МОНРЕАЛЬ – «Принципы работы: Функционирование корневых серверов
Воскресенье, 3 ноября 2019 года, 15:15–16:45 по EDT
ICANN66 | Монреаль, Канада

СТИВ КОНТЕ: Мы собираемся начать через несколько минут. У нас больше места в зале, чем нам нужно. Если вы, ребята, хотите подойти ближе, это здорово, тогда мы могли бы вас увидеть. Мы собираемся сделать это следующим образом, RSSAC собирается провести презентацию, а затем у нас будут блоки для вопросов, и мы обратимся к вам за вопросами. Я уже выполнил свою норму по шагам на сегодня, так что чем ближе вы, тем лучше будет и для меня, и это все обо мне. Мы начнем буквально через минуту.

ЭНДРЮ МАККОНАХИ (ANDREW MCCONACHIE): Здравствуйте, меня зовут Эндрю МакКонахи, я работаю в ICANN, оказываю помощь Консультативному комитету системы корневых серверов, и сегодня я расскажу об учебном пособии по системе корневых серверов - по-моему, это вот здесь. Мне нравится ходить по помещению, поэтому я не собираюсь садиться, я прошу прощения у удаленных участников, камера должна следовать за мной или как-то так. Я обещаю, что презентация намного интереснее, чем любые мои фотографии, поэтому мы просто продолжим.

Я собираюсь делать это по согласованию с моим коллегой Озаном Сахином, который будет заниматься второй частью.

Сначала я проведу обзор DNS, который, вероятно, станет существенным обзором для многих людей в этой комнате, потому что, как я понимаю, у вас уже был DNS101, но мы затронем это. Затем я расскажу об Anycast и о том, чем Anycast отличается от Unicast, и почему это важно для системы корневых серверов. Затем я перейду к современной системе корневых серверов, приведу примеры и немного расскажу об истории. После этого Озан расскажет о RSSAC, группе подготовки RSSAC и о текущей работе по развитию системы корневых серверов. Итак, приступим.

Обзор DNS. Я предполагаю, что большинство людей в этой комнате уже знают об идентификаторах в интернете и о различных видах идентификаторов. На этом слайде просто говорится об IP-адресах и их важности для интернета. Всем хостам, подключенным к интернету, требуется IP-адрес, есть два разных типа, IPv4 и IPv6. Это числовая метка, это не имя. Это фундаментальный идентификатор для интернета.

Почему DNS? В чем была проблема с использованием только IP-адресов? IP-адреса трудно запомнить, они часто меняются. Существуют и современные проблемы, возникшие после введения DNS, которые заключаются в том, что IP-адреса могут быть общими. Клиенты могут иметь несколько IP-адресов, серверы могут иметь несколько IP-адресов, хосты могут иметь более одного IP-адреса, так какой из них вы используете? Вы можете использовать систему имен, чтобы помочь с этой проблемой.

Как вы, вероятно, узнали из обсуждения DNS101, презентации, система DNS является иерархической, у нее

есть корень вверху, под ним есть так называемые домены верхнего уровня, вот несколько примеров: .UK, .ORG, .EDU, и под ними есть второй уровень и затем третий уровень и так далее. Можно считать, что существует сопоставление между именами и IP-адресами, которое, вероятно, будет называться отображением A или Quad A, если вы знакомы с этими терминами. Есть и другие сопоставления, имена также сопоставляются с именами почтовых серверов, есть также обратный поиск DNS.

Здесь у нас есть несколько определений, будет два слайда, полных определений, и было бы хорошо, если бы мы ознакомились с ними, прежде чем углубиться в предмет, чтобы люди узнали эти термины. Это некоторые термины, которые RSSAC использует довольно часто, не только в наших документах, но и в этой презентации. Первым, который я уже использовал ранее, является «система корневых серверов», это набор корневых серверов, которые совместно образуют корневой сервер. Мы углубимся в это чуть позже.

Затем есть корневая зона, которая на самом деле представляет собой данные, как на последнем слайде, когда я говорил об иерархии DNS, мы на самом деле говорим о данных, которые система корневых серверов помогает распространять. Корневая зона - это данные, которые система корневых серверов помогает распространять. Она не имеет родителя и содержит всю информацию, необходимую для связи с расположенными ниже доменами верхнего уровня. Наконец, на этом слайде показано зеркало Anycast корневого сервера, все операторы корневого сервера

используют Anycast, когда мы говорим об отдельных серверах или физических машинах, мы на самом деле говорим о зеркалах Anycast.

Здесь у нас некоторые организационные роли. У нас есть администратор корневой зоны, эта организация отвечает за управление данными, содержащимися в корневой зоне. По сути, это функция IANA, и это включает назначение оператора доменам верхнего уровня и ведение их технических административных данных, а это означает, что способы разрешения домена верхнего уровня требуют наличия сервера для этого домена верхнего уровня, который может отвечать на запросы, и люди, управляющие этим доменом верхнего уровня, иногда могут обновлять информацию о том, что это за сервер, а затем они должны поговорить с администратором корневой зоны.

Есть также специалист по обслуживанию корневой зоны, в настоящее время это Verisign, эта организация отвечает за прием данных от администратора корневой зоны, а затем форматирование их в файл зоны и, что наиболее важно, за криптографическую подпись, а затем - распространение их среди операторов корневого сервера. Операторы корневых серверов, их 12, и это организации, отвечающие за управление услугами корневой зоны по IP-адресам, указанным в корневой зоне и файле корневых ссылок. Это отдельные организации, которые управляют физическими корневыми серверами.

Я уже немного говорил об этом, здесь мы говорим о разнице между данными и тем, как получить данные. Есть серверы,

которые предоставляют данные, и есть сами данные. Корневая зона - это данные, это файл зоны, затем система корневых серверов состоит из RSO, у которых есть серверы, которые затем обслуживают эти данные. Этот слайд сравнивает два понятия. Можно рассматривать корневую зону как отправную точку. Это список TLD и их DNS-серверов, для разрешения. Вы должны перейти на DNS-серверы TLD, чтобы разрешить имена под этими TLD. Корневая зона управляется ICANN в соответствии с политикой сообщества.

Как указано на последнем слайде, специалист по обслуживанию корневой зоны обеспечивает соответствие требованиям и распространение всем RSO; корневые сервера предоставляют информацию. Система корневых серверов - это система, состоящая из серверов, которая передает данные из корневой зоны в ответ на запросы. В настоящее время существует 26 IP-адресов, которые составляют систему корневых серверов, 13 для IPv4 и 13 IPv6, и существует более 1000 физических зеркал. Количество меняется, оно постепенно растет со временем. Сейчас мы просто говорим - более 1000. У нас был слайд, в котором было указано точное число, а затем нам приходилось обновлять его, поэтому мы решили: «Хорошо, теперь есть чуть более 1000». Это чисто техническая роль - обеспечивать работу корневой зоны, и ответственность за нее несут операторы корневых серверов.

Этот слайд рассматривает все детали DNS-запроса и ответа. Я собираюсь потратить некоторое время на этот слайд и просто показать, что происходит с компьютером, когда он

хочет разрешить имя, и он проходит через рекурсивный DNS-сервер.

Если мы начнем справа, мы увидим, что у нас есть наш пользователь, у нас есть наш интернет-пользователь, также известный как клиент, и они используют компьютер, и они хотели бы попасть на сайт www.example.com. Теперь, если предположить, что этот рекурсивный сервер только что включен и в его кэше ничего нет, то есть он по сути невежественный и ничего не знает кроме того, как добраться до корневых DNS-серверов. Этот пользовательский компьютер прежде всего свяжется с этим рекурсивным DNS-сервером, который расположен в середине изображения, и он отправит запрос на этот рекурсивный DNS-сервер, говорящий: «Эй, какой IP-адрес у www.example.com?»

И этот рекурсивный DNS-сервер, поскольку он только что включен и у него ничего нет в кэше, сначала свяжется с системой корневых серверов, с корневым DNS-сервером. Скорее всего, он отправит весь запрос на этот корневой DNS-сервер и просто спросит: «Эй, какой IP-адрес у www.example.com ?» И этот корневой DNS-сервер скажет: «Я не знаю адрес www.example.com, но я знаю, как вы можете общаться с .COM и, кстати, вот подпись для этих данных».

И он отправит его обратно на рекурсивный DNS-сервер. И рекурсивный DNS-сервер затем говорит: «Хорошо. Теперь я знаю, как добраться до .COM, и у меня к тому же есть эта подпись, я сравню ее криптографически с публичной частью ключа для подписания ключей корневого KSK, который находится на рекурсивном DNS-сервере, и определю, что да,

этот ответ от корневого DNS-сервера о расположении .COM правильный, теперь я свяжусь с .COM».

Затем рекурсивный DNS-сервер отправляется к DNS-серверу домена .COM и спрашивает: «Где находится www.example.com?» DNS-сервер .COM отвечает: «Я не знаю, где это, но я знаю, где находится example.com, и, кстати, вот подпись для этих данных». Тогда рекурсивный DNS-сервер будет делать в основном то же самое, он скажет: «Хорошо. У меня есть example.com, я могу проверить это с помощью криптографических подписей». Затем он отправится на DNS-сервер example.com и, наконец, получит ответ для www.example.com вместе с подписью. Он возвращается к рекурсивному DNS-серверу, рекурсивный DNS-сервер говорит: «Отлично, теперь у меня есть IP-адрес для www.example.com, и у меня есть подпись, и я сделаю криптографическое сравнение. Отлично, она подтверждается».

Только теперь рекурсивный DNS-сервер возвращается к пользователю или обратно к компьютеру пользователя и говорит: «Вот ваш IP-адрес». Здесь показано, что простой запрос, инициированный пользователем, активирует рекурсивный, итеративный, сложный и длительный процесс, который выполняется на рекурсивном DNS-сервере, и пока он не завершит его, он фактически не вернется к пользователю.

Это чуть более подробно о том, о чем я только что говорил. Корневые серверы знают только, какие серверы должны быть запрошены далее. В последнем примере они знали только, как добраться до серверов .COM. Они не знают, как

разрешить имя целиком. Однако на рекурсивных серверах они будут запоминать эти ответы и кэшировать их.

На самом деле им не нужно часто заходить на корневые серверы, а время существования, часто называемое «TTL» для этой кэшированной информации, составляет два дня. Рекурсивный сервер спросит у корневого сервера, где, например, находятся DNS-серверы .COM, он запомнит эту информацию на два дня, и, вероятно, затем ему не придется запрашивать снова, пока срок действия информации не истечет.

Современные DNS имеют некоторые усовершенствования. Мы говорили о криптографической подписи данных DNS. Это все определено в DNS Sec или расширениях безопасности для DNS. DNS Sec просто используется в качестве краткого термина для обсуждения всех процессов подписания и проверки, необходимых для криптографического обеспечения того, что рекурсивные серверы и клиенты получают правильную информацию от серверов. В последнее время произошли некоторые улучшения конфиденциальности в DNS, поскольку запросы могут допускать утечку информации. Оригинальный или традиционный DNS сообщит о том, что 53 UDP или TCP был просто открытым текстом, существуют стандарты по шифрованию транспорта DNS. У нас также есть «DNS по TLS», также есть «DNS по HTTPS».

Anycast - это еще одно современное усовершенствование. На данный момент у всех операторов корневых серверов, которые внедрили Anycast, у нас есть целый раздел, посвященный Anycast, мы можем поговорить об этом тогда.

Это подводит меня прямо к объяснению Anycast. Вначале был только Unicast. Unicast означает, что все пакеты из источников отправляются в один и тот же пункт назначения, есть один пункт назначения, а пакеты из всех источников направляются в этот пункт назначения.

По сути, IP-адрес соответствует одному серверу, он соответствует одной конечной точке. Это хорошо, если не требуется масштабирование. Anycast обеспечивает масштабируемость, значительно упрощает масштабируемость, и это важно, если вы хотите расширить обслуживание, если вы получаете больше действительных запросов. Также очень хорошо, если люди запускают распределенные атаки типа «отказ в обслуживании» на ваш сервис, и вы хотите, чтобы часть этого трафика была выгружена на множество разных серверов, просто становится намного проще справиться с этим.

В Anycast сопоставление между IP-адресом и конечной точкой меняется, и теперь у вас есть один IP-адрес, сопоставленный нескольким серверам и нескольким конечным точкам. Разные источники будут попадать в разные пункты назначения, но все они все еще обмениваются данными или отправляют трафик на один и тот же IP-адрес, просто он попадает в разные физические пункты назначения. Источники получают данные быстрее, промежуточных переходов меньше, потому что источники могут быть ближе к своим пунктам назначения. Трафик DDoS-атаки будет, как мы называем, «слит» - отправлен ближайшему зеркалу, и не будет нарушать работу других зеркал.

Вот довольно простой пример трафика Unicast, и есть единственный кратчайший маршрут к одному пункту назначения. У нас есть один источник, и у нас есть один пункт назначения. Если вы добавите сюда другой источник, он пойдет в тот же пункт назначения. Вот Anycast, у вас есть несколько пунктов назначения, это фиолетовая или синяя капля, помеченная как пункт назначения. У нас все еще есть только один источник, но вы можете себе представить, если другой источник, находящийся ближе к другому пункту назначения, идет к этому другому пункту назначения. Это позволяет - просто намного проще распределять трафик.

Вот одно из реальных преимуществ, одно из главных преимуществ Anycast в том, что происходит при распределенных атаках типа «отказ в обслуживании» - источники, использующие пункты назначения, удаленные от DDoS-атаки, не затрагиваются ей. Если это локальная, в некотором смысле локальная или географически или топологически локальная атака, она будет «слита» на одном сервере и не повлияет на операции и остальной мир. Это одно из больших преимуществ Anycast.

Теперь я расскажу немного об истории системы корневых серверов и сегодняшнем состоянии системы корневых серверов. В 1983–86 годах система корневых серверов имела четыре адреса, и с тех пор она постоянно увеличивалась до 1998 года, когда стало 13 адресов. Возможно, слово «адреса» не совсем подходящий термин, но вы можете видеть, что эти изменения растут со временем, и в настоящее время, поскольку был добавлен IPv6, мы теперь говорим, что

система корневых серверов имеет 26 адресов. 13 IPv4 и 13 IPv6. Благодаря Anycast мы можем сказать, что существует 26 IP-адресов, 13 IPv4, 13 IPv6, фактически более 1000 физических зеркал.

Это список имен хостов и адресов IPv4 и IPv6, а также менеджера, оператора корневого сервера для текущей системы корневых серверов. Все операторы, все имена хостов имеют адреса IPv4 и IPv6, связанные с ними. Вы можете видеть, что они маркированы буквами от A до M.

Эта карта взята с root-servers.org, она может быть неточной, географически неточной. Вы можете сделать следующее: если вы зайдете на root-servers.org, вы можете посмотреть ее, она находится прямо на главной странице, а затем вы можете фактически отследить отдельные города, вы можете посмотреть на континент, а затем на страну, а затем на город, а затем посмотреть, какие операторы управляют серверами или рабочие зеркала в этих городах. Это на самом высоком уровне, когда вы полностью уменьшаете масштаб, картографическое программное обеспечение просто группирует объекты.

По сути, это показывает, что есть зеркала во всем мире, на каждом континенте, я не должен говорить так, потому что я не знаю, есть ли такое зеркало в Антарктике, может кто-то может поправить меня, но по крайней мере на каждом континенте, кроме Антарктики. Если вы заинтересованы в более подробном изучении этого вопроса, интересно перейти на root-servers.org, детально изучить карту и посмотреть,

в каком городе рядом с вами есть зеркала корневых серверов, кто ими управляет и тому подобное.

Это показывает процесс изменений в корневой зоне и то, как они реализованы в фактических корневых серверах, а также, как их получают резолверы. Слева находятся операторы TLD. Допустим, что оператор TLD должен сделать запрос на изменение, он связался бы с IANA и сказал бы IANA: «Наш TLD, наши DNS-серверы, мы используем этот IP-адрес, мы хотели бы изменить их на этот другой IP-адрес».

И они скажут это IANA, а затем IANA проведет ряд процедур проверки, чтобы удостовериться, что она действительно разговаривает с оператором TLD, что это хорошее изменение, это ничего не сломает. Как только IANA одобрит это изменение, мы передадим его, когда IANA сообщит специалисту по обслуживанию корневой зоны: «Вот новый файл корневой зоны». Он просто обновит эту информацию и следующий файл корневой зоны, который поступит специалисту по обслуживанию корневой зоны. Специалист по обслуживанию корневой зоны, который соответствует корневой зоне и криптографически подписывает его, а затем распространяет его среди операторов.

Затем, справа, все эти маленькие пузырьки с «RS», которые должны представлять отдельные зеркала, их очень много для каждого оператора. Затем справа мы видим рекурсивные резолверы, отправляющие запросы и получающие ответы. Так происходит изменение информации, очень общее описание того, как меняется информация в корневой зоне, и процесс для этого.

Дополнительная информация об операторах корневых серверов, как я уже сказал, их 12, и они в первую очередь ориентированы на надежность, стабильность и доступность для всех интернет-пользователей. Они сотрудничают друг с другом через RSSAC и Root Ops и другие площадки. Сосредоточены на профессионализме и есть разные виды организаций, не все они некоммерческие, не все они правительственные, это разные виды организаций, и они разнообразны с точки зрения технической, организационной, географической, моделей финансирования.

Это некоторые из способов их координации. Я упомянул некоторые из различных отраслевых форумов и органов, таких как ICANN и RSSAC, ITF, конференции RIR, группы сетевых операторов, DNSORC, и они также используют другие различные виды инструментов, как и любые организации, которые должны координировать свои действия. Они обмениваются данными друг с другом, а также проводят периодические мероприятия, такие как «настольные учения» и все, что нужно для планирования аварийных операций и так далее.

RSO связаны с эксплуатацией и развитием сервиса. Оценка и развертывание предлагаемых технических модификаций, возможно, протокола, такого как протокол DNS. Для этого они участвуют в IETF. Убедиться, что поддерживается стабильность, надежность и доступность. Однако операторы не вовлечены в формирование политики и они не участвуют в модификации данных. RSO просто публикуют данные, они не имеют отношения к содержанию данных.

На этом слайде показаны некоторые из мифов, с которыи RSSAC и я сталкивались на протяжении многих лет, а также реальность. Первый миф состоит в том, что корневые серверы контролируют, куда идет интернет-трафик; в реальности направление трафика контролируют маршрутизаторы пакетов. Корневые серверы просто отвечают на запросы с рекурсивных серверов.

Другой миф состоит в том, что большинство DNS-запросов обрабатываются корневым сервером, и большинство DNS-запросов не обрабатываются корневым сервером, главным образом из-за кэширования, поскольку рекурсивные серверы просто запоминают ответы, полученные от корневых серверов, поэтому им не нужно задавать каждый раз один и тот же вопрос. Другой миф состоит в том, что администрирование корневой зоны и предоставление услуг - это одно и то же. Опять же, это восходит к разнице между данными и обслуживанием данных. Администрирование данных сильно отличается от ответов на запросы о данных.

Другой миф состоит в том, что некоторые из идентификаторов сервера имеют особое значение. Ни у кого из них нет особого значения. Другой миф состоит в том, что есть только 13 корневых серверов. Нет, из-за Anycast их более 1000, но есть только 13 технических идентификаторов. Операторы корневых серверов не работают полностью независимо, они взаимодействуют друг с другом, о чем мы говорили на последнем слайде. На этом последнем, операторы корневых серверов получают только часть запроса, относящуюся к TLD.

Когда я рассмотривал весь процесс разрешения DNS, у меня была вся строка запроса, идущая к корневому серверу, и это традиционно работает таким образом, и, вероятно, так работает в 90 процентах случаев. Поэтому, как правило, это смело, есть новая технология, называемая QNAME Minimization, это новая технология обеспечения конфиденциальности, я думаю, мы могли бы назвать ее выходящей из IETF, которая нацелена на изменение этого, но она не очень широко развернута. Она разворачивается все шире, но в настоящее время реальность такова, что операторы корневых серверов обычно получают весь запрос.

