МАРРАКЕШ – Вопросы формирования политики в отношении
DNS по HTTPS (DoH), DNS по TLS (DoT) и сопутствующие вопросы
Вторник, 25 июня 2019, 15:15 – 16:45 по WET
ICANN65 | Марракеш, Марокко

АЛЕХАНДРА РЕЙНОСО: Добрый день! Пожалуйста, садитесь. Мы начнем через минуту. Большое спасибо.

Подготовьте, пожалуйста, презентацию. Спасибо. Пока ее готовят, спасибо всем за участие. Мы разберем тему, представляющую особый интерес: DNS по HTTPS и DNS по TLS. Порядок действий такой: сначала я озвучу цели этого заседания и представлю всех членов дискуссионной панели.

Мы ознакомимся с техническим обзором по нашей теме, после которого будет часть вопросов и ответов. Затем мы сможем обсудить опасения, связанные с потенциальным развертыванием, снова пройдем сессию вопросов и ответов, и в итоге проведем дискуссионную панель по вопросам развертывания. Мы надеемся, что все вы примите участие в обсуждении этой темы, представляющей особый интерес. Для этого в нашем распоряжении имеются портативные микрофоны. Дайте о себе знать, там есть отметки в виде цифр. Вот четыре, шесть, три, и пять, кажется, там – сзади. Мне не видно, но она должна быть там. Вот она.

Хорошо, как только у вас возникнет вопрос, поднимите руку как можно выше, чтобы к вам могли подойти и дать микрофон. И будет здорово, если кто-нибудь включит презентацию.

Для начала я представлюсь. Я Алехандра Рейнозо (Alejandra Reynoso) из сообщества национального домена верхнего уровня (ccTLD) .GT. Я заместитель председателя Организации поддержки национальных доменов (ccNSO). Со мной – Дэнни Макферсон (Danny McPherson). Дэнни – исполнительный вице-президент и руководитель службы безопасности в Verisign. Он также входит в состав Консультативного комитета по безопасности и стабильности (SSAC).

Кроме того, рядом со мной – Питер Кох (Peter Koch). В настоящий момент Питер работает в DENIC (Регистратура национального домена Германии) советником по вопросам политики. Также здесь присутствует Барри Лейба (Barry Leiba). Барри Лейба – руководитель отдела стандартов в Futurewei Technologies. С начала 1980-х годов Барри работал над электронной почтой и сопутствующими технологиями, и в настоящее время он сосредоточен на интернете вещей, обмене сообщениями и взаимодействии на мобильных платформах, вопросах безопасности и конфиденциальности интернет-

приложений, а также разработке и внедрении стандартов интернета. Барри также входит в состав SSAC.

Там у нас Алисса Мур (Alyssa Moore). Простите, я не показываю на людей пальцем. Алисса работает старшим советником по политическим и правозащитным вопросам в CIRA – это ведомство Канады по регистрации в интернете и регистратура национального домена .CA.

Барри и Алисса будут модерировать наши вопросы и ответы. Среди остальных участников дискуссионной панели: Тим Эйприл (Tim April) – главный архитектор системы информационной безопасности в компании Akamai Technologies, которая занимается вопросами безопасности сетевой конфигурации DNS и реагирования на инциденты. Тим также входит в состав SSAC.

Пролистайте, пожалуйста, пару слайдов вперед. Также с нами Витторио Бертола (Vittorio Bertola). Витторио Бертола – глава отдела по формированию политики и разработке инноваций в Open-Xchange (головная компания PowerDNS). На протяжении последнего года он обсуждал вопросы политических последствий шифрования DNS на нескольких площадках.

И наконец, Мишель Нейлон (Michele Neylon). Мишель – основатель и генеральный директор компании Blacknight Solutions (регистратор, аккредитованный ICANN). Мишель также входит в состав Совета

Организации поддержки доменов общего пользования (GNSO).

Пролистайте, пожалуйста, несколько слайдов вперед. Кажется, у нас опять какие-то технические сложности, но незначительные. Не знаю, можно ли начать с технического обзора, с других слайдов? Можно? Чтобы сэкономить время.

Подождем еще минутку, может, удастся выгрузить слайды. Если нет – то нет, но дадим презентации пару секунд. А вы пока можете скачать слайды в расписании, чтобы следить за обсуждением. Думаю, пора начинать. Прошу вас, Дэнни, если вы не против.

ДЭННИ МАКФЕРСОН: Разумеется. Я начну без слайдов, для многих эта тема была достаточно сложной даже с поддержкой слайдов, так что будет интересно.

Меня зовут Дэнни Макферсон, я член SSAC и поэтому показываю слайды SSAC. Так что ошибки не мои, а SSAC. Будем придерживаться этой позиции.

Сегодня мы озвучим одну тему: я расскажу о технической стороне, а затем Питер и участники дискуссионной панели обсудят некоторые возможные последствия. Но основной темой, которая вызывает в последнее время большой интерес, является вопрос: что мы

подразумеваем под DOH и DOT (то есть под «DNS по HTTPS» и «DNS по TLS»)?

В двух словах, эти технологии призваны обеспечить конфиденциальность транзакций DNS. В стандартной DNS не было ни малейшего намека на конфиденциальность, как и на целостность: к ней «прикрутили» DNSSEC для обеспечения защиты целостности DNS. Однако сама DNS по целому ряду причин была уязвима перед слежкой, прослушиванием и потенциальной модификацией ответов различным клиентам. Это могло требоваться для родительского контроля, государственной цензуры или блокировки доступа к вредоносному сайту, чтобы защитить пользователя.

В любом случае, существует ряд причин, почему мы хотим этого, и на слайде шесть этой презентации вы увидите несколько таких причин. Главное здесь – стандартная DNS, а с учетом самой [идеи] конфиденциальности, а также геополитических обстоятельств и различных экономических последствий, обеспечение конфиденциальности транзакциям DNS имеет различные преимущества и некоторые ответвления.

Поэтому мы обсудