь, интернет-провайдер или оператор авторитативного сервера, должен захотеть выполнить проверку подлинности DNSSEC, за исключением вклинившегося посередине Доктора Зло, поскольку основная задача, для которой создан DNSSEC, заключается в том, чтобы противостоять этому.

Поэтому, когда вы подумаете об этом, когда мы поговорим об этом в смысле DNS, DNS не пересылает деньги между пользователем и банком туда и обратно. Для этого есть специальные приложения.

Поэтому, когда злоумышленники атакуют DNS и подменяют информацию, почти во всех случаях они пытаются сделать это потому, что другие приложения, другие функциональные средства делают это через интернет.

Поэтому, если ваш DNS работает неправильно, то, будь то браузер, электронная почта или обмен сообщениями какого-либо вида, они тоже не будут работать правильно. Вы не попадете в те места, куда рассчитывали или надеялись попасть.

В этом и заключается фундаментальный вопрос, почему вы хотите получить правильный DNS: он должен быть правильным, чтобы остальные приложения, которые его используют, также могли правильно работать.

Этот перехват страницы интернет-банка, который намеревалась продемонстрировать наша маленькая сценка, фактически нацелен на то, чтобы заставить эти экземпляры прикладных программ общаться с некоторым местом, с которым пользователь ни в коем случае не намерен был общаться.

Со временем появилось множество приложений, которые были атакованы, когда атака начиналась с DNS. Фактически некоторые атаки, которые начинались с DNS, заканчивались созданием вредоносного кода, использующего два, три и иногда четыре других протокола. Начиная с DNS, преступники получают информацию DNS, которая нужна, чтобы перейти в определенное другое место, где они могут обмануть людей, которых они стараются обмануть.

Одно время – я думаю, это ушло из интернета, я не находил этого в последнюю пару лет – в университетах был специальный курс – фактически, два в двух разных университетах – которые требовали от своих студентов по компьютерным специальностям написать реальное хакерское программное средство для атаки на DNS. Это дает пример, как относительно легко это было сделать. В интернете можно найти программы для атаки на DNS.

Однако, проблема с университетскими курсами, судя по информации на их сайтах, в том, что в них ничего нет об этической стороне вопроса и реальном использовании, даже если профессор требует сделать это, как часть их курсовой работы.

Поэтому неясно, как много существует программ для перехвата страницы в интернете, но они есть, легко доступны или могут быть легко написаны людьми, интересующимися программированием.

Поэтому, когда пользователи используют DNSSEC, как Уэс сказал ранее и проиллюстрировал в виде сценки, идея заключается в использовании криптографической информации в обычной структуре DNS, поскольку DNSSEC является частью DNS. Они полностью интегрированы в стандарт DNS.

Когда получатель ответа получает подписанный DNSSEC ответ, независимо от того, где произошла проверка, в локальном валидирующем резолвере или непосредственно в самом приложении, основная идея в том, что пользователь, пославший запрос на информацию, может получить криптографическую гарантию, что он пришел, откуда предполагалось, и что по дороге он не изменился.

Фактически это позволяет вам быть уверенными в том, что полученные вами ответы содержат информацию, которую вы можете использовать, независимо от того, делаете вы запрос страницы сайта, обращаетесь к серверу электронной почты, разговариваете друг с другом или это сеанс Jabber или Twitter или еще что-либо подобное.

Как еще один упрощенный пример, как работает обмен информацией DNS, здесь показан пользователь Джо, делающий свой запрос. Я не изменил числа, чтобы они соответствовали указанным на наших футболках. Прошу

прощения. Итак, пользователь Джо отправляет запрос своему интернет-провайдеру, рекурсивному серверу имен. Рекурсивный сервер имен затем посылает запрос авторитативному серверу имен о месте, в которое хочет перейти пользователь Джо. Сервер имен получает ответ от авторитативного сервера имен и затем возвращает этот ответ пользователю Джо. Это фактически первый сценарий, который вы видели во время представления сценки.

Следующий после этого – о, простите. После того как ответ вернулся, начинается фактический обмен данными между самими приложениями. Пользователь Джо затем общается с веб-сервером и выполняет здесь свою работу.

Теперь, когда в игру вступает группа подписанных DNSSEC зон и валидирующие резолверы, вы можете откорректировать сайты так, чтобы они предоставляли индикаторы того, что фактически происходит обмен правильной информацией. В данное время огромное большинство сайтов, которые могут использовать DNSSEC, не имеют таких индикаторов, но на это у нас есть еще несколько лет, просто чтобы люди смогли действительно увидеть, что могут получить цепочку DNSSEC при обмене информацией. Если в основе этого у вас нет цепочки DNSSEC, вы делаете другие индикаторы, когда она возвращается.

Таким образом, частью оптимизации сайта будет введение индикатора атаки. Атака та же, как и у Доктора Зло, который следит за тем, когда отправляется запрос. Рекурсивный сервер запрашивает авторитативный сервер, но еще до того, как

авторитативный сервер получит этот запрос, Доктор Зло уже дал ответ пользователю Джо. Теперь пользователь Джо переходит в неправильное место. Он заходит на сайт Доктора Зло.

В это время стандартные запросы DNS только покинули сеть, но машина пользователя Джо уже имеет ответ, поэтому она игнорирует правильный ответ и отправляет указание приложению подключиться к сайту Доктора Зло.

Он никогда не получит эту информацию до тех пор, пока в игру не вступит DNSSEC. Когда в игру вступает DNSSEC, пользователь Джо отклонит плохие ответы, которые вы видели в сценке, и перейдет на правильный сайт.

Итак.

Теперь, в этом случае, оснащенный сайт содержит правильную информацию, и, хотя мы делаем это на этом сайте, мы оснастили его таким образом, чтобы демонстрировать переход к другому сайту.

Это то, что получит валидирующий резолвер, что вы видите отмеченным зеленым флагом. Первая запись: «.org разделяет рекомендацию Comcast DNSSEC для интернет-провайдеров».” Но невалидирующий резолвер будет видеть, как говорит Стив Крокер, «DNSSEC не устранит всемирного голода» как первую запись. Вы видите, что следующий выдал такую страницу: «.org разделяет рекомендацию Comcast DNSSEC для интернет-провайдеров».

Что существенно, информация была вставлена в страницу сайта таким образом, что пользователь, если не увидит треугольник вверху, не будет иметь не малейшего намека на то, что этот сайт подвергся атаке DNS по подмене страницы, атаке подмены содержимого, направленной против него.

Вы можете сказать: «Здесь нет множества разрешений DNS, не так ли?» Что ж, это было около десяти лет назад, когда мы измеряли CNN. Около пяти лет назад. Для одной страницы содержимого от CNN.org это заняло такое количество запросов DNS. Это множество запросов.

Важная информация о DNS и DNSSEC – критическая часть – что важно, это сами данные зоны.

Другая иллюстрация, которая показывает, как этот процесс работает и где должны произойти измерения. Вы видите дальше слева, что информация о зоне помещена в авторитативные сервера. Она затем доступна в DNS. Рекурсивные сервера, которые вы видите в центре, общаются с авторитативными серверами в ответ на запросы, которые они получают от клиентов.

Клиент – как вы видите, .1, первая стрелка, номер один. Номер два, рекурсивный запрашивает авторитативный. Номер три, авторитативный отвечает рекурсивному. И затем, рекурсивный отвечает клиенту.

Когда вы реализуете DNSSEC, существует еще один этап, через который вы проходите, где вы добавляете дополнительные данные и дополнительную

функциональность. Реализация вашей части DNS, за работу или обслуживание которой вы отвечаете – это зависит где вы находитесь во всей структуре DNS, это то, что вам необходимо сделать. Службы, которые сильно и глубоко связаны с DNS, возможно, захотят выполнить все эти действия сами, поскольку они уже имеют компетентный в DNS персонал.

Если размер и сложность того, что вы делаете, действительно тесно связаны с DNS – вы можете видеть некоторые примеры здесь: [арх]-регистратура, большое предприятие, мероприятия в некритических зонах DNS, которые легко работают, небольшие и легкие в управлении – они, возможно, захотят сделать многое из этого сами, еще раз напомню, что защита самих данных зоны DNS является критическим фактором.

Так, на последней иллюстрации, там где необходимо добавить информацию зоны, чтобы реализовать функции подписи и валидации DNSSEC – подписанная информация вводится в систему владельцем авторитативного сервера. После этого она доступна для включения в ответы. Затем валидирующий рекурсивный сервер, который вы можете видеть внизу, осуществляет фактическую валидацию, чтобы сказать: «Да. Это верно, криптографически».

Итак, если существующая организация, которую вы ищете, работает и выполняет множество операций и функций DNS и сильно ориентирована на DNS, то вы можете выполнить DNSSEC изнутри, сделать это сами.

Если деятельность мало или минимально использует DNS в смысле основной функциональности, велика вероятность, что существует отдел ИТ, или возможно использовать стороннего исполнителя каким-либо образом. Вы можете спросить любого из провайдеров, либо свой отдел ИТ или своих поставщиков сторонних услуг, могут ли они осуществить DNSSEC. Если нет, скажите, «Вы должны научиться делать это, я планирую заняться глобальной деятельностью» поскольку, фактически, сегодня в сфере DNSSEC имеется достаточно людей, которые могут стать достаточно реальной возможностью. Вы можете решить использовать поставщиков, чтобы сделать DNSSEC.

Это конец главной части презентации. Мы намерены провести очень открытое совещание в форме вопросов и ответов. Мы будем – да. Я передаю право слова обратно Уэсу и пусть он будет главным, кто будет давать слово другим, поскольку мы оба во многом не только игроки в области DNSSEC в этом зале, но мы также обладаем весьма большими знаниями о DNSSEC.

Итак, пожалуйста, задавайте свои вопросы. Мы готовы предоставить все, что вы захотите узнать.

УЭС ХАРДЕЙКЕР: Хорошо. Итак, DNSSEC еще нет – как на счет этого? Нет. Да. Включите микрофон сзади.

Проверка, проверка, проверка, проверка, проверка, проверка. Проверка – да, вот так. Хорошо. Хорошо. А этот работает? Ладно. Так, у нас есть два. Я могу использовать оба.

Итак, DNSSEC — это не просто. Там много сложностей. Мы гарантируем, что в зале есть вопросы. Поэтому мы отвели большую часть оставшегося времени только для ответов на вопросы. В зале присутствует множество экспертов, которые помогали создать DNSSEC, достаточно много, если у вас есть вопрос, мы можем на него ответить.

У кого-нибудь есть вопросы? Поднимите руку, и мы передадим вам микрофон.

ТАН НГУЙЕН (THANH NGUYEN): Здравствуйте. Я Тан Нгуйен из Вьетнама. Спасибо за презентацию. Она очень полезная и содержит множество информации [неразборчиво] DNS.

Я увидел множество [неразборчиво] DNSSEC, когда развертывал [неразборчиво], чтобы защитить ccTLD и gTLD, но я думаю, когда, фактически, в реализовываете это в DNSSEC, вам необходимо задуматься о [неразборчиво] [к некоторым вызовам]. Это подобно тому, как вы [неразборчиво] DNSSEC, подписание DNS, подписание зоны и некоторые этапы, о которых я не помню.

Но, на основании этого этапа, я думаю, хакеры или [неразборчиво] могут атаковать посредством DDoS, или они могут, на основе уязвимости DNSSEC, выглядеть [подобно] синхронизации времени DNSSEC, поскольку это занимает время, чтобы ввести – прежде всего, вы вводите некоторые дополнительные пункты в систему DNS, но это увеличивает

время ожидания ответа. Так, хакер может, на основе этой уязвимости, атаковать этот пробел в системе DNSSEC.

Есть ли у вас способ решения этой проблемы?

УЭС ХАРДЕЙКЕР: Я думаю, вы задали пару вопросов. Во-первых, вы спросили, существует ли длительная задержка при ожидании запрошенных данных пользователями, правильно? Поскольку, если вы запрашиваете больше данных, это немного замедляет поиск DNS. Это так, немного, не … пользователей больше заботят те, которые используются мгновенными приложениями, где им необходимо выполнить множество поисков DNS, и они должны просмотреть все эти ответы, и как быстро. Поэтому обычно это использование браузера и подобные вещи.

Помните, поскольку есть кэш, это может замедлить только один поиск, а все остальные после этого, включая записи безопасности, попадут в кэш.

Таким образом, начальный поиск может быть на несколько миллисекунд медленнее, но после этого он попадет в кэш. Таким образом, обычно, если задержка заметна, ее замечает единожды только один пользователь одного интернет-провайдера, переходя на сайт.

Я полагаю, другой заданный вами вопрос касается того, что записи DNSSEC очень большие и это фактически может быть использовано в атаке с лавинообразным умножением данных.

Если вы зададите вопрос серверу DNS и получили больший ответ, если вы подделаете, откуда он пришел, то ответ может прийти к неправильному субъекту.

Типовым решением в настоящее время является так называемое ограничение быстроты отклика, поэтому большинство серверов DNS сегодня не позволят вам запрашивать так много записей одновременно. Если вы попробуете и запросите 100 записей все за одну секунду, значит вы делаете что-то неправильное, и я перестану вам отвечать.

Вот типовое решение, которое работает сегодня. Я фактически отвечаю за работу одного из корневых серверов. В момент, когда мы его включили, вдруг все сразу, мы получили намного меньше запросов и такая вещь случилась. Это было много лет назад. Больше такой проблемы почти не существует.

Эндрю, я думаю, что –

ЭНДРЮ ФРЕЙЗЕР: Да. Уоррен хочет что-то еще добавить по этому поводу?

УОРРЕН КУМАРИ: Нет.

ЭНДРЮ ФРЕЙЗЕР: Нет? Хорошо.

УЭС ХАРДЕЙКЕР: Хорошо.

УОРРЕН КУМАРИ: [неразборчиво] атакующий посылает запрос [неразборчиво].

УЭС ХАРДЕЙКЕР: Вы хотите пройти и сесть здесь, тоже? Любые эксперты в зале приглашаются пройти и сесть за стол чтобы … продолжить.

ЭБЕРХАРД БЛОЧЕР (EBERHARD BLOCHER): Здравствуйте. Меня зовут Эберхард Блочер я из Германии. Я не эксперт. Я совершенно простой человек.

УЭС ХАРДЕЙКЕР: Все в порядке.

ЭБЕРХАРД БЛОЧЕР: [Неразборчиво]. У меня вопрос, связанный с давней историей. Я знаю, что DNSSEC существует уже долгое время, я думаю, уже лет десять. Скажите кто-нибудь, Стив Крокер в основном создал это, или это было создано коллективом людей.

Сегодня, как я понимаю, по прошествии большого количества времени, теперь мы оказались в новой ситуации. В этом году все мои конечные пользователи... Я предоставляю услуги домена по запросу на шифрование SSL. Теперь мы используем Let’s Encrypt, что бесплатно. В основном это еще один способ защиты сайтов.

Как я понимаю, сертификат SSL связан только с одним доменным именем, поэтому вопрос в том, нужен ли нам все еще DNSSEC, или какая разница между шифрованием сайтов DNSSEC и SSL?

Если я выполняю шифрование моего сайта при помощи сертификата SSL, зачем мне все еще нужны DNSSEC?

Второй вопрос, возможно – я просматривал статистику, и я знаю, что многие регистраторы предоставляют данные о том, как много доменов имеют шифрование DNSSEC. Существуют регистратуры, которые имеют очень мало проникновений. Почему это так? И снова тот-же вопрос: нужны ли все еще DNSSEC?

УЭС ХАРДЕЙКЕР: Отличный вопрос. Одна из самых трудных вещей в отношении безопасности интернета состоит в том, что вы не можете просто решить одну проблему, поскольку фактически оказывается, что все работает на множестве уровней.

Так, например, вы осуществляете поиск DNS – скажем, переходите на защищенный SSL сайт. Если вы попали сюда, вы знаете, что это правильный сайт. Дело в том, что DNS вступает в игру задолго до этого, и это фактически перенаправляет вас на совершенно неправильное место.

С этим связан ряд проблем. Первое, они могут просто отправить вас в неверное место, и вы никогда не попадете на правильный сайт. Маршрутизация имеет эту же проблему.

Поэтому, если не защитить уровень маршрутизации и инфраструктуру маршрутизации – так, реальность в том, что интернет построен на стеке. Действительно, каждый уровень в этом стеке должен быть защищен, чтобы полностью защитить конечного пользователя.

Таким образом, да, DNSSEC остаются необходимыми.

Вы хотите поговорить об истории, создании и возможно развертывании DNSSEC и о Стиве Крокере? Здесь присутствует много людей, внесших вклад в DNSSEC. Стив определенно помог, но …

РАСС МАНДИ: Ну да. Разработка, реализация и развертывание DNSSEC имеют давнюю историю. Как сказал Вес, ее целью было гарантировать, чтобы при использовании DNS пользователь получал правильный ответ.

Как сейчас это используется в зависимости от приложения [независимо.] Фактически главные работы начались в 1993 году, когда усилия были сосредоточены на разработке и планировании DNSSEC. Мы собирались и обменивались информацией. Стив Крокер был одним из людей, участвовавших в этих собраниях. Так случилось, что я тоже был одним из этих людей.

Но многое было переделано впоследствии, поскольку это был первый случай вообще, когда фактически на лету средства безопасности были введены в работающий протокол. Две

первые разработки имели множество серьезных проблем. Третья оказалась верной.

В 2010 г. была подписана сама корневая зона. После этого были подписаны пара TLD.

Так что да, множество людей сделали большой вклад. Над этим очень серьезно трудилось множество организаций. Но в итоге мы указали, чтобы предотвратить то, что случилось на этом слайде, используете вы сертификат SSL или нет, поскольку существует достаточно проблем с подлинностью сертификата, ошибочным или неверным выпуском сертификатов, и вы можете получить, фактически, именно этот результат, включая проблемный CA на сайте, а пользователь по прежнему получит подписанный SSL сайт.

УЭС ХАРДЕЙКЕР: Следует еще отметить, что просмотр сайтов — это не единственный механизм, который нуждается в защите поиска имен. Электронная почта — это другой хороший пример проблемы, которую невозможно фактически решить при помощи традиционной системы сертификатов.

Обо всем этом будет немного говориться в среду на семинаре по DNSSEC, о чем мы расскажем позже, и все приглашаются его посетить. Это программа на целый день, подробнее о DNSSEC.

Одна из тем обсуждения о том, почему DNSSEC является фактически единственным имеющимся решением для защиты

серверов интернета от атаки посредника, похищения вашей электронной почты и перенаправления в неправильное место. Обычные сертификаты TLS здесь не помогут по причине, которую я объясню в этот день. Это сложно.

Итак, Эндрю?

АХМАД АЛСАДЕХ (AHMAD ALSADEH): Меня зовут Ахмад Алсадех. Я участник программы Fellowship ICANN. Хочу спросить, почему это не развернуто также широко, как DNS. Почему всем и каждому не развернуть DNSSEC? Это первый вопрос.

Мой второй вопрос, как вы полагаете, новая технология, такая как блокчейн, может стать обещающим решением для безопасности DNS? Спасибо.

УЭС ХАРДЕЙКЕР: Итак каждый из двух по очереди. Один, другой участник, уже интересовался информацией о том, почему некоторые регистратуры имеют большее развертывание и все такое прочее. Это действительно хороший вопрос. Каждый регион в мире, похоже, имеет разный уровень развертывания и все такое прочее.

Некоторые TLD – в частности, Швеция, Чешская Республика и некоторые другие – фактически предоставили вам финансовые стимулы для подписания вашей зоны. Поэтому они имеют гораздо более высокие поступления и все такое прочее.

Многие ли последовали, есть ли стимулы? Имеется местный стимул, фактически подталкивающий компании к использованию этой технологии? Поэтому темпы принятия в общем растут медленно.

Но мы снова обращаем внимание, если вы придете в среду, я действительно располагаю цифрами статистики, и смогу фактически подтянуть – хорошо, это сейчас трудно сделать. В настоящее время подписаны миллионы зон. Даже хотя процент низок, поскольку доменов очень много, развернуты миллионы и миллионы. Примерно 85% TLD подписаны, я думаю, на данный момент. Это так, но переключение во всем мире — это долгий процесс.

РАСС МАНДИ: Одна из причин, если разрешите добавить, — это не только TLD и домены второго уровня. Конечные пользователи, предприятия, обычно активно не требуют DNSSEC, поскольку большинство времени они просто не осознают, как это важно для их деятельности.

Но в последние пять лет правительство США – в соответствии с требованием подписания всех доменов .gov – и некоторые другие правительства заняли аналогичную позицию. Мне наиболее известно положение в США.

Теперь они также требуют, чтобы валидация выполнялась на всех их доменах. Таким образом, к этому подталкиваются конечные предприятия в некоторых организациях. Например, компания в которой я работаю, Parsons – parsons.com –

является подписанным доменом и работает по этому принципу.

Поэтому процесс идет, поощряя людей спрашивать об этом. Поэтому вы видите в нескольких местах высказывание «Спросите своего интернет-провайдера, собирается ли он обеспечить службу DNS средствами DNSSEC».

УЭС ХАРДЕЙКЕР: Многим современным регистраторам и владельцам регистрации достаточно просто нажать кнопку. Если вы собираетесь разместить DNS своего узла у них, все что вам нужно сделать, — это нажать кнопку, и ваша зона будет подписана. Так что это очень просто.

Но многим людям, имеющим собственный DNS, потребуются затраты, связанные с развертыванием и работой механизма защиты. Не имеет значения, будет это сертификат TLS, DNSSEC или что-то другое. Вам надо научиться. Надо собраться и сделать это. Сегодня есть множество инструментов, которые помогут сделать это достаточно легко, но десяти лет уже не будет. На этот раз это более странно.

Есть еще вопросы? Да?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Хола. Мой вопрос касается опубликованного комментария о последнем обновлении ключа на прошлой неделе.

Мой вопрос, планируется ли добавить в [браузер подпись DNSSEC], в домен?

УЭС ХАРДЕЙКЕР: Обновление ключа произошло на прошлой неделе, и это вообще первый случай. Все прошло достаточно гладко. Все оказалось в порядке.

Вы хотите поговорить от этом, Джон?

ДЖОН ЛЕВИН (JOHN LEVINE): Есть следующий вопрос.

УЭС ХАРДЕЙКЕР: Хорошо. У вас следующий вопрос. Итак, обновление ключа прошло на самом деле очень хорошо. Несколько интернет-провайдеров действительно не изменили свой ключ, но обычно этот ключ необходим не браузеру. Он необходим интернет-провайдеру, как вы видели ранее сегодня. Пользователь Джо, с его браузером, на самом деле фактически не должен что-либо делать. Он даже не должен знать, что появились DNSSEC.

Здесь еще есть и другие проблемы, что случится, если вы в кафе с беспроводным доступом, и ваш интернет-провайдер использует DNSSEC, и вы здесь в безопасности? Это совсем другая программа.

Поскольку обычно только интернет-провайдер действительно должен знать о новых ключах.

Пока ICANN будет продолжать этот процесс в будущем, они будут обновлять их опять, и когда этот день настанет, будет обсуждение, я полагаю, позже на этой неделе, фактически. В течение, возможно, нескольких лет, будет принято решение, как часто мы собираемся продолжать делать это? Должны ли мы делать это таким же образом? Каков наш механизм обновления ключей?

Поэтому еще много должно быть определено на основании извлеченного из этого события опыта, поскольку это было всего неделю или три дня назад.

РАСС МАНДИ: Если можно, Вес, добавлю еще кое-что. Определенно сообщество внесет свои предложения по решению, когда будет следующее обновление ключей. Организация в ICANN – организация CTO – очень заинтересована в получении предложений от сообщества. Так, если у вас есть предложения, идеи или мысли, они определенно хотят их услышать. Чтобы достичь цели, необходимо разработать множество механизмов, подумайте об этом и поделитесь своими мыслями.

УЭС ХАРДЕЙКЕР: Снова напомню, что в среду на семинаре по DNSSEC будет показана презентация по обновлению ключей.

ДЖОН ЛЕВИН: Привет, Уэс. Меня зовут Джон Левин. Я хочу задать вопрос, который задаю всегда, а именно, мой узел DNS насчитывает около 300 зон [неразборчиво]. Для половины этих зон я являюсь реселлером регистратора. Таким образом, я имею фактически непосредственный доступ к регистратору. Для них всех подписи DNSSEC фактически работают.

Для другой половины я сторонний провайдер DNS. С наилучшим [неразборчиво] в мире, на данный момент, для всех других пользователей, единственным субъектом, который может выполнить работу по DNSSEC, является владелец домена, или субъект с учетными данными владельца регистратора. Итак, либо я должен провести своих пользователей через процесс установки записей DS, что является легким для вас и меня, не обязательно для кого-нибудь еще, либо я должен получить учетные данные их регистратора, чего я не хочу.

Думаю, эту проблему необходимо решить либо на уровне регистратора, добавив каким-то образом контакт для обновления DNS, либо что-то исправив в IETF, посредством – ну, вы знаете, определенной автоматической процедуры.

Похоже, прогресса не видно ни в том, ни в другом. Я понимаю, что мой случай не является самым общим, но я считаю, что сторонние провайдеры DNS не являются редким исключением, и нам необходимо это исправить.

УЭС ХАРДЕЙКЕР: Да. Вы правы, эта работа должна быть сделана, особенно для людей, обслуживающих большое количество зон. Я делаю все это вручную, поскольку я тоже обслуживаю свои собственные зоны. И это требует больших усилий. Это должно быть улучшено.

Теперь я хочу рассказать о некоторых вещах, произошедших за последние два года. Первое, некоторые провайдеры создали кнопку, и если вы публикуете свою запись DS, надо просто нажать на ключ, который говорит, «это правильный ключ?», так что вам больше не надо его вставлять. Фактически она выполнит поиск за вас.

Второе, Уоррен Кумэри – вы должны рассказать ему однажды, или [Оливер], кто создал запись CDS, способ автоматического обновления, чтобы обеспечить передачу информации DNS между дочерней зоной и регистратором.

Но, я знаю –

ДЖОН ЛЕВИН: Да, но не устанавливает его. На данный момент только обновляет. [Неразборчиво]

УЭС ХАРДЕЙКЕР: Это спор по поводу прежде всего доверия и аналогичных вещах. Об этом много спорят за последнее время: люди беспокоятся – почему бы вам не выйти вперед, Уоррен? Я должен передать слово Уоррену. Однако сегодня люди говорят фактически о переходе к стадии применения. Наконец я начал

видеть трафик, давайте реализуем это. Кто это реализует? Фактически, пока очень рано, вот о чем речь.

Вы хотите выступить?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Да.

УЭС ХАРДЕЙКЕР: Пусть первым будет Уоррен.

УОРРЕН КУМАРИ: Нет, вы первый.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Да. Я просто хочу отметить, что сегодня есть две или три страны, где это уже работает (введение записей CDS): Чешская Республика, Швейцария и Лихтенштейн. Если ваш домен в этих странах и вы просто показываете CDS в вашей зоне, это берет регистратура, а затем устанавливается [вся] цепочка.

По крайней мере здесь сделаны некоторые попытки и, конечно, это демонстрирует необходимость глобальной инициативы, поддерживаемой «.com». Возможно, это только начало, и нам нужно кое-чему научиться на этом. Думаю, что в среду на семинаре DNSSEC об этом будет сделана презентация. Я приглашаю вас присоединиться. [Неразборчиво].

УЭС ХАРДЕЙКЕР: Много работы необходимо проделать, но хорошая новость в том, что есть движение вперед, я думаю, на данный момент. Да, это панельная дискуссия на среду, как он и сказал.

РУДОЛЬФ ДАНИЕЛЬ (RUDOLPH DANIEL): Здравствуйте. Добрый день. Меня зовут Рудольф Даниель. Я участник программы Fellowship ICANN.

УЭС ХАРДЕЙКЕР: Добро пожаловать!

РУДОЛЬФ ДАНИЕЛЬ: Не знаю, относится ли это к делу, но недавно упоминалось про обновление ключа KSK. Я хотел бы знать – до сих пор это было успешно, старые ключи удалены, или они все еще работают?

УЭС ХАРДЕЙКЕР: Хороший вопрос. Два момента. До сих пор это было успешно. TTL в данных (время существования) позволяло оставаться в кэш только два дня. Теперь они удаляются через десять дней? Я точно не помню. Ага, да. Я могу подсчитать. Десять дней. 21 минус 11. Удаление через десять дней, это значит, что так долго DNS-резолвер должен хранить их. Они должны обновлять свою информацию, и замечать неисправность, иначе они будут выполнять что-то совершенно сломанное.

Мы здесь находимся на пределе – любой должен заметить отказ как сейчас.

После удаления старого ключа возникает два вопроса. Первый, у нас все еще остается старый ключ в корневой зоне, но он не используется. Он по-прежнему находится здесь, но он не используется.

11 января он будет помечен специальным флагом. Его флаг будет изменен так, чтобы он говорил, «С данного момента ему доверять нельзя». Это называется битом отзыва. Другими словами, вы оказываетесь ему доверять. Это будет опубликовано в течение трех следующих месяцев, затем 11 апреля он будет фактически удален из корневой зоны полностью.

Таким образом, процесс обновления ключа сложнее, чем кажется. В данный момент нет оснований полагать, что мы вернемся к использованию старого ключа, поскольку кажется, что все идет успешно.

Хорошо. Хороший вопрос. Спасибо.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Хола. Планируется ли интегрировать в браузер уведомление для пользователя о сертификате, о том, что [неразборчиво] сайт с DNSSEC?

Еще один вопрос. Я рекомендую своему клиенту использовать «.com», а не обычный TLD, поскольку они не подписаны в доменах общего пользования верхнего уровня. Это дополнительная маркетинговая реклама для других доменов, и они вынуждены быстрее внедрять DNSSEC.

Мой вопрос, планируется ли показывать пользователю, что это правильный сайт?

УЭС ХАРДЕЙКЕР: Извините, я не расслышал концовку? Планируется показывать что?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: В браузере. [неразборчиво] Мы видим [неразборчиво] подпись любого … я вижу на слайде уведомление в браузере, и я вижу изображение браузера. Это интегрировано, возможно, в расширение браузера или что то аналогичное?

УЭС ХАРДЕЙКЕР: Вы хотите обсудить это? Нет? Хорошо. На самом деле существует расширение браузера, называемое DNSSEC, которое можно установить… я закрыл имя. Если вы ищете расширение для браузера Chrome и Firefox, существует одно, которое установлено в ICANN в вашем браузере.

Поставщики браузеров еще не очень заинтересованы выполнять DNSSEC непосредственно в самих браузерах. С этим связана длинная история. Вы можете обратиться к ним с претензией.

Итак, валидатор DNSSEC – спасибо, Тим. Оно называется валидатор DNSSEC. Если вы решите получить его, фактически он будет установлен. Много лет назад Расс и я разработали

браузер, выполняющий DNSSEC на низком уровне в основной библиотеке. Этот браузер называется Bloodhound. Кстати, он не обновлялся, поэтому фактически не имеет нового ключа. Это использовалось один раз в [Twitter.]

РАСС МАНДИ: Да. Нам нужно подумать, как это сделать.

УЭС ХАРДЕЙКЕР: Да. Это фактически изменить Firefox, в частности, чтобы фактически идти и выполнять DNSSEC непосредственно в браузере на низком уровне. Еще больше происходит при использовании электронной почты и других вещей. Опять повторю, что я расскажу об этом в среду, и покажу интересные графики тенденций фактически все большего и большего использования в электронной почте [неразборчиво].

БАРРИ ЛИБА (BARRY LEIBA): Рассказывая пользователям об этом, со временем появляется много свидетельств, что пользователи не понимают то, о чем мы рассказали, и пытаться рассказать пользователям, которые не имеют ни малейшего понятия, что такое DNSSEC, так чтобы они поняли это, просто невозможно. Тут нет никаких сомнений.

УЭС ХАРДЕЙКЕР: Да. Другими словами, как люди говорят об этом, сегодня это сделано так, что вы просто выдаете сообщение об ошибке, вы

даже не показываете им зеленый или красный цвет. Вы просто не позволяете им зайти сюда. Множество свидетельств говорит о том, в общем, что конечные пользователи не имеют информации, чтобы принять правильное решение по безопасности, вы не даете им принять решение о безопасности. Вы просто запрещаете им.

За вами, Эндрю.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Просто замечание по этому поводу, это не значит, что мы не хотим вмешиваться и говорить конечному пользователю и объяснять, почему это сообщение появилось. Не имеет значения, будет это объявление на странице или блокировка контента. Это будет более или менее поясняющее сообщение, поскольку, если это первый раз, да, это нововведение. Вы не знаете, что это такое. Но, если сообщение самоочевидное, в определенном смысле, это будет хороший метод, когда оно появится следующий раз, это действительно поможет, или …

УЭС ХАРДЕЙКЕР: Да. Это длительный спор по общей безопасности о том, как много позволить пользователю делать. Я, лично, будучи техническим фанатом, всегда надеюсь, что мне дают возможность видеть максимум возможных деталей. Но я работаю с моими ближними, которые не понимают эти вещи, и зовут меня. Поэтому, это большая разница.

У кого-то еще есть вопросы?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Есть один. У нас много проблем. Мы можем хранить данные на локальном узле, и узел [неразборчиво]. Если мы увидим уведомление в браузере … Я не знаю, если [неразборчиво] прокси-сервер, и сможем рассмотреть другие вопросы, чтобы использовать преимущество подписи. Поэтому очень важно идентифицировать пользователя и рассмотреть много вопросов [неразборчиво] интернет.

УЭС ХАРДЕЙКЕР: Да. Сегодня мы говорим на самом деле только об именах. Если прокси-сервер также использует резолвер интернет-провайдера и он прошел валидацию, он также будет защищен. Но вы правы, существует множество уровней и не один кэш в механизмах типа HTTP или в электронной почте и всех других вещах этого типа. Все эти поиски DNS должны пройти валидацию, чтобы получить полную цепочку безопасности. Вы правы на этот счет.

Один за вами, Эндрю. Это всегда за вами. Вы это заметили?

ХОСЕ АЛБЕРТО (JOSE ALBERTO): Здравствуйте. Меня зовут Хосе Альберто. Я участник программы Fellowship ICANN.

Мой вопрос связан с Tor. [Если мы используем Tor для чего-нибудь, применима ли безопасность DNS к Tor?] Она применима, в этом случае … я не знаю. Это возможно? Они используют другой метод безопасности в DNS?

УЭС ХАРДЕЙКЕР: Это хороший вопрос, и это напомнило мне то, что я пропустил также вопрос о блокчейн. Существуют альтернативные системы имен, используемые в интернет. Они менее популярны. Tor одна из них. Фактически имеется Namecoin, система имен, основанная на блокчейн. Они не совместимы с DNS. DNSSEC фактически защищает только DNS – общепринятую систему разрешения имен. Она не препятствует использованию этих других механизмов. Она не препятствует использованию ими собственных систем безопасности.

Нет, я не думаю, что DNSSEC применима к Tor. Предполагаю, в теории это возможно, поскольку она работает подобно DNS. Но я не специалист по Tor, к сожалению. Кто-то еще?

Не достаточно для ответа. Хорошо.

Предположу, что возможно, ответа нет, тут ничем не поможешь. Наверно, вам следует обратиться к кому-нибудь, кто знает Tor лучше. К сожалению, в зале нет экспертов по Tor.

Это не работает. Хорошо. Мы нашли определенный ответ. Нет, это не поможет.

ФАН-ЧИ ЛИН (FAN-CHIEH LIN): Здравствуйте. Это Фан-Чи Лин из Chunghwa Telecom. Меня зовут Джейсон, между прочим. Это опять я. Как я понял, DNSSEC предназначен для защиты транзакции DNS. Я прочитал статью о введении куки в DNS [RFC, MTA, MT3]. Не является ли это более легким методом? Не могли бы вы прокомментировать эти аргументы?

Спасибо. Надеюсь, я не отклонился сильно от темы.

УЭС ХАРДЕЙКЕР: Нет, это замечательно. Куки в DNS решают совершенно другую проблему. Я должен поправить самое первое предложение, сказанное вами. Оно содержит небольшую ошибку. Она не серьезная, но вы сказали, они защищают транзакции. DNSSEC не защищают транзакции. Они защищают данные.

Позвольте мне привести вам пример. Если я дам Рассу некоторую информацию DNS и скажу: «Вне DNS я собираюсь сказать ему что узел с моим именем имеет адрес 1.1.1.1, и вот моя подпись», он может передать ее по всему залу, и может проверить весь путь обратно. Это фактически фиксирует сами данные.

Меня не беспокоит, как они переданы. Это может быть DNS. Это может быть почтовый голубь. Это не имеет значения. DNSSEC не соединение защищает соединение. Защищает сами данные.

Это важно из-за того, что есть кэш, в DNS это может занимать несколько переходов. Если вы используете резолвер Google с

адресом 8.8.8.8, например, у них есть много узлов, образующих систему, совместно использующую кэш.

И неважно, кто спрашивает и кто отвечает. До тех пор, пока вы сможете проверить данные в конечной точке, не важно как вы их получили.

Механизм куки разработан для защиты отдельной транзакции, часто слишком большое количество данных, позволяет получать от сервера ответ большего размера, чтобы предотвратить атаки типа отказа от обслуживания. Сервер может затребовать от вас в ответ TCP или что-то не подверженное ложной атаке.

Куки решают поэтому другую проблему. Они не защищают данные внутри транзакции DNS.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Здравствуйте. Как я понял, чтобы защитить данные DNS, у нас есть механизмы двух типов. Первый это DNSSEC, а второй DNS поверх TLS [неразборчиво].

Обычно, как я вижу, DNSSEC очень популярен, более популярный, чем DNS поверх TLS. Не могли бы вы провести сравнение между этими двумя типами механизмов? Каковы наиболее предпочтительные характеристики DNSSEC по сравнению с другим? Спасибо.

УЭС ХАРДЕЙКЕР: Они также имеют различные цели. DNSSEC, повторю, для защиты данных. Не имеет значения, передаются они поверх TLS или нет. Неважно, как вы их получили.

DNS поверх TLS предназначен для защиты транзакции между одним субъектом, задающим вопрос, и местом, откуда он получает ответ.

Если ваш браузер запрашивает вашего интернет-провайдера, он может сделать это поверх соединения TLS, чтобы никто в кафе не подсмотрел ваш запрос. Но вы не знаете, способен ли резолвер интернет-провайдера запросить корень и «.com» и «bigbank.com» поверх TLS.

DNSSEC защищает целостность данных, чтобы вы получили правильный ответ. DNS поверх TLS разработан, чтобы обеспечить приватность, чтобы никто другой не увидел, что вы спрашиваете, и ответы, которые вы получаете.

Возможно, однажды TLS будет использоваться повсюду, но вы все равно не будете знать, из-за множества переходов, безопасны ли на самом деле данные, которые вы получили из точки A до B до C до D. DNSSEC обеспечивает эту безопасность, независимо от того, сколько произошло переходов, вы знаете что данные правильные.

КЕН ХЕРМАН (KEN HERMAN): Здравствуйте. Добрый день. Кен Херман, независимый консультант. Да, я убежден в значении DNSSEC.

УЭС ХАРДЕЙКЕР: Ура!

КЕН ХЕРМАН: Не могли бы вы рассказать об уровне проникновения? Как много людей его используют? Как организации или просто отдельные лица могут знать, что DNSSEC установили эту цепочку доверия вдоль маршрута?

В-третьих, не могли бы вы сказать что-нибудь о стоимости реализации для организаций? Возможно, это немного для малого бизнеса, который зависит от своих интернет-провайдеров, но, возможно, для больших организаций стоимость может быть высокой. Спасибо.

УЭС ХАРДЕЙКЕР: Приглашаю вас на семинар DNSSEC. Самая первая презентация на каждом семинаре DNSSEC, который на этот раз состоится в среду – если все будет нормально, фактически в конце недели – содержит изобилие карт и данных о том, где произошло проникновение, в каких частях мира наблюдается максимальное использование, включая прочие аналогичные вещи. Я проведу презентацию по количеству доменов [неразборчиво] и насколько успешно развертывается DANE. Так что здесь может будет много технической информации. Я не могу повторить всю ее здесь. [неразборчиво] [батарея.] Да, фактически.

В смысле … какова вторая часть вопроса?

[КЕН ХЕРМАН]: Стоимость.

УЭС ХАРДЕЙКЕР: Да, стоимость. Это будет сделать гораздо труднее. Если вы попросите вежливо своего интернет-провайдера включить валидацию DNSSEC, вероятнее всего, они это не сделают, пока не попросят люди. Если их попросит достаточно людей, они это сделают. В настоящее время конфигурация для включения минимальна, поэтому у них нет значительных причин для извинений, другой вопрос, что они должны знать как провести отладку, когда произойдет сбой. Они должны знать, что делать, когда произойдет обновление ключа.

Большинство в наше время уже должно быть автоматизировано. В прошлом этого не было. Вам необходимо было знать намного больше. Теперь это совершенно очевидно.

В начальный период, чтобы подписать свою зону, если вы собрались сделать это сами – вы должны были иметь собственный узел DNS и самостоятельно его подписать – при помощи последовательности, примерно, из 12 команд. Мы это изложили в документе руководства по раннему развертыванию. Он был очень длинный и утомительный. Расс и я работали вместе. Наши коллеги вместе с нами разработали одно средство. Вы выполняете [зона-подписчик-пробел-имя файла] и все сделано, а затем вы публикуете результаты.

Инструменты делают работу намного проще, поэтому стоимость ниже. Но бесплатной безопасности не существует. Определенная безопасность всегда существует.

Еще одну вещь вы должны знать о DNSSEC, если собираетесь делать это сами, перед использованием DNS следует опубликовать и забыть. Вам никогда не придется модифицировать вашу зону. Просто выходите и публикуете один раз. Вы может оставить ее на три года, и данные все еще будут верными.

С DNSSEC, из-за ограничения по времени, вы должны повторно подписываться раз в месяц, или в зависимости от выбранных вами параметров. Обычно это месяц. Для своей зоны я повторно подписываюсь каждые две недели, хотя цепи доверия остаются верными в течение месяца.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: У меня одно замечание по поводу только что сказанного вами, поскольку, например, узловой резолвер, выполняющий все подписание для вашей зоны … если у вас есть система, которая публикует запись CDS, именно как это обычно должно быть. Просто публикуешь один раз, и все автоматические механизмы позаботятся о безопасности. То есть стоимость действительно минимальная.

УЭС ХАРДЕЙКЕР: Да. Он поднял хороший вопрос. Если вы просто скажете своему резолверу – я полагаю фактически большинство

авторитативных резолверов теперь имеют автоматическое подписание – они просто будут продолжать подписывать для вас. Чтобы это все автоматизировать, имеется масса персонала.

Я параноик. Я делаю это на собственном ноутбуке, это потому, что я так стал делать с самого начала, не потому, что я все еще должен.

Есть еще вопросы? Все эти вопросы были просто фантастическими. Большое спасибо.

ТАН НГУЙЕН: У меня есть еще один вопрос. Это не технический вопрос. Возьмем конкретную страну Вьетнам – поскольку я из Вьетнама – например, у моего правительства собственная система DNS, она [неразборчиво]. Мы хотим заменить всю систему DNS на DNSSEC. Так сколько будет стоить перейти от DNS на DNSSEC, и сколько это займет времени? Могли бы вы примерно рассчитать время и стоимость?

УЭС ХАРДЕЙКЕР: Такие вещи трудно рассчитать, поэтому я не уверен …

РАСС МАНДИ: Позвольте мне сделать замечание по этому поводу. Я не претендую на точные, конкретные ответы, но могу дать вам представление.

Следует указать на одну вещь, когда люди начинают устанавливать DNSSEC, настраивать и вводить в действие, они часто обнаруживают, что их программное обеспечение DNS не обновлялось надлежащим образом.

Если они используют авторитативные сервера имен, или, если они также являются интернет-провайдерами и используют рекурсивные сервера имен – что они устарели на три, пять или даже десять лет. Поэтому самым первым этапом в большинстве случаев, как этот, необходимо проверить инфраструктуру DNS вашего государства.

Если оно находится в хорошем и актуальном состоянии с текущим программным обеспечением, как было сказано ранее, проблемы с внедрением DNSSEC могут быть иногда настолько простыми, как изменение одного или двух вариантов настройки в файле конфигурации теневого мастера настройки, который выполняет фактическое распределение по авторитативным серверам.

Это может быть намного сложнее, если вы захотите настроить отдельный от сети криптографический механизм.

Все по-разному, но первое и самое важное, это посмотреть на саму вашу инфраструктуру DNS. Начните отсюда. В сети есть множество информации. Иногда сообщество DNSSEC распространяет чрезвычайно полезную информацию, и в сети имеется масса информации о том, что еще, в масштабах страны, должно быть сделано.

УЭС ХАРДЕЙКЕР: ISOC создала сайт, который вы видели ранее, с развернутыми DNSSEC, тот, с фотографией Стива Крокера на нем. Это хорошее место для начала поиска ресурсов по DNSSEC, которые помогут вам пройти весь путь до конца. Это прекрасный сайт с множеством информации.

У меня есть свой с немного более техническим названием средства DNSSEC. Также вы можете обратиться к своему регистратору. Многие из них имеют эти средства, если вы позволите разместить на узле ваши данные и они используют сервера DNS, тоже, они сделают это также просто, как поставить галочку в нужном поле.

Поэтому сколько это стоит, зависит от того, как вы хотите это сделать. Вам необходимо провести оценку, о которой говорил Расс. Он сказал, что вы должны начать с того, что имеете сейчас, а затем спрогнозировать, что это будет вам стоить.

РУДОЛЬФ ДАНИЕЛЬ: Здравствуйте. Руди, еще раз, участник программы Fellowship ICANN. Я только что вспомнил, что видел вещь под названием EDNSSEC. Есть такая вещь?

УЭС ХАРДЕЙКЕР: Я думаю, что вы спутали две вещи. EDNS, без SEC, это расширение в механизме DNS, добавляющее дополнительную информацию, когда вы ее запрашиваете.

Фактически, когда вы говорите, «Я хочу сделать DNSSEC. Дайте мне все подписи и прочие материалы.» Это механизм расширения внутри DNS, который необходим для DNSSEC.

РУДОЛЬФ ДАНИЕЛЬ: Ага, хорошо. Спасибо.

УЭС ХАРДЕЙКЕР: Последние вопросы? Барри?

БАРРИ ЛИБА: Если есть минутка, я бы хотел вернуться к прежнему вопросу о DNSSEC и HTTPS.

Изначально вы обычно не переходите на сайт при помощи HTTPS. Вы заходите по HTTP, и получаете переадресацию. Атакующий может не позволить отправку вам переадресации и обманом заставить вас не использовать HTTPS. Поэтому здесь вам все еще необходима верификация.

Затем, вы выходите с тем, что называется «Strict Transport Security», где сайт, когда вы заходите на него, говорит, «Используй HTTPS, и, кроме того, всегда используй HTTPS и никогда не принимай подключение ко мне без этого». Это использует технологию, называемую «доверяй первому использованию», предполагающую, что атакующий не перехватит первый запрос.

Чтобы осуществить это, браузеры сегодня помещают список строгой сетевой безопасности в браузер, поэтому вам нет

необходимости доверять даже первому использованию. Вы никогда не попытаетесь зайти на этот сайт.

Но затем вы все еще имеете надежный ЦС, упомянутый Рассом, где, если заглянуть в ваш браузер и посмотреть, скольким корневым центрам сертификации доверяет ваш браузер, сотням из них, от Verisign до компаний в Тайване, о которых вы никогда не слышали.

Если любой из них будет скомпрометирован и будет убежден выдать сертификат «bigbank.com», то вы тоже скомпрометированы.

Таким образом, теперь у нас есть вещь под названием DANE, где банк публикует свою собственную запись DNS говорящую: «Это сертификат, который я хочу, чтобы вы использовали». Это решает проблему, но угадайте, что необходимо DANE? DNSSEC, поскольку вы собираетесь получать сертификаты из DNS.

Таким образом, все зацикливается, и мы приходим к тому, что сказал Уэс о том, что все разделено на уровни. Вам необходимо защитить каждое звено на всем пути.

УЭС ХАРДЕЙКЕР: Реальность такова, первое, что вводит пользователь в любое приложение, браузер или другой, это имя, чтобы выполнить поиск по этому имени. Эта первая уязвимая точка. Существуют другие способы обойти все эти проблемы, и все они

проблематичны. Но если вы защитили DNS, то, фактически, исчезает целый ряд проблем.

Это не значит, что после этого вам не надо использовать HTTPS. Это решает другую проблему.

Последние вопросы?

АХМАД АЛСАДЕХ: Еще раз, Ахмад Алсадех, участник программы Fellowship ICANN. Когда я смотрю на эту схему, все в цепочке должны иметь сертификат или проверять подпись. Если один из них не реализовал DNSSEC, они будут безуспешными. Это так? Я правильно понял?

УЭС ХАРДЕЙКЕР: Близко. Они не будут безуспешными, но вы определенно будете знать, что вы теперь переходите в место, не имеющее подписи DNSSEC, и может продолжить и выпасть из цепочки доверия.

Имеются неподписанные части дерева DNS, и ваш браузер будет по-прежнему работать с ним совершенно прекрасно, поскольку DNSSEC фактически предоставят вам ответ. Они скажут «Хорошо, так. Вам нужно перейти на «bigbank.com». Кстати, они не внедрили DNSSEC. У вас нет выбора. Вы вынуждены продолжить с обычным DNS».

Это механизм выпадения, где, по мере продвижения резолвера по цепочке, он обычно доходит до точки, когда

говорит, «Дальше я не могу обеспечить безопасность, но вам, возможно, все равно еще нужен ответ».

Вот где мы находимся сегодня, где много вещей подписано и много нет. Мы не даем пользователю большой наглядности, за исключением сообщений.

АХМАД АЛСАДЕХ: Хорошо. Спасибо.

УЭС ХАРДЕЙКЕР: Хорошо. Возможно у нас есть время еще на один вопрос, кто желает задать последний вопрос.

Один здесь.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: [Неразборчиво]. В этом сценарии вы получаете сообщение об ошибке?

УЭС ХАРДЕЙКЕР: Хороший вопрос. Итак вопрос, в этом сценарии вы получаете сообщение об ошибке? Да, так как это случилось – хорошо, вы не получили сообщение об ошибке, когда выпали в небезопасную часть просто из-за того, что ваш резолвер продолжает предоставлять вам ответ. Ваш резолвер скажет вашему приложению, получили вы безопасный или небезопасный ответ.

Сейчас браузеры или другие приложения фактически не смотрят на этот бит информации, поскольку как именно представить это пользователю и будет ли это мудрый выбор представить это пользователю в духе понятия, полезно это конечному пользователю или нет.

Что мы получим, если DNSSEC откажет в некоторой точке, если Доктор Зло фактически окажется посередине, сообщение о неисправной странице сайта, говорящей: «Это имя не найдено» как бы резолвер не старался. Он пытался найти это имя, и если ни разу не получил правильный ответ, поскольку продолжает получать неправильные ответы, и никогда не получит правильно подписанный ответ, вы получите страницу, которую получаете, когда переходите по любой нерабочей ссылке. Она говорит: «Это имя не найдено».

Вы не будете знать, что это произошло потому, что вас защищает DNSSEC. Вы будете знать, что невозможно найти нужное вам имя.

Хорошо. На этом, я думаю, мы будем заканчивать. Вы хотите в заключение добавить комментарии в отношении среды?

РАСС МАНДИ: Да, у нас есть несколько привлекательных – ненавязчивых, но это хорошо – объявлений на среду. У нас будет несколько панельных дискуссий. Одна из них касается DANE. Во вводной части мы поговорим о составленных картах с выборкой количества и типов размещения DNSSEC в различных частях планеты, географически.

Мы приглашаем всех вернуться в среду. Начало в 09:00 и продлится, я думаю до 14:30? Кати, это правильно?

КАТИ ШНИТТ (KATHY SCHNITT): 3:00.

РАСС МАНДИ: 3:00. Хорошо. Пожалуйста, подумайте об этом. Спасибо, что пришли. Надеемся вы получили ответы на свои вопросы. Если вам нужно встретится с любым из нас, или любым из сегодняшних участников, по вопросам DNSSEC, мы готовы дополнительно ответить в личной беседе в холле.

Благодарю всех.

УЭС ХАРДЕЙКЕР: Да. Спасибо. Один последний момент. Завтра технический день, здесь также часто происходит обсуждение многих концепций, связанных с DNSSEC. Почти всегда. Я не помню на данный момент повестку дня. Но обычно много презентаций о TLD, развертывающих DNSSEC, и аналогичных вещах.

РАСС МАНДИ: Да. Начало сразу после церемонии открытия в 10:30.

УЭС ХАРДЕЙКЕР: Сразу после церемонии открытия. Хорошо. Спасибо, что пришли. Надеюсь, вы получили массу удовольствия.

[КОНЕЦ СТЕНОГРАММЫ]