Если вы эксплуатируете сеть, подумайте о вашем DNS и взаимодействии с корневыми серверами. Вы, вероятно, захотите три или четыре зеркала поблизости. Поблизости по своему значению, имеется в виду топологическая и сетевая близость, необязательно географическая близость. Вы можете увеличить количество одноранговых соединений, если у вас возникают задержки. Есть много разных вещей, которые вы можете сделать.

Другой момент - включить резолверы валидации DNS Sec, это может гарантировать, что для данных, подписанных в корневой зоне, вы получаете правильные данные, вы получаете неизмененные данные IANA, между вашим рекурсивным сервером и корневыми серверами и другими авторитативными серверами, никто не вмешивается в передаваемые данные. Проверка DNS Sec для подписанных данных, вы проверяете эти данные в локальном резолвере, это просто помогает.

Если вам интересно, вы также можете принять участие и внести свой вклад в работу Группы подготовки RSSAC, и мой коллега Озан расскажет подробнее о том, что такое RSSAC и Группа подготовки RSSAC.

Если вы являетесь сетевым оператором и заинтересованы в хостинге зеркала Anycast, вы можете поговорить с членом RSSAC после этой презентации, вы, конечно же, можете поднять этот вопрос на этапе вопросов и ответов или отправить письмо по этому адресу: ASK-RSSAC@ICANN.ORG.

Теперь я передаю презентацию моему коллеге Озану Сахину, который рассмотрит организационные аспекты.

ОЗАН САХИН (OZAN SAHIN): Спасибо, Эндрю. Привет всем, меня зовут Озан, я член корпорации ICANN, поддерживаю работу Консультативного комитета системы корневых серверов или RSSAC.

Давайте начнем с роли RSSAC, она узкая. Функция Консультативного комитета системы корневых серверов состоит в предоставлении сообществу ICANN и Правлению ICANN рекомендаций касательно работы, администрирования, безопасности и целостности системы корневых серверов Интернета.

На этом слайде есть две заметки о том, что RSSAC делает, а что нет. Это комитет, который дает рекомендации в первую очередь Правлению ICANN, а также другим органам ICANN и другим организациям, вовлеченным в общий бизнес DNS.

Операторы корневых серверов представлены в RSSAC, но RSSAC не занимается операционными вопросами.

Если вы посмотрите на организацию RSSAC, она состоит из назначенных членов, назначенных представителей операторов корневых серверов. У этих представителей также есть дублеры и контактные лица. Кроме того, существует другой орган, который называется «Группа подготовки RSSAC», это группа волонтеров, экспертов в области DNS. Члены Группы подготовки RSSAC утверждаются RSSAC на основании выражения заинтересованности. Если вы хотите стать участником Группы подготовки RSSAC, вы отправляете, как только что рассказал мой коллега Эндрю, ваше заявление о заинтересованности, и RSSAC подтверждает ваше членство.

У нас есть два сопредседателя, они в этой комнате, Брэд Верд и Фред Бейкер. Я также хочу отметить, что RSSAC переходит на модель «председатель/заместитель председателя». К концу года пройдут выборы заместителя председателя. RSSAC будет... руководство будет состоять из председателя и заместителя председателя.

Как я только что сказал, в RSSAC есть представители, четыре из которых являются внутренними и четыре - внешними, то есть есть представитель оператора функций IANA, один от специалиста по обслуживанию корневой зоны, один из Совета по архитектуре Интернета или IAB, а один от Консультативного комитета по безопасности и стабильности, который является еще одним консультативным комитетом в системе ICANN. Существует четыре внешних представителя: один - в Правлении ICANN, один - в Номинационном комитете

ICANN, один - в постоянном комитете потребителей и один - в комитете по анализу изменений корневой зоны (RZERC).

Группа подготовки RSSAC насчитывает более 100 членов, являющихся техническими экспертами DNS. Как я уже сказал, любой желающий подает заявку на членство в группе RSSAC, представив свое выражение заинтересованности, и они получают общественную благодарность за вклад в работу RSSAC. Группа подготовки действительно добавляет транспарентности RSSAC, так что вы можете участвовать в работе RSSAC, войдя в состав Группы подготовки RSSAC. Как я уже говорил, это эксперты DNS, которые делятся своим опытом в публикациях.

В настоящее время в рамках RSSAC действуют рабочие группы. Одним из них ведет изучение алгоритмы работы современных резолверов; она изучает поведение существующего развернутого программного обеспечения и рекурсивных резолверов как на основе кода, так и на основе доступных наборов данных. Другая посвящена ожиданиям системы корневых серверов и связанным показателям. Рабочей группе поручено определить общесистемные, доступные для внешней проверки показатели, способные демонстрировать работоспособность RSS в целом и отправку правильных и своевременных ответов конечным пользователям.

Существуют некоторые инструменты и механизмы, которые способствуют транспарентности RSSAC и операторов корневых серверов. Например, есть веб-страница RSSAC.ICANN.ORG, где вы можете найти имена членов RSSAC, членов Группы подготовки RSSAC, получить доступ к

публикациям. Вы также можете найти протоколы телеконференций RSSAC. Кроме того, RSSAC проводит открытые конференции, если вы заинтересованы, вы можете участвовать в них.

RSSAC также проводит встречи с другими группами ICANN во время открытых конференций ICANN, например, во время этой конференции был проведен брифинг сопредседателей RSSAC для Правительственного консультативного комитета, также Правление ICANN будет проводить встречу с RSSAC, а RSSAC проведет закрытое заседание с Консультативным комитетом по безопасности и стабильности. Это общение с другими группами. У RSSAC есть публикация 000, которая определяет его рабочие процедуры, что также повышает транспарентность.

У RSO тоже есть такие, у них есть веб-страница root-servers.org. Я думаю, что на этой странице можно найти карту, которую только что показал мой коллега Эндрю, с зеркалами по всему миру. Кроме того, у операторов корневых серверов RSO есть свои отдельные страницы, и они публикуют совместные отчеты по основным событиям, Эндрю только что рассказывал об этом, если у вас есть вопросы, вы можете отправить свои вопросы на адрес ASK-RSSAC@ICANN.ORG и получить ответы.

Во второй части презентации я расскажу о работе над развитием системы корневых серверов. Давайте начнем с рассмотрения графика этой работы. Более года назад были опубликованы документы RSSAC037 и 38. В них предлагается новая модель управления системой корневых серверов.

Затем Правление ICANN поручило корпорации ICANN просмотреть эти документы и поработать над ними. В апреле 2019 года корпорация ICANN наконец опубликовала Концептуальный документ. В августе 2019 года завершился период общественного обсуждения Концептуального документа. Были получены консультации от разных групп. Рассмотрев все комментарии, разработаны следующие шаги: к январю 2020 года будет создана рабочая группа по управлению, которая будет заниматься разработкой модели в 2020 и 2021 годах. Ожидается, что к 2022 году новая модель будет реализована.

Давайте посмотрим, что говорится в RSSAC037. В документе определено 11 принципов эксплуатации и развития системы корневых серверов. По сути, он предлагает начальную модель управления для системы корневых серверов и ее операторов. Он также демонстрирует, как модель RSSAC037 работает через набор сценариев назначения и удаления операторов корневых серверов.

На этом слайде вы видите три рекомендации, которые дополняют RSSAC037. Первая заключается в том, чтобы инициировать процесс создания окончательной версии модели на основе 37. Вторая - оценить расходы на разработку модели в системе корневых серверов. Первоначальные усилия также должны быть направлены на разработку графика, а также на внедрение окончательной версии модели, основанной на принципах подотчетности, транспарентности, устойчивого обслуживания и целостности.

На этом слайде вы увидите предложение в виде графика. Вы видите три разных области: одна - это управление, другая - корневые операции DNS, а также ввод и вывод из эксплуатации операторов корневого сервера. В области управления вы видите три заинтересованные стороны: сообщество ICANN, IFT и Совет по архитектуре Интернета и операторы корневых серверов. На слайде также показаны пять функций, предложенных моделью.

А именно, это функция мониторинга и измерения эффективности, функция назначения и удаления, финансовая функция, функция политики в области архитектуры стратегии и функция секретариата. Все пять функций были предложены моделью. Обратите внимание: в нижней части слайда есть некоторые показатели производительности, которые будут использоваться при вводе и выводе из эксплуатации операторов корневого сервера. Это относится к назначению операторов корневых серверов и их удалению.

Мы только что говорили о функциях и, возвращаясь к концептуальной модели, она предполагает следующие структуры, основанные на модели 37, которая соответствует пяти функциям. Одна из них - это Руководящий совет системы корневых серверов, другая - Постоянный комитет системы корневых серверов, Группа экспертов системы корневых серверов, последние две функции - это финансовая функция и функции секретариата, корпорация ICANN.

В концептуальном документе описан процесс, управляемый сообществом, для подготовки окончательного варианта новой модели сотрудничества и управления для RSS, основанный

на рекомендации в RSSAC 38, которая является еще одной публикацией, относящейся к развитию системы корневых серверов. На первом этапе корпорация ICANN рассматривает и оценивает RSSAC037 по указанию Правления ICANN; это сделано.

На втором этапе - рабочая группа по управлению концептуальным документом RSSAC037, документ был доступен для общественного обсуждения, и мы об этом говорили. Третий этап связан с разработкой новой модели сотрудничества и управления для RSS, и здесь есть два направления: одно - структурное, другое - административное. Рабочая группа по управлению (структурное направление) разрабатывает модель, на административном направлении планируется внедрение модели рабочей группы по управлению, возглавляемой корпорацией ICANN.

Что такое рабочая группа по управлению и каков ее состав? В ее состав входят представители RSSAC, Организации поддержки имен ccTLD, Группы заинтересованных сторон-регистраторов и Консультативного комитета по безопасности и стабильности. Также будут представители от Правления ICANN, IANA и специалиста по обслуживанию корневой зоны.

Рабочей группе по управлению поручено разработать детали модели. В концептуальном документе также изложены некоторые руководящие принципы для Рабочей группы по управлению: соблюдение сроков с четкими этапами, открытая и транспарентная работа, поиск информированных источников по мере необходимости, также документ охватывает принципы, изложенные в RSSAC037, и в

основном ссылается на концептуальный документ RSSAC037 и полученные комментарии общественного обсуждения.

Теперь переходим к вопросам и ответам. В зале присутствуют представители операторов корневых серверов, которые являются членами RSSAC. Позвольте мне предложить им выйти на сцену и занять свои места, чтобы отвечать на вопросы аудитории. Будут передвижные микрофоны, если вы поднимете руку, мы дадим вам микрофон, чтобы вы могли задать свой вопрос.

СТИВ КОНТЕ: Пока они его настраивают, у меня есть вопрос, но мы подождем, пока все корневые серверы рассядутся. Наш первый вопрос был здесь, с этой стороны.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: У меня нет технического опыта, но мне интересно, как вы определяете, когда и где вам нужен другое зеркало корневого сервера? Чем он отличается от DNS-сервера и что такое рекурсивного DNS-сервера, и в чем разница между этим и вашим обычным DNS-сервером?

ФРЕД БЕЙКЕР: Мы решаем разместить новый корневой сервер, бросив дротик в доску и посмотрев, куда он попадет. Это не так. У нас на самом деле есть процесс, который мы выполняем, который начинается с потребности. Зачем нам нужен новый корневой сервер? Зачем нам нужен новый RSO? Затем, если на самом

деле есть действительная потребность, существует набор принципов, по которым мы можем определить компанию или организацию, которая может это сделать, которая хочет это сделать. Я бы предложил вам прочитать RSSAC037, где это описано, там есть немало.

УЭС ХАРДЕЙКЕР: Я думаю, Фред, что он спрашивает о зеркале корневого сервера, а не об операторе корневого сервера.

ФРЕД БЕЙКЕР: Да, хорошо. Зеркало корневого сервера: вы можете обратиться к одному из нас, одному из операторов корневых серверов, например, к моей компании ISC. Если вы перейдете на веб-страницу ISC.ORG, вы найдете что-то прямо на странице, где сказано: «Нажмите здесь, если вы хотите новый корневой сервер или зеркало корневого сервера».

И я думаю, что это распространяется на всех нас. Тогда мы поговорим с вами о ваших требованиях. У нас есть некоторые ожидания; нам понадобится подключение к системе как по IPv4, так и по IPv6. Там должна быть адекватная полоса пропускания. Там нужно электричество, такого рода вещи. В конечном итоге мы обмениваемся MOU. Затем начните работать, и мы будем управлять сервером, он будет находиться в вашей стойке, но мы будем управлять им удаленно. По сути, если вам нужен сервер, вы спрашиваете, и мы начинаем этот диалог.

УЭС ХАРДЕЙКЕР: Хотелось бы добавить еще кое-что. Я думаю, вы слышали, что мы получаем требования из разных мест. Мы получаем внешние требования, когда люди создают новые пункты обмена интернет-трафиком и тому подобное, это последнее, что мы разместили - новый пункт обмена интернет-трафиком, который пришел к нам и сказал: «Мы собираемся предложить кое-что совершенно новое, но у нас там ничего нет, вы готовы помочь? «Мы были готовы сделать это, и мы были первыми, но у нас есть внутренние требования в отношении того, как мы анализируем, как мир обслуживается прямо сейчас.

В настоящее время я занимаюсь развертыванием новых систем и пытаюсь охватить географически разбросанные регионы, чтобы обеспечить как можно больший охват. Это сочетание как внутренних, так и внешних показателей, и мы ценим вклад любого, кто считает, что в вашем регионе нет адекватного обслуживания.

БРЭД ВЕРД: Здесь вы слышите разные подходы, потому что у каждого из операторов корневых серверов есть свои особенности. Это может быть основано на потребности, фактической потребности в трафике. Это может быть основано на геополитической необходимости. Есть любое количество различных потребностей, которые оправдывают создание зеркала.

Я думаю, что вторая часть вашего вопроса, в чем разница между рекурсивным резолвером и авторитативным сервером - мы запускаем авторитативные сервер, мы

являемся авторитативными для корня. Ваш рекурсивный резолвер - это то, с чем вы разговариваете внутри своего ISP. Ваш рекурсивный резолвер - ваш посредник между всеми авторитативными серверами.

Например .COM - это авторитативный сервер, корень - это авторитативный сервер, .US и так далее. Вы, по большей части, вероятно, не говорите напрямую с нами, вы говорите со своим рекурсивным, а затем ваш рекурсивный говорит с нами, когда это необходимо, и если ответ еще не кэширован. Надеюсь, я ответила на ваш вопрос.

ОЗАН САХИН (OZAN SAHIN): У нас есть еще один вопрос здесь.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Спасибо. Я не знаю, если это для комиссии, предыдущего джентльмена или я не в той комнате. Это касается чтения DNS по HTTPS, как я понимаю, Firefox и Chrome будут двигаться в этом направлении в очень короткие сроки, возможно, считанные недели или месяцы. Это означает, что 95 процентов трафика DNS может быть зашифровано, я не знаю. Я вижу, что там кто-то качает головой.

В этом суть моего вопроса: я ничего не знаю о том, как это повлияет на это, как это повлияет на всю презентацию в начале этой встречи о том, как работает DNS, она изменится или просто будет такой же, но скрытой? Я не видел никаких комиссий во всем расписании ICANN, и это кажется чем-то

действительно важным. Если не могу узнать об этом здесь, может, вы, ребята, можете сказать, где я могу узнать об этом?

УЭС ХАРДЕЙКЕР: Я также вхожу в Совет по архитектуре Интернета, который участвует в IAFT, где эта работа продвигается в плане стандартизации. Немного фактов о развертывании Firefox и Chrome. Они делают это совсем по-другому, поэтому не заблуждайтесь насчет того, как это произойдет. Другая вещь, которую они делают, это только между A, веб-браузером и резолвером.

В случае Firefox они выбирают резолвер, затем резолвер по умолчанию запускает мой Cloudeflare, у них будет выпадающее меню в вашей конфигурации, где можно выбрать нужный резолвер, и они по умолчанию его включат в США в этом месяце, что касается остальных стран, они ищут других партнеров для этого. Этот резолвер не использует зашифрованный DNS для остальной части системы и включает в себя корневые серверы, он включает в себя серверы TLD, такие как .COM и серверы ccTLD, example.com и тому подобное.

Chrome, с другой стороны, делает что-то немного другое. Они пытаются выяснить, поддерживает ли резолвер вашего местного ISP DoH, и если да, и если он входит в их утвержденный список, они свяжутся с ISP по DoH. Они не делают то, что делает Firefox, и отправляют все это в одно место. Существует совершенно другая проблема развертывания, и, к сожалению, существует много путаницы,

потому что эта информация меняется так быстро, что даже желание Firefox сделать только США с Cloudeflare было очень недавним решением, и то, что произойдет на следующей неделе, большой вопрос.

Через две недели в IETF будет гораздо более активно обсуждаться вопрос о том, какая Инженерная проектная группа Интернета будет работать в Сингапуре. Вот где идет технический разговор. Через пару месяцев все будет по-другому, сейчас все меняется очень быстро.

БРЭД ВЕРД: Позвольте мне дополнить. Еще раз повторю, сейчас это происходит между клиентом и резолвером, где происходит шифрование, а не между резолвером и авторитативным сервером. Полагаю, об этом говорили в ICANN, в Марракеше была очень интересная тема, поэтому я вернусь к повестке дня в Марракеше.

Я не помню, в какой день это было, но SSAC организовал большую презентацию, и я думаю, что это была CCNSO, там была площадка, где говорят об этом, и они продолжают говорить. Я знаю, что SSAC работает над этим, и параллельно ведется другая работа. На это все обращают внимание.

ФРЕД БЕЙКЕР: Итак, Уэс, позвольте мне задать вопрос о DNSSEC; браузеры обычно не поддерживают DNSSEC, они зависят от того, кто

это делает, поэтому, когда браузер переходит в DoH, проверяется ли DNS?

УЭС ХАРДЕЙКЕР: Отличный наводящий вопрос, Фред. Это очень хороший вопрос. Есть два аспекта безопасности в целом, о которых думает большинство людей. Существует шифрование, другими словами, защищены ли ваши данные, и возникает вопрос, являются ли ваши данные подлинными, действительно ли это правильные данные? Они могут быть зашифрованы, и все равно быть неправильными. Например, вы можете получить неправильный зашифрованный файл.

В DNSSEC защита начинается от источника, от того места, где были созданы данные, в данном случае это IANA и через специалиста по обслуживанию корневой зоны, который подписывает эти данные, остальные данные корневой зоны и, фактически, большинство TLD и все остальное, что подписывается ниже, не имеет значения, вы могли бы фактически передать это мне на бумаге, я мог бы прочитать и отсканировать его, и я могу проверить подпись, сравнив ее в том месте, где она была первоначально создана в IANA и во всех остальных местах вниз по дереву.

Главный вопрос Фреда заключался в том, что DoH также обеспечивает целостность, но только между двумя точками, поэтому, если та организация наверху, тот резолвер, с которым вы небезопасно разговаривали, он не узнает и передаст его вам непроверенным способом. Некоторые распознаватели DoH будут выполнять проверку DNSSEC.

Если вы знаете, что разговариваете с резолвером DoH по защищенному каналу с защищенной целостностью и знаете, что они выполняют проверку, вы, вероятно, в безопасности от начала до конца. Cloudflare - это один из резолверов, который, по моему мнению, выполняет проверку по умолчанию, а об остальных я не знаю.

БРЭД ВЕРД: Но это стоит проверить, если вы занимаетесь этим.

СТИВ КОНТЕ: Это быстрое продолжение, которое у вас есть? Хорошо.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: ISP больше не видит данные в среде HTTPS, они больше не могут видеть ошибки? Все, что проходит через их сеть, но вы, ребята, все еще можете это видеть? Кто еще сможет увидеть - кто будет видеть запросы DNS, а кто нет в мире DNS или HTTPS?

УЭС ХАРДЕЙКЕР: Сегодня очень сложно ответить, потому что, как я сказал, в следующем месяце, вероятно, все будет иначе. Это верно для людей, использующих Firefox, который общается с провайдером DoH где-то еще, но тот провайдер DoH, как Cloudeflare, сможет это увидеть. Оттуда он распространяется по всему... в какой-то момент вы должны задать кому-то вопрос, в какой-то момент вы должны обратиться к кому-то и сказать: «Я должен задать вопрос».

Человек, которому нужно задать вопрос, например, где находится этот сайт, они всегда смогут его увидеть. Всегда есть кто-то, кто должен знать ответ на ваш вопрос. Для Chrome, с другой стороны, поскольку они станут DoH для ISP, для вашего резолвера у вашего ISP, это не изменит видимость ISP.

Это сильно зависит от ситуации развертывания, и Chrome и Firefox делают разные вещи. С другой стороны ваш почтовый клиент, например, нет никаких планов, чтобы ваш почтовый клиент поддерживал DoH. Если вы работаете с почтой внутри веб-браузера, тогда это будет. Это очень... это не тот вопрос, на который можно ответить «да» или «нет». Понимаете?

ФРЕД БЕЙКЕР: Итак, сейчас стоит упомянуть о QName Minimization. Это проект, над которым работают в IETF и который когда-нибудь выльется в программное обеспечение рядом с вами. Идея состоит в том, чтобы выдать как можно меньше информации и все же получить ответ на вопрос. Если бы я искал, например, www.example.com, я мог бы спросить мой рекурсивный сервер, и рекурсивный сервер сказал бы: «Я не знаю, где находится .COM, я еще не понял этого».

Таким образом, теперь он вместо отправки полного имени на корневой сервер, что он и делает сейчас, отправляет COM на корневой сервер, корневой сервер будет знать, что он запрашивает .COM, и выдаст ему это имя, а затем он может спросить example.com. Действительно, только рекурсивный

резолвер будет иметь доступ к этой информации. Вам следует посмотреть QNAME Minimization.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Другая часть этого - агрегирование. Если у вас есть тысячи и тысячи людей, обращающихся к одному и тому же рекурсивному резолверу, да, этот рекурсивный резолвер знает, что вы сделали этот запрос, но теперь, если вы получаете тысячи запросов от одного и того же рекурсивного всего, это не обязательно может быть приписано человеку, просто кому-то, одному из многих, многих людей, которые на самом деле используют этот рекурсивный сервер.

СТИВ КОНТЕ: Спасибо. Следующий вопрос на этой стороне.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Я хочу знать, сохраняют ли DSO журналы и, если да, есть ли какие-нибудь правила, например, в отношении конфиденциальности? Просто интересно, как финансируются DSO для обслуживания домена?

БРЭД ВЕРД: Вы имели в виду RSO? Мы все время слышим «DSO», я просто хотел убедиться, что вы имели в виду RSO, правильно?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Да, простите.

БРЭД ВЕРД: Хорошо, я вернусь назад. Я не слышал первую часть вопроса, но последняя часть очень проста - о том, как они финансируются. Сейчас это нефинансируемый мандат, все это делают волонтеры. По мере естественного роста интернета появились волонтеры для эксплуатации этих корневых серверов, со временем их количество увеличивалось, в основном в период с 82 по 98 год, и с 1998 года новых корневых серверов не было. Кажется, в 2001 году появился Anycast, которым начали использоваться корневые серверы, поэтому мы перешли от 13 идентификаторов, 13 серверов к тому, что мы находимся на тысяче серверов, но с теми же 13 идентификаторами. Используя Anycast, мы можем распространить это повсюду, и это все сделано, это все финансируется самими организациями. Так вы помните другие части вопросов, или вы могли бы повторить их?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Меня интересует, сохраняете ли вы журналы запросов и есть ли какие-либо правила относительно их конфиденциальности?

БРЭД ВЕРД: Единственное, к чему я могу вас отослать, это ежегодная «коллекция Diddle», «День в жизни», ее называют Diddle, это 48-часовое окно, в котором исследователи могут получить

целую кучу данных, чтобы увидеть, что интернет делает в определенный день. Все операторы корневых серверов могут внести свой вклад в это, наряду со многими другими TLD и ccTLD и крупными организациями, крупными операторами DNS, это работа сообщества, и эти данные хранятся в базе данных DNS, и для доступа к базе данных вы должны стать членом и подписать документы о конфиденциальности и еще много чего.

УЭС ХАРДЕЙКЕР: Еще один момент, который заключается в том, что многие операторы анонимизируют данные перед их передачей в OARC и это означает, что они анонимизируют IPS, запрашивающий IP-адрес часто является резолвером, поэтому он не привязывается к одному конкретному компьютеру конечного пользователя, он связан с резолвером, который обслуживает множество вещей. Я думаю, особенно с новыми, особенно после ввода GDPR. Я думаю, что большинство операторов анонимизируют, но вам нужно поговорить с каждым, я не помню текущий статус того, кто анонимизирует и на каком уровне.

ОЗАН САХИН (OZAN SAHIN): У нас еще один вопрос.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Во-первых, я должен извиниться, потому что я думаю, что на этот вопрос будет сложно ответить. Ранее на слайдах я заметил, что большинство организаций, которым

принадлежита IP-адреса корневых серверов - все это американские организации, и мне было интересно, например, американское правительство не собирается придерживаться нейтралитета; что может гарантировать или существует какой-либо механизм, который гарантирует, что корневые серверы для основы Интернета остаются нейтральными?

ФРЕД БЕЙКЕР: Отвечая на это, и, вероятно, существует более одного ответа, но одна из вещей, над которой сейчас работает RSSAC, это вопрос о том, как вы измеряете систему? Одно из измерений, одна из вещей, которые нас беспокоят, заключается в том, действительно ли измеряемый RSO, а мы измеряем их все, но речь идет об одном из них в любой момент времени, фактически обслуживает систему, которая пришла от IANA.

Если корневая зона, которую вы получаете с определенного сервера, отличается, то это нарушение некоторых вещей, которые мы считаем довольно важными. Этого будет считается плохой вещью. Что мы делаем, так это то, что мы буквально загружаем информацию, каждые несколько минут или что-то в этом роде, загружаем информацию из IANA, мы предоставляем ее на некоторое время и загружаем еще больше. Мы всегда передаем то, что нам дала IANA.

Итак, что нам дала IANA? TLD, ccTLD, gTLD поворачиваются и сообщают IANA, у меня были эти имена, и у них были эти записи, связанные с ними, и IANA является нейтральной стороной и управляет этим. Я думаю, что с точки зрения нейтральности вы на самом деле зависите от этики IANA,

ccTLD, которые занимаются этим бизнесом, и RSO. Я ответил на ваш вопрос?

УЭС ХАРДЕЙКЕР: Позвольте мне кое-что добавить, Фред, прежде чем вы продолжите. Я настоятельно рекомендую вам прочитать документ RSSAC023, это документ с 0 по 23, это история того, как система корневых серверов стала такой, какая она есть сегодня. Фактически, мы говорили об этом сегодня утром на нашей встрече RSSAC, на которую вы также можете прийти и послушать.

Это объясняет, как мы добрались до организаций, которые в настоящее время обслуживают это, и так сложилось исторически, это не изменилось за 20 лет; одна из целей RSSAC037, которая представляет собой архитектуру того, как мы вносим изменения в этот процесс в будущем, так как последний человек, который вносил изменения, скончался 20 лет назад, находится на повестке дня.

Что еще более важно, те же разговоры, о которых я говорил ранее в отношении DNSSEC, если вы выполняете проверку DNSSEC, а домен, который вы делаете, проверяется сверху вниз, то вы знаете, что он не был изменен и на самом деле не имеет значения, через какие страны он прошел, он полностью политически независим, потому что технически было бы [неразборчиво] невозможно подделать эти данные. Это самое безопасное, что я могу вам посоветовать сделать, это убедиться, что вы используете валидирующий резолвер DNSSEC.

БРЭД ВЕРД: И я просто немного добавлю, это RSSAC037, который был опубликован и доступен для всех, и там изложены руководящие принципы, определенные операторами корневых серверов. Один из этих руководящих принципов - оставаться нейтральным, это аполитичная точка зрения, здесь нет никакой политики, мы обслуживаем корневую зону, которую мы получили от IANA. Что касается комментариев по поводу базирования в США, то это просто результат естественного роста. Интернет появился в США, он вырос в США, были нужны операторы корневых серверов, и вот как это произошло, не было другой причины, кроме естественного роста.

ФРЕД БЕЙКЕР: И, конечно, у нас есть операторы корневых серверов, которые находятся за пределами США, у нас есть один в Швеции, один в Нидерландах и один в Японии.

СТИВ КОНТЕ: Я возьму следующий в тени, справа от вас.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Я знаю, что атаки типа «отказ в обслуживании» и распределенные атаки типа «отказ в обслуживании», как и многое другое в сфере безопасности, это «кошки-мышки», злоумышленники становятся сильнее, безопасность усиливается, и наоборот, и так без конца. Что именно делается для постоянной защиты корневых серверов?

Встречается ли RSSAC с SSAC и проводит ли встречи по вопросам защиты корневых серверов или как это работает?

БРЭД ВЕРД: Первое, что я могу ответить вам сейчас - недавно операторы корневых серверов опубликовали документ, который отвечает на ваш вопрос напрямую. Это угрозы для системы корневых серверов и то, что они делают и что они сделали, чтобы смягчить некоторые из этих всеобъемлющих угроз.

Что касается RSSAC, RSSAC - это контактная беседа с Правлением, с SSAC в отношении любого типа угрозы для системы, поэтому я считаю... был в начале вопрос о DoH и DoT, мы говорили об этом и о последствиях для инфраструктуры, когда что-то подобное происходит. Эти разговоры происходят постоянно. Хотя они на самом деле не рабочие, рабочие вопросы возникают внутри RSO и между RSO, и в случае DDoS или чего-то еще, информация передается, и принимаются меры для смягчения.

УЭС ХАРДЕЙКЕР: Где он может найти этот документ, Брэд?

БРЭД ВЕРД: Извините. Это не документ RSSAC, он находится на веб-странице корневого сервера по адресу www.root-servers.org; я думаю, это в начале страницы.

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Прекрасно, большое спасибо. Я могу задать последний вопрос? Я знаю, что в случае неверной настройки серверов DNSSEC существует вероятность для запуска атак с усилением, и я знаю, что есть большой нажим для развертывания DNSSEC, мне интересно, есть ли какой-нибудь способ также использовать усиленные настройки на серверах DNSSEC? Например, добавить ограничение скорости и другие методы? Я знаю, что в 2013 году от имени ICANN велась большая дискуссия по усилению безопасности DNS.

УЭС ХАРДЕЙКЕР: Можете ли вы уточнить свой вопрос о том, где неправильно настроенные серверы DNSSEC вызывали проблемы, потому что это либо слишком широко, либо вы ссылаетесь на что-то очень конкретное?

НЕИЗВЕСТНЫЙ ДОКЛАДЧИК: Если кто-то устанавливает неправильно настроенный сервер с поддержкой DNSSEC, а кто-то запускает атаку на основе UDP, и они подделывают IP-адрес, вы можете просто собрать список неправильно настроенных серверов DNSSEC, и это просто позволит атаке усиления быть сильнее, чем нормальное усиление DNS.

УЭС ХАРДЕЙКЕР: Вы беспокоитесь об атаке с использованием отражения запросов. DNSSEC добавляет много данных в подписи, они становятся достаточно большими, ключи достаточно

большие, и вы абсолютно правы, особенно в прошлом, DNSSEC использовался для атак с отражением запросов, потому что вы отправляли очень маленький пакет, будто бы с адреса, который вы хотите атаковать, и очень большое количество трафика идет в этом направлении.

Сегодня большинство серверов, и я говорю не только о корневых серверах, но большинство серверов имеют технологии, использующие то, что называется адаптивным ограничением скорости, и это не позволяет одному серверу задавать слишком много вопросов, а просто отключает их и говорит: «Я больше не разговариваю с тобой. Ты все еще можешь говорить со мной, но тебе нужно вернуться через TCP, который подделать гораздо сложнее».

То, что делают настройки для каждого авторитативного сервера, очень и очень отличается. Я могу сказать, что до того, как большинство людей обратится к этому, вы увидите только ежедневные всплески трафика, потому что все его используют, а затем, спустя годы, графики трафика большинства людей просто выровнялись, потому что люди поняли, что это уже не жизнеспособный путь. В DNSSEC атаки с отражением запросов больше не используются. Я уверен, что где-то они все еще существуют.

СТИВ КОНТЕ: Хорошо, большое спасибо. Есть еще у кого-нибудь вопросы? Я проверил онлайн, вопросов онлайн нет. Последний шанс для вопросов в зале.

УЭС ХАРДЕЙКЕР: Это все отличные технические вопросы, спасибо.

СТИВ КОНТЕ: Я хотел бы поблагодарить Эндрю; я хотел бы поблагодарить Озана за прекрасную презентацию. Я хотел бы поблагодарить наших операторов корневых серверов за ответы на эти вопросы, и я собираюсь сделать бесстыдное объявление; я знаю, что день почти закончился, но в серии «Принципы работы» у нас совершенно новая сессия, которая начинается в пять в зале 512G. Мы пригласили Аарона рассказать о региональных интернет-регистратурах, о том, чем они занимаются, и об основных знаниях по этому вопросу. Прошу вас присоединиться к нам для еще одной сессии, 17:00, 512G для сессии по региональным интернет-регистратурам. На этом спасибо. Благодарю вас, Эндрю, спасибо, Озан, и спасибо, что уделили нам время.

УЭС ХАРДЕЙКЕР: Могу я сделать еще одно объявление?

СТИВ КОНТЕ: Да, пожалуйста.

УЭС ХАРДЕЙКЕР: С конфликтом, к сожалению, Стив, я прошу прощения. Есть еще беседа «DNSSEC для начинающих», которая также состоится в пять часов.

СТИВ КОНТЕ: Хорошо, тогда ты должен выбрать свой яд. Всем спасибо.

[КОНЕЦ СТЕНОГРАММЫ]