КОБЕ — DNSSEC для всех: руководство для начинающих
Воскресенье, 10 марта 2019 года, 15:15 – 16:45 по JST
ICANN64 | Кобе, Япония

УЭС ХАРДЕЙКЕР (WES HARDAKER): Секундочку, сейчас все поправим. Сейчас должно быть везде. Хорошо.

Ладно. Сегодня мы поговорим о DNSSEC, о том, как они защищают вас при работе в Интернете и о том, какое участие во всем этом принимает ICANN. Меня зовут Уэс Хардейкер, я из Института информатики Университета Южной Калифорнии. Через минуту к нам присоединятся наши прекрасные персонажи, которых я вам представлю.

А пока я хочу рассказать вам историю DNSSEC. Наша история началась очень и очень давно — примерно за 5000 лет до рождества Христова в эпоху динозавров. Все началось с Огвины — нашего главного персонажа. Она живет на краю Большого Каньона в пещере. Это Ог. Он живет на другой стороне Большого Каньона в пещере. Они живут далеко друг от друга. Большой Каньон очень глубокий и широкий. Спускаться очень далеко, и у них нет возможности много общаться — они очень далеко друг от друга.

Во время одного из нечастых визитов они пересекли канал и поговорили друг с другом. Они увидели, что от очага Ога

исходит дым, и подумали, что его можно использовать. Мы можем общаться с помощью дымовых сигналов. И уже очень скоро они начали довольно часто общаться с помощью дымовых сигналов. И все шло хорошо. Вплоть до одного дня, когда злой пещерный человек по фамилии Камински поселился неподалеку и начал посылать дымовые сигналы в то же время.

Теперь Огвина пребывает в полном замешательстве. С другой стороны каньона поступает два набора дымовых сигналов, и она не знает, который из них для нее. Поэтому Огвина спустилась в каньон, чтобы попытаться разобраться во всем этом беспорядке. Огвина и Ог обратились за помощью к мудрым старцам деревни. Пещерный человек Диффи — некоторые уже знакомы с ним. Диффи — знаменитый криптограф, который помог создать технологию DNSSEC, и мы рассмотрим это дальше. Он пошел в пещеру Ога, в которой нашел волшебный синий порошок. Так как у порошка был странный цвет, Диффи подошел к огню и бросил его в огонь. Синий порошок дал синий дым, и теперь Огвина и Ог могут продолжить свои беседы: Огвина знает, что она должна обращать внимание на синий дым, потому что синяя пыль есть только в пещере Ога.

Теперь все стало на свои места. Мы закончили. Это было краткое пояснение того, что представляет собой DNSSEC. Мы поясним это подробнее, но суть такова. Концепция

DNSSEC заключается в том, чтобы преобразовать что-то одно во что-то другое, что, как вы знаете, поступает из правильного места.

Давайте вернемся к DNS и начнем с концепции DNS. Если вы знаете, что такое DNS или в свое время или вчера ознакомились с руководством по DNS для новичков, вы, возможно, видели такую схему — DNS начинается с самого верха, с корня, что подробно обсуждалось на встрече ICANN. Далее идут все TLD, иногда коды стран, такие, как .com, а ниже идут домены второго уровня, такие как co.uk, bigbank.com и nic.ma. Сегодня мы сосредоточимся на bigbank.com.

Очень важно знать, что ваш интернет-провайдер имеет резолвер, а резолвер знает, где размещается корневая зона. Зная ее размещение, он может проследить цепочку до самого конца, чтобы узнать, где находится все остальное. Начинаться все должно с корня, а затем спускаться вниз. Он знает, где находится com, а затем опускается вниз. Мы поговорим об этом более подробно, а через минуту вы увидите пример. Каждый уровень отсылает резолвер на один уровень вниз. Так что все, что он должен знать в начале, — это то, где находится корень. В конце концов ответ на вопрос получен и резолвер кэширует эту информацию для будущего использования.

Итак, вот в чем проблема. В DNS нет безопасности. Когда DNS была изобретена, не знаю в каком году, но очень давно — в 84, безопасность в ней не была предусмотрена. Тогда все были добрые, и зла не существовало. Но позднее имена стали подделывать, и люди поняли, что они могут делать все, что угодно, в системе и подставлять вам неверные ответы. Это приводило к отравлению кэшей, и резолверу приходилось запоминать и правильные, и неправильные ответы за длительный период.

Далее мы проиллюстрируем вам это и представим вам небольшую пьесу (вот актеры — они в белых рубашках) о том, что делает резолвер и интернет-провайдер. Начнем с Джо Юзера — вот он слева. Сегодня ему нужно выполнить некоторые банковские операции на bigbank.com, и мы посмотрим, как DNS поможет ему получить правильный ответ.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Они хотят, чтобы вы меня увидели.

РАСС МАНДИ (RUSS MUNDY): Привет, интернет-провайдер.

УЭС ХАРДЕЙКЕР: Да.

РАСС МАНДИ: Мне нужно поговорить кое с кем из bigbank.com. Вот имя нужного мне человека.

УЭС ХАРДЕЙКЕР: Я не знаю, где находится bigbank.com. Давайте я попробую поискать. Я скоро вернусь.

Привет, корень. Я хочу попасть на www.bigbank.com. Вы можете сказать мне, где он?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Привет, Я Сервер корневой зоны. Я знаю, где находятся домены верхнего уровня. Вы ищете .com? Почему бы не перейти к серверу .com по адресу 1.1.1?

УЭС ХАРДЕЙКЕР: Хорошо, давайте попробую. Здравствуйте, .com. Я ищу www.bigbank.com. Вы могли бы подсказать, где мне его найти?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Я не знаю, где найти www, но могу сказать, где находится bigbank.com. Он находится по адресу 2.2.2.2.

УЭС ХАРДЕЙКЕР: Привет. Я хочу попасть на www.bigbank.com. Вы могли бы подсказать, где мне его найти?

РАСС МАНДИ: Да, я bigbank.com и я знаю, где находится www.bigbank.com. Он находится по адресу 2.2.2.3.

УЭС ХАРДЕЙКЕР: Отлично. Тогда я сообщу об этом пользователю.

РАСС МАНДИ: Возможно, ему понадобятся его деньги.

УЭС ХАРДЕЙКЕР: Здравствуйте, вы подключились к 2.2.2.3. Здесь находится www.bigbank.com.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Спасибо, bigbank.com.

УЭС ХАРДЕЙКЕР: Да. Ладно. Благодарим актеров труппы учебника по DNSSEC. Мы признательны за это. Мы вернемся к вам через секунду. Давайте им поаплодируем. Но не спешите, все может быть еще лучше. Следующий слайд, пожалуйста.

Вся эта сценка похожа на разговор Огвины с Огом через резолвер и получение сигналов до появления злого человека. Вопрос в том, что происходит, когда

вмешивается злой Каминski и посылает альтернативный дымовой сигнал? Как это влияет на DNS? Как можно обмануть DNS? Как возникают проблемы?

Здесь мы возвращаемся к нашей сценке — она будет такой же забавной, можете мне поверить.

РАСС МАНДИ: Здравствуйте, интернет-провайдер.

УЭС ХАРДЕЙКЕР: Здравствуйте.

РАСС МАНДИ: Я хочу положить деньги на депозит в bigbank.com. Не могли бы вы мне помочь найти его?

УЭС ХАРДЕЙКЕР: Да, без проблем. www.bigbank.com. Сейчас я спрошу у корня.

Здравствуйте, корень. Один из моих пользователей хочет попасть на www.bigbank.com. Вы можете сказать мне, где это находится?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Обратитесь к серверу .com по адресу 1.1.1.1.

УЭС ХАРДЕЙКЕР: Хорошо, пойду и спрошу. Здравствуйте, серверы .com. Один из моих пользователей хочет попасть на www.bigbank.com. Где он находится?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Я не могу сказать, где находится www, но я могу сказать, что bigbank.com находится по адресу 2.2.2.2.

УЭС ХАРДЕЙКЕР: Отлично. Сейчас я спрошу там. Здравствуйте, один из моих пользователей хочет попасть на www.bigbank.com. Вы можете сказать мне, где это?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Разумеется. Конечно.

УЭС ХАРДЕЙКЕР: Отлично.

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

УЭС ХАРДЕЙКЕР: Конечно, спасибо. Здравствуйте, пользователь, переходите по адресу 6.6.6.6. Здесь находится www.bigbank.com.

РАСС МАНДИ: Хорошо. Или типа того. Сейчас я собираюсь...

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Принимаю ваш депозит, сэр. Большое спасибо.

УЭС ХАРДЕЙКЕР: Ладно. Итак, вы видите проблему? Бедный Джо Юзер не знает, какому ответу верить. Он считает, что верным является первый полученный им ответ. Это та же проблема, что и проблема дымовых сигналов. Как и в том случае, есть два сигнала, и пользователь считает истинным один из них. Они подаются в случайном порядке и в данном случае Огвина не знает, какому набору дымовых сигналов ей следует верить.

Но вернемся к нашей основной концепции DNS. Чуть раньше мы говорили о корнях верхнего уровня и доменах .com и bigbank.com под ними. Если резолвер вашего интернет-провайдера говорит с несоответствующей системой, он может получить либо правильный ответ — синий, либо неправильный — красный.

DNSSEC устраняет эту проблему, и вы сегодня здесь именно по этой причине. DNSSEC с помощью цифровых подписей повышает безопасность DNS, которой фактически не было раньше. При этом выполняются две важные функции. Прежде всего, речь идет о том, что информация не изменяется ни в какой точке вдоль пути следования, и она поступает из верного источника. Вы можете быть уверены в том, что она поступает из правильного источника, даже если хранится под стелькой в ботинке или другом подобном месте. Она была подписана, значит, она истинна. Ключи в подписях хранятся в самой DNS, что очень хорошо, потому что для того, чтобы определить ее безопасность, вы можете использовать саму DNS для проверки и определить, какие ключи вам нужны. Мы рассмотрим пример через секунду.

Резолверу нужно только... Как и в предыдущем примере, резолверу нужно знать только то, где начинаются корневые серверы, и затем он может проследить цепочку до самого конца, как DNSSEC. Резолверу нужно знать, где находятся корневые серверы, а они должны знать тот самый единственный корневой ключ, и затем они могут построить цепочку доверия, поскольку каждый уровень подписывает ключ следующего уровня вплоть до окончания цепочки. Таким образом, двигаясь по криптографической цепи вниз, вы знаете, что получите правильные ответы.

Теперь поговорим о преимуществе. Если вернуться к предыдущей схеме, вспомним ситуацию, когда Джо Юзер не знал, какому ответу верить. Он не знал, какому ответу верить — синему или красному. Теперь мы можем проверить их истинность и понять, что красный ответ не является истинным. Он не работает.

Давайте сосредоточимся на этом вопросе в ходе нашей игры и посмотрим, как нам перейти на сторону добра и уйти со стороны зла.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Это было отлично.

РАСС МАНДИ: Эй, интернет-провайдер, мне нужно поговорить с bigbank.com и мне нужно убедиться в том, что данный ответ является истинным.

УЭС ХАРДЕЙКЕР: Хорошо, это разумно. Давайте посмотрим. Здравствуйте, корень. Один из моих пользователей хочет поговорить с www.bigbank.com. Вы можете сказать мне, где это?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Я могу рассказать вам, где находится .com: по адресу 1.1.1.1. А вот сертификат, который доказывает, что информация является верной.

УЭС ХАРДЕЙКЕР: Отлично, я верю. Я пройду дальше и спрошу серверы .com.

Привет, знаете что? Один из моих пользователей хочет поговорить с www.bigbank.com. Вы можете сказать мне, где это? А после того, как вы скажете, я проверю вашу подпись.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Разумеется, вы, похоже, часто об этом просите. Я не могу сказать, где находится www.bigbank.com, но я могу сказать, где находится bigbank: по адресу 2.2.2.2, и вот подпись.

УЭС ХАРДЕЙКЕР: Отлично. Пойду дальше и спрошу там. Здравствуйте, я хочу знать адрес www.bigbank.com. Не могли бы вы мне сказать?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Bigbank.com находится по адресу 6.6.6.6.

УЭС ХАРДЕЙКЕР: Ладно, подождите минуту. А где подпись?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: У меня ее нет. О, нет!

УЭС ХАРДЕЙКЕР: Спрошу кого-то другого. Я вам не верю, вы мошенник.

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

РАСС МАНДИ: Ну, я знаю, что www.bigbank.com находится по адресу 2.2.3, и вот подпись.

УЭС ХАРДЕЙКЕР: Выглядит достоверной. Здравствуйте, г-н Юзер, bigbank.com находится по адресу 2.2.2.3, я проверил подпись, вы можете не сомневаться.

РАСС МАНДИ: Я вижу здесь подпись, и благодарю вас за это. Спасибо, Big Bank. Отправьте деньги.

УЭС ХАРДЕЙКЕР: Отлично, большое спасибо. Поаплодируем нашим актерам! Они делают важную работу. На следующих встречах ICANN мы будем делать это постоянно. Кто-то раньше видел эту сценку? Ага, несколько человек.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: [Неразборчиво]

УЭС ХАРДЕЙКЕР: Это то же самое, что и синий дым. Да. В конце концов Огвина смогла видеть синий дым, потому что он был подписан. В данной сценке мы обозначили это небольшими медалями, которые мы повесили на шею актеру, символизирующими ключи, которые мы использовали для подписи каждого уровня дерева DNS.

Дальше я передам слово моему соучастнику в этом [неразборчиво] преступлении, Рассу Манди, который приведет несколько примеров, демонстрирующих, зачем нужны DNSSEC, и несколько простых рекомендаций по использованию.

РАСС МАНДИ: Спасибо, Уэс. Меня зовут Расс Манди, я из Parsons, и сейчас я помогу вам лучше понять, как следует выполнять развертывание и расскажу о некоторых вещах, которые вам нужно проверить и подумать в ходе процесса.

Одним из важнейших аспектов DNS, о котором многие люди не думают, заключается в том, что сегодня DNS используется практически каждым приложением в Интернете. Поэтому, когда с вашей DNS что-то не так, она

изменена, или по какой-то причине возникла какая-то проблема, неполадка или что-то в этом роде, из-за проблемы страдают приложения. Вы не можете подключиться. В нашем случае Джо Юзер не сможет поговорить со своим банком. Это наиболее важная и распространенная проблема, связанная с тем, чем является DNS и что она делает.

Итак, если важно сделать так, чтобы все приложения работали, почему люди атакуют DNS? Я занимаюсь вопросами DNS и безопасности DNS на протяжении многих лет и, честно говоря, я никогда не видел и не слышал о ситуациях, когда люди начинают атаковать DNS, потому что просто хотят изменить DNS, а затем выйти и все. Их цель не в этом.

Их цель — получить доступ к информации, содержащейся в приложениях после получения запросов DNS. Возможно, их цель заключается лишь в том, чтобы сделать копию всех электронных сообщений, поступающих из определенного места. В таком случае, для всех адресатов почтового сервера, которым совершается рассылка, они могут задать ложный адрес на промежуточном почтовом сервере и получать все электронные сообщения, поступающие от данного конкретного сервера, а затем, при желании, направлять их в нужные места так, что получатели не увидят никакой разницы. Это так называемая атака посредника.

Несколько лет назад, не знаю, смогу ли я найти эти курсы снова, поскольку, похоже, что их больше нет в Интернете, были одни или двое курсов, где инструкторы просили обучающихся написать программу для перехвата DNS. И там нигде не было сказано, что это плохо и делать этого нельзя. Также существовали пакеты программ, которые позволяли выполнять то же самое. Не так уж и сложно найти нужные инструменты или ПО. Чем же полезна DNSSEC?

В пьесе вы видели, как вопрос, заданный пользователем, прошел через процесс проверки правильности источника информации и того, что содержимое не было изменено по пути.

Вот пример того, как работает перехват. Я приведу очень простой пример. Не такой простой, как в нашей сценке, но давайте посмотрим... Вы видите, что первый запрос, обозначенный пунктирной линией, поступает от Джо Юзера. Затем он проходит через разные этапы для связи с авторитативным сервером, а затем поступает на рекурсивный сервер с ответом. Затем он направляется обратно пользователю и, наконец, после этого запрос поступает на веб-сервер. Как видите, в сети наблюдается интенсивный трафик, о котором большинство людей даже не думает — это трафик DNS, возникающий перед трафиком веб-сервера или почтовым трафиком или трафиком Facebook или трафиком в любых других местах.

Несколько лет назад мы сделали вот что: мы создали оптимизированный под требования пользователя веб-сайт, который будет проверять входящие запросы, проверенные DNSSEC запросы и выполнять проверки DNSSEC. Мы придумали небольшой знак X, небольшой знак проверки, специально для этого веб-сайта. Если вы входили и подавали тот же запрос и не делали проверку DNSSEC, вы могли видеть по содержимому страницы, что она не была проверена DNSSEC.

Затем мы смоделировали перехват DNS, который показал, что случится, когда это произойдет. Давайте перейдем дальше и щелкнем первый.Теперь следующий щелчок. Доктор Зло, наш прекрасный помощник — вот он здесь, сбоку в большом черном плаще с капюшоном, внезапно появился и дал ответ, который перенаправил Джо Юзера на другой сайт. При этом запрос и правильный ответ все равно переданы системой, но Джо Юзер и его компьютер так и не получили его, потому что первый полученный им ответ, ответ от злого перехватчика, уже поступил на его компьютер, и компьютер сказал: «Отлично, я получил ответ, и меня больше ничего не беспокоит».

При использовании DNSSEC вы получаете тот же набор пакетных потоков, что и указанный здесь, но разница состоит в том, что проверка и валидация поступающих пакетов и ответов DNS, поступающих от злого перехватчика, не принимаются компьютером Джо Юзера.

Надеюсь, было еще несколько [ошибок], но, в любом случае, да — это пакеты, просто передающиеся туда и обратно.

Как же выглядит настраиваемая страница? Эта настраиваемая страница выглядит точно так же, как тогда, когда я вам ее показывал. А вот следующая. Мы выполнили перехват и в данном случае это было в период, когда председателем Правления ICANN был Стив Крокер, который тоже был вовлечен в процесс разработки DNSSEC на протяжении длительного времени. Поэтому мы включили шуточную ссылку на другой сайт, контент которого содержал часть экрана, которую пользователь видел, если переходил на него без валидации DNSSEC. Таким образом, мы перехватывали собственные данные. В данном случае мы делали это, чтобы продемонстрировать, что может произойти при такой атаке на страницу.

Вот что происходило 10 лет назад, если вы начинали с пустого резолвера, пустого браузера и переходили на cnn.com. Все выглядело вот так. Сегодня все существенно сложнее. Все выглядит скорее так. Это все для заполнения только одной страницы. Далее.

Здесь важно отметить один момент: DNSSEC используется для того, чтобы проверить правильность

зоны DNS, содержимое самой зоны, а также поток передачи соответствующих данных через Интернет.

Вот еще одна простая иллюстрация — это неподписанная зона, здесь выполняется запрос и ответ... Здесь всего несколько шагов, поэтому процесс выполняется очень быстро и в фоновом режиме. Затем, когда в игру вступает DNSSEC, при каждом открытии резолвера и выполнении проверки, будь это интернет-провайдер или локальная сеть предприятия, при выполнении масштабной операции на DNS-сервере, вы можете запускать регистратор и указывать множество DNS-серверов. Если при этом вы уже можете использовать собственные системы DNS, развертывание DNSSEC в этих системах будет относительно простым. Самой большой проблемой в данном случае является необходимость обеспечить поддержку ПО в течение длительного времени для использования функций DNSSEC. Следует отметить, что эти операции были существенно оптимизированы на протяжении последних лет, поэтому в большинстве случаев доступ к DNSSEC будет получен. Если вы используете собственные DNS-серверы, вам нужно просто использовать соответствующее ПО.

Если вы выполняете по-настоящему крупномасштабные операции, как для домена верхнего уровня или очень крупного предприятия, вы можете предпочесть выполнять их самостоятельно, а не передавать на аутсорсинг. Так

что это расширение функций, которые у вашей организации могут уже иметься.

Если вы конечный пользователь, то вы, как индивидуальное лицо, сидящее в этой комнате, можете попросить своего поставщика услуг выполнить валидацию DNSSEC — будь это предприятие или интернет-провайдер. В этом случае вы, скорее всего, не управляете собственными DNS-серверами (хотя некоторые это делают), и кто-то другой делает это за вас. В таком случае именно этих лиц нужно попросить выполнить валидацию DNSSEC, чтобы не позволить доктору Зло проникнуть к вам и украсть ваши данные DNS.

Как я сказал раньше, основная цель DNSSEC заключается в том, чтобы введенные в начале действия данные зоны, идет ли речь о bigbank или com, или о другом предприятии, обрабатывались в системе и доставлялись работающей системой DNS конечному пользователю и не изменялись в середине пути.

Таким образом, значение имеет, главным образом, содержимое зоны, и по-настоящему вам нужно сосредоточиться на том, чтобы содержимое зоны было доставлено туда, куда нужно, и это так же важно, как и все остальное... С одной стороны, многие люди на самом деле работали над этим — да, DNS использует криптографию, и это очень специфичная область, нам приходится

заниматься довольно необычными вещами. Вам необходимо следить за правильным управлением криптографией и ключами, но это делает большая часть современного ПО. Нужно помнить, что также необходимо обеспечить правильное управление контентом — правильно вводить его и обеспечить его неизменность в ходе процесса доставки на DNS-серверы, а затем, когда он находится на этих серверах, DNSSEC должна выполнить валидацию для доставки его конечному пользователю.

Таким образом, как видно из самых первых изображений, в данном случае нет существенных отличий от последней блок-схемы. Концепция заключается в том, чтобы добавить несколько дополнительных типов записей, как они называются в системе DNS, включаемых путем генерирования зоны, содержащейся в авторитативном DNS-сервере, а затем выполнить валидацию этой информации с помощью рекурсивного сервера, т.е. проверить медали по ходу выполнения операции интернет-провайдером от корня до bigbank.

То есть, при развертывании объектов с помощью DNSSEC важно учесть, насколько значительно ваша организация или ваш конкретный объект участвует в управлении вашей текущей DNS. Если вы сами управляете своей DNS на всех DNS-серверах и сами управляете серверами, вы, вероятно, сможете выполнять дополнительные функции, необходимые для предоставления подписи DNSSEC и

валидации в соответствующих точках. Если вы не управляете всем этим самостоятельно, например, многие крупные предприятия передают функцию управления DNS на аутсорсинг (скажем, parsons.com), то вы используете услуги внешнего провайдера. Одной из причин, почему такие услуги передаются на аутсорсинг, является то, что такие внешние провайдеры проводят проверку DNSSEC.

Так что, пользуясь услугами внешнего провайдера, вы можете захотеть попросить его провести для вас проверку DNSSEC. И не бойтесь перейти на другого провайдера, если первый говорит: «Простите, я не знал, что вам нужна проверка DNSSEC, я таких услуг не предоставляю». Найдите такого, который это сделает. Таких предостаточно.

Данное мероприятие проводится совместно ICANN и Консультативным комитетом по безопасности и стабильности. Также нам сегодня помогали члены Консультативного комитета системы корневых серверов, что само по себе очень хорошо, и программы Общества Интернета Deploy360 — все эти участники с нами уже долгое время. Кажется, это был последний слайд. Итак, пришло время для вопросов.

УЭС ХАРДЕЙКЕР: Хорошо, большое спасибо, Расс. Наш доктор Зло взял микрофон и спускается к вам, так что, если у вас есть вопросы о DNSSEC или вам нужно что-то уточнить, поднимайте руку и Эндрю, прошу прощения, — доктор Зло, подойдет к вам и даст вам микрофон.

АНЖЕЛА: Здравствуйте, меня зовут Анжела. Я из Ведомства по регулированию в сфере связи Ботсваны. Если открытый ключ перехватывается перехватчиком, есть ли какие-то механизмы, которые позволяют это выявить и проверить истинность ответа?

УЭС ХАРДЕЙКЕР: Это был поразительно точный вопрос. Я не привык к таким прекрасным вопросам. Благодарю вас. Итак, это отличный вопрос. Что же происходит, если ваш ключ скомпрометирован?

Происходит ряд вещей. Здесь сегодня собралось много экспертов. Если кто-то хочет ответить, поднимайте руки и отвечайте.

В данном случае в ситуации участвует два ключа — мы существенно упростили сценарий, но, по факту, мы имеем открытый и закрытый ключ. Вы говорили об открытом ключе. Вы можете дать открытый ключ кому угодно. Это можно делать без опасений. Цель использования

открытого ключа заключается в том, чтобы распространить его максимально широко. Но для защиты мы используем закрытый ключ. Если он скомпрометирован — кто-то вторгся в вашу систему и украл ваш закрытый ключ, то да, вы должны сообщить родителю. Если вы bigbank.com, вы должны сказать вашему родителю: «У меня новый ключ, пожалуйста, переключите цепь».

Помните порядок проверки медалей? Проще говоря, вам нужно заменить одну из этих медалей, висящих на .com, и сказать: «У меня для тебя есть новая медаль, у меня новый ключ, который я буду использовать. Теперь у меня другой закрытый ключ». Таким образом замену можно выполнить довольно быстро. Однако тут может возникнуть ряд сложностей. Есть значения времени существования и захвата, и много чего другого важного, но, если вкратце, вам нужно сделать именно это. Сказать вашему родителю: «У меня новый ключ. Мне нужно немедленно его заменить». Это позволит довольно быстро восстановить систему.

Есть еще вопросы? Отличный вопрос, спасибо.

САВЬО ВИНИСИУС ДЕ МОРАИС (SAVYO VINICIUS DE MORAIS): Здравствуйте, меня зовут Савьо, я из Бразилии, NextGen. Хочу задать вопрос о самой большой проблеме, с которой вы

столкнулись при попытке распространения DNSSEC в Интернете.

УЭС ХАРДЕЙКЕР: Вопрос в следующем: в чем заключается самая большая проблема, связанная с привлечением большего числа пользователей к его использованию? Кто-нибудь хочет ответить на этот вопрос? Могу я, но Расс?

РАСС МАНДИ: Мы занимаемся этим уже продолжительное время — разъяснением, мотивацией через разные форумы, такие как этот, и на разных мероприятиях, направленных на мотивацию поставщиков ПО обеспечить нужную структуру и функции в ПО, а также работаем с поставщиками приложений, чтобы мотивировать их обеспечить нужную поддержку.

Одним из самых существенных полезных для нас аспектов, направленных на привлечение большего количества людей, являются пользователи — индивидуальные лица или пользователи, являющиеся частью предприятия, которые заявляют: «Я хочу использовать DNSSEC». Некоторые из функций регистратора компаний не используют DNSSEC, что усложняет получение доступа к DNSSEC, если вы пользуетесь услугами такой компании. Почти все

операторы регистратур обеспечивают надлежащую обработку, но, с точки зрения конечного пользователя, конечные пользователи также могут подавать запрос поставщикам ПО, что повышает спрос и количество запросов на использование DNSSEC. Это, мне кажется, может быть самой существенной мотивацией, поскольку со временем, по мере того как разные программы сталкивались с этим вопросом, ответ в большинстве случаев был таким: «Наши клиенты не просят об этом». Именно по этой причине мы проводим мероприятия, подобные сегодняшнему — чтобы помочь людям понять, о чем идет речь, и объяснить конечным пользователям, что они могут просить об этом.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Хочу добавить кое-что к тому, что сказал Расс. На нескольких предпоследних слайдах была схема, связанная с валидирующими резолверами. При оценке успешности DNSSEC одним из учитываемых нами показателей является количество подписанных зон. Но разве не менее важно то, кто выполняет валидацию? Какая польза будет от того, что все домены мира будут подписаны, если приложения не будут иметь подписей и рекурсивные резолверы не будут выполнять валидацию того, что они получают? Было еще что-то, но я не помню что, поэтому на этом все.

УЭС ХАРДЕЙКЕР: Все в порядке. Хороший вопрос. Мы постоянно стараемся собирать статистику, отслеживать использование и следить за ростом DNSSEC. Если посмотреть на динамику развертывания по времени, DNSSEC продолжает расти. Конечно, рост не такой быстрый, как нам хотелось бы, потому что так никогда не бывает. Если бы все было так быстро, как нам хотелось бы, то все подписались бы уже сегодня.

Вот страница. Она называется stats.dnssec-tools.org. Данные поступают от одного специалиста, Виктора Духовны (Victor Duchovny), который занимается вопросами связывания DNSSEC с почтой. Как видите, за последнее время было несколько больших скачков — совсем недавно, в течение последних нескольких месяцев — мы проверяли, используют ли почтовые сервера записи электронной почты с подписями DNSSEC. Причиной некоторых из этих больших скачков стали компании, которые переключили все свои операции, все свои почтовые сервера. Они управляют несколькими доменами с рядом почтовых серверов и они все перевели их одновременно. Вот из-за чего наблюдались большие скачки.

Так что, хорошая новость заключается в том, что использование расширяется, но, в большинстве случаев, это происходит благодаря сарафанному радио, таким

мероприятиям как это и мероприятиям, которые проводит Общество Интернета. Впереди еще много работы, даже несмотря на то, что на данный момент подписано уже около 10 млн. доменов или вроде того. Но на самом деле их на .com намного, намного, намного больше, и мы стремимся непрерывно расти. Есть еще вопросы?

[КОФИ (COFY)] Меня зовут [Кофи], я из регистратуры доменных имен Ганы, и у меня есть два коротких вопроса. Первый: стоит ли регулярно менять закрытые ключи, или лучше их менять только после факта компрометирования? Второй: является ли проверка DNSSEC обязательным требованием для получения аккредитации ICANN для регистраторов и т.п.?

УЭС ХАРДЕЙКЕР: Это хороший вопрос. По поводу первого вопроса — скажем так, есть две точки зрения. Некоторые считают, что менять ключи нужно только после того, как они были скомпрометированы. В наши дни, если ваши ключи достаточно надежные, потому что мы понимаем, что ключи могут быть и слабыми, вам не нужно их часто менять. Скажу так: свои ключи я часто не меняю.

Но, пока вы этого не сделаете, вы не будете знать, как это сделать. Так что, с практической точки зрения, если вы

делаете это регулярно, вы будете знать, как сделать это быстро в случае необходимости. Многие люди регулярно меняют ключи — раз в год или около того.

Второй вопрос: у ICANN есть ряд требований к организациям, с которыми у нее есть контракт. Например, все новые gTLD должны поддерживать DNSSEC. Я не знаю, как обстоит дело с регистраторами. Новые регистраторы [неразборчиво] должны поддерживать DNSSEC?

РАСС МАНДИ: Не могу сказать точно, но, мне кажется, к регистраторам такое требование не предъявляется.

УЭС ХАРДЕЙКЕР: Хороший вопрос. Спасибо. Другие вопросы, пожалуйста. Один был здесь и два сзади, Эндрю, когда вы освободитесь.

[КОРИ (CORY)]: Меня зовут [Кори], я из США. У меня вопрос следующий: о DNSSEC нам известно уже несколько лет, но в последнее время начались разговоры о DNS через HTTPS или TLS. Как это соотносится с DNSSEC? Они дополняют друг друга, противоречат, или как они друг с другом соотносятся?

УЭС ХАРДЕЙКЕР: Хороший вопрос. Вы все очень хорошо информированы. Я поражен. Есть ряд аспектов, и они друг другу не противоречат. Они, скорее, дополняют друг друга. DNSSEC подписывает данные, поэтому не имеет значения, как они передаются или где хранятся. Они подписаны, и вы знаете, что запись не была изменена. Есть DNSSEC через TLS, что соответствует актуальной спецификации шифрования и аутентификации трафика между двумя устройствами. DNS через HTTPS выполняет ту же задачу, но отправляет данные через HTTPS, и основное преимущество этого метода заключается в невозможности блокировки брандмауэрами, что обеспечивает нормальный веб-трафик.

Таким образом, существуют разные причины, по которым следует выбирать ту или иную технологию, но основным важным отличием между DNSSEC и другими двумя методами является то, что DNSSEC подписывает данные, и не имеет значения, откуда они поступили — они достоверны. Таким образом, их целостность защищена. Если вы используете DNSSEC через TLS или HTTPS, вы знаете, что одна транзакция — это хорошо, но у вас нет истории получения этих данных.

Таким образом, DNS использует много разных транзитных шлюзов. В большинстве случаев, например, если вы

используете DNS через HTTPS для общения с провайдером, который предоставляет такие услуги, вы не знаете, что именно они делают и не можете быть уверены в том, что они получают правильные данные и проверяют их. Авторитативные серверы еще не используют метод DNS через TLS или HTTPS.

РАСС МАНДИ: Кое-что в связи со встречей в среду. В среду будет встреча по DNSSEC, и на ней будет презентация по этой теме.

УЭС ХАРДЕЙКЕР: Среда — отличный день. Если вам нужно знать больше о DNSSEC, среда как раз будет посвящена этому.

РАСС МАНДИ: Позвольте подытожить сказанное: DNSSEC предназначены для защиты данных. DNS через зашифрованный протокол предназначена для защиты конфиденциальности вашего запроса, в этом и отличие.

УЭС ХАРДЕЙКЕР: Да. За вами, Эндрю. Следующий, сзади. Хорошо.

[БАЛГИШНЕР (BALGISHNER)]: Здравствуйте, меня зовут [Балгишнер], я из Непала. DNSSEC предназначены для защиты конечного

пользователя, правильно? Существуют ли какие-то сложности, чтобы сделать DNSSEC... может быть, не обязательными, но установить, например, конечные сроки, когда все должны перейти на DNSSEC? Есть ли в этой связи какие-то сложности?

УЭС ХАРДЕЙКЕР: Это сложно, потому что мы живем в свободном мире и люди сами вольны выбирать, использовать DNSSEC или нет. Есть всем известная фраза: интернет-политики не существует. Никто не решает, что в Интернете хорошо, а что плохо. Поэтому вы сами можете выбирать технологии и сами выбираете сайты, которые используют эти или подобные технологии. Так что, к сожалению, нет способа заставить кого-то использовать DNSSEC. Если бы все было иначе, было бы проще. Но нет.

РАСС МАНДИ: У меня есть один комментарий: некоторые организации решили внедрить политики безопасности, предписывающие необходимость использования технологий безопасности. Поэтому некоторые организации решили их внедрить, но нет единого ответа на все вопросы.

УЭС ХАРДЕЙКЕР: Очень хорошее замечание, и некоторые правительства решили, что вся их инфраструктура должна использовать DNSSEC. Это наглядный пример. Спасибо, это очень хорошее замечание.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Здравствуйте, меня зовут [неразборчиво], я из Шри-Ланки. У меня есть краткий вопрос. DNSSEC нарушает нормальный поток DNS. Когда это происходит, замедляется ли Интернет? Если да, то как и насколько?

УЭС ХАРДЕЙКЕР: Если я вас правильно понял, вас беспокоит снижение скорости из-за того, что DNSSEC выполняет валидацию. Отличный вопрос. Несколько моментов. Прежде всего, DNSSEC немного замедляет работу, поскольку выполняет несколько дополнительных запросов. Есть множество исследований. Вы можете найти эти исследования со всеми показателями.

Это самый важный момент. Данные DNS кэшируются, и я уже упоминал об этом на одном из слайдов, но особо мы на этом не останавливались. Аспекты безопасности также кэшируются, то есть, когда вы ищете bigbank.com, все эти записи снабжаются временными ссылками, сохраняемыми на протяжении определенного вами времени. Повторная валидация каждый раз не

выполняется. После первой валидации данные помещаются в кэш, помечаются как безопасные и остаются доступными на протяжении длительного времени. Что хорошо, когда речь идет о DNS, это то, что первый человек, который переходит по адресу, может наблюдать небольшое замедление, тогда как все последующие получают кэшированные данные, и очень быстро. Хороший вопрос.

[КРИСТИАНА (CHRISTIANNE)]: Меня зовут [Кристиана], и я из Берега Слоновой Кости. Я хочу кое-что уточнить: у меня не много технических навыков, поэтому мой вопрос может звучать немного глупо.

УЭС ХАРДЕЙКЕР: Нет, все нормально. Продолжайте.

[КРИСТИАНА]: Я хочу знать: если происходит перехват DNS, есть ли какая-то процедура, которая позволяет DNSSEC разрешить проблему? Были ли случаи, когда вам приходилось выполнять нарушения и действовать напрямую?

УЭС ХАРДЕЙКЕР: Вы озвучили очень сложную проблему, с которой сталкиваются множество функций безопасности во многих протоколах и даже физических системах. Люди не защищают свои системы, вплоть до момента, когда становится слишком поздно.

Итак, вы спрашиваете, если ваш дом взломан и ваши деньги украдены, что вы можете сделать? Ничего. Вам нужно было заранее установить более надежные замки на ваших системах, чтобы предотвратить произошедшее. DNSSEC не может исправить проблему, если DNS взломана. Хорошая новость заключается в том, что таким же образом срок хранения кэша со временем истекает, плохие данные исчезнут и ваши пользователи начнут получать хорошие данные. Но в реальности, если вы хотите защитить свои данные DNS уже сегодня, вам нужно развернуть DNSSEC до того, как эти проблемы возникнут. Понимаете? Спасибо.

АБРАХАМ (ABRAHAM): Меня зовут Абрахам, и я из Нигерии. Я хочу спросить, должны ли мы поднять требования к аппаратному обеспечению системы при внедрении DNSSEC, или мы можем пользоваться тем, что у нас было до начала внедрения? Спасибо.

УЭС ХАРДЕЙКЕР: Если я правильно расслышал, потому что у меня тут мощное эхо, я стою возле этого монитора. Вы спрашиваете о том, повышаются ли требования к оборудованию для внедрения DNSSEC? Это так? Более мощный процессор и больше памяти, так? Да, понятно, хорошо.

РАСС МАНДИ: По этому вопросы было проведено несколько разных анализов. В основном они выполнялись людьми, сосредоточенными на уровне домена верхнего уровня или корня. Если вкратце, то достаточно придерживаться нормального цикла развития и замены оборудования.

Каковы же количественные показатели? Насколько я помню, влияние оборудования на возможность подписи может составлять от 3 до 8%, но это не на сегодня. Вы подписываетесь до загрузки зоны. Для валидации цифры примерно такие же. Может быть около 10%, но этот фактор не оказывает существенного воздействия, скорее его следует учесть в рамках имеющейся программы обновления оборудования инфраструктуры DNS.

УЭС ХАРДЕЙКЕР: Спасибо. Также следует отметить тот факт, что требования к памяти возрастают, поскольку количество записей увеличивается и так далее. Вам понадобится чуть больше памяти. Я, например, обслуживая около 20 зон,

никогда не покупал новое оборудование для развертывания DNSSEC для выполнения своих проектов. Если речь идет о крупном домене верхнего уровня со множеством записей, вам нужно учесть этот аспект, но, может быть, не в каждом случае, все будет работать на имеющемся оборудовании без проблем.

[ПОЛ (PAUL)]: Здравствуйте, меня зовут [ПОЛ], я из Великобритании. Есть ли механизмы, предусмотренные политикой, для отслеживания мониторинга нарушений DNS на уровне доменов верхнего уровня или реестров?

УЭС ХАРДЕЙКЕР: Для мониторинга чего? Сегодня мы говорим о DNSSEC. Речь идет о мониторинге эффективности безопасности или данных, которые они [распространяют]?

[ПОЛ]: Мониторинге базы данных нарушений для отсеивания плохих парней?

УЭС ХАРДЕЙКЕР: Очень сложно мониторить неправильное использование, потому что для этого вам нужно мониторить весь мир. Я могу выполнять мониторинг непосредственно возле домена верхнего уровня и проверять, распространяют ли

они правильную информацию, но на этом уровне атаки, как правило, не выполняются. Атаки происходят [на ваших конечных пользователей] и так далее, поэтому, в конце концов, вам нужно мониторить каждого интернет-провайдера в мире. Это очень сложный вопрос. Если вы хотите более подробно обсудить этот вопрос, обращайтесь ко мне, поскольку это сложная проблема и, если бы у нас были ответы, мы бы уже отловили всех плохих парней.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Спасибо. Хочу немного дополнить предыдущий ответ относительно требований к оборудованию при внедрении DNSSEC: Сетевой информационный центр Чешской Республики, nic.cz, регулярно публикует критерии для серверов DNS и DNSSEC. Найдите меня потом. Я покажу вам эту ссылку, так что влиянием оборудования можно пренебречь. Оно небольшое и вы ничего не заметите, если только на одном устройстве у вас не будет нагрузки в миллион запросов в секунду.

УЭС ХАРДЕЙКЕР: Хорошо, большое спасибо. Эндрю, вот здесь.

[БРОУНВИН (BRONWYN)]: Здравствуйте, меня зовут [Броунвин], я из Австралии. У меня вопрос: в показанной вами пьесе резолвер

выполнял валидацию сертификата на каждом уровне домена. Есть ли какие-то обязательные обновления или изменения ПО на уровне резолвера для обеспечения поддержки такой дополнительной валидации? Я спрашиваю, потому что резолвер, как я понимаю, будет предоставлять резолюции для доменов с поддержкой DNSSEC и без нее.

УЭС ХАРДЕЙКЕР: Это очень хороший вопрос. Хорошая новость заключается в том, что большинство современного ПО резолверов имеет поддержку DNSSEC, например BIND и unbound (они самые известные). Не помню версии unbound, но оба эти ПО поддерживают каждую важную функцию DNSSEC в течение последних 5 или 10 лет. Так что, при покупке чего-то нового или даже получении чего-то через платформу сервера интернет-провайдера, например, ОС (я могу гарантировать, что резолверы Windows тоже это делают), проблем не будет. Наша система не такая уж и новая.

[КРЕДЖАН (CREJAN)]: Здравствуйте, спасибо. Меня зовут [Креджан], я из Науру. Мне кажется, это DNSSEC для чайников, поэтому я хочу задать глупый вопрос. С точки зрения интернет-провайдера, существуют ли какие-либо индикаторы или красные флажки, которые свидетельствуют о том, что требуется DNSSEC?

УЭС ХАРДЕЙКЕР: Это очень хороший вопрос. Именно интернет-провайдеры должны внедрить валидатор, вы видели моего друга Воррена, который ходил во время пьесы от человека к человеку. Они должны проделать основную работу. Они должны общаться с корнем, доменами верхнего уровня и серверами, и они должны заботиться о том, чтобы их ПО могло обрабатывать безопасные и небезопасные поиски, поскольку в реальности вы не можете заставить активировать DNSSEC, пока весь мир не станет безопасным.

Следует отметить, что мы не говорили об этом на слайдах и в пьесе, но DNSSEC сама по себе даст ответ: «Я безопасна. Небезопасен другой сервер, который вы спрашиваете. Моя проверка показала, что он небезопасен, так что решайте сами». Есть встроенные методы, обеспечивающие частичную безопасность, и именно так, пройдя до конца, вы можете понять, в безопасности вы или нет.

Интернет-провайдер должен проверять свои журналы и убедиться, в частности при обнаружении ошибок валидации, что произошла атака или в Интернете может быть проблема. Проверка журналов очень важна, независимо от того, пытаетесь ли вы внедрить безопасные технологии или нет.

[АЛФИФА (ALFIFA)]: Здравствуйте, меня зовут [Алфифа], я из Бангладеш. Я не знаю, стоит ли вам задавать этот вопрос.

УЭС ХАРДЕЙКЕР: Если я не смогу ответить, то он сможет.

[АЛФИФА]: Вопрос в следующем: если вы сталкиваетесь с серьезной аварией после обновления ключа для подписания ключей, как вы с этим справляетесь?

УЭС ХАРДЕЙКЕР: Хороший вопрос. Вопрос подводит нас к встрече, посвященной DNSSEC, и состоит в том, были ли проблемы после обновления ключа для подписания ключей, и что вы делали с этим?

РАСС МАНДИ: Спасибо. Простите, не расслышал. Акустика здесь немного сложная. В любом случае, обновление ключа для подписания ключей в рамках многих анализов не учитывалось, а после отзыва старого ключа был отмечен ряд отличий объема трафика. Тем не менее, мы планируем провести встречу по этому вопросу, и там будет представлена определенная информация в этой

связи. По факту же, с эксплуатационной точки зрения не было выявлено никакого существенного влияния на обновление ключа для подписания ключей. Это, по всем показателям, был успех с эксплуатационной точки зрения. Это был огромный успех.

УЭС ХАРДЕЙКЕР: Есть еще много презентаций, которые вы можете посмотреть в рамках этой и предыдущих конференций по DNSSEC, посвященных тому, почему обновление ключа для подписания ключей было отложено на год. Также там вы найдете некоторые открытия. Многие презентации представлены мною, многие — другими людьми. В среду мы, наверное, представим последний набор презентаций, посвященных этой теме, потому что мы немного переделали то, что было представлено 11ro января, и это был последний этап обновления ключа. Мы получили ряд интересных данных, на которые стоит взглянуть. Найдите меня позднее, если вам нужен список URL-адресов. Я могу прислать вам видео, которые вы можете посмотреть позднее, если вы устали. Видео хорошие. Есть еще вопросы? У нас осталось немного времени.

Ладно. Я не вижу больше рук, поэтому благодарю всех вас за вдумчивые вопросы. Вы, и я не шучу, едва ли не сама информированная аудитория, с которой мы встречались. Все ваши вопросы отличались высоким техническим

уровнем и свидетельствуют о том, что вы заранее сделали свою домашнюю работу. Не бывает глупых вопросов. Если хотите, позднее вы можете обратиться ко мне с любыми вопросами. Нужно какое-то время, чтобы понять все аспекты этой технологии, и мы занимаемся этим уже более 10 или даже 20-ти лет. Поэтому забудьте о том, что какие-то вопросы могут быть глупыми. Все вопросы стоят того, чтобы их задавать, и вам предстоит узнать еще многое.

Многие из нас будут здесь и в дальнейшем. Не стесняйтесь подходить к нам и задавать вопросы. А сейчас желаю вам с пользой провести время на этой конференции ICANN и приглашаю вас на встречу по DNSSEC, которая пройдет в среду. Если сможете, то приходите, там будет много интересного. Также приглашаю вас на технический день, который часто проводится по понедельникам. Большое спасибо.

[КОНЕЦ СТЕНОГРАММЫ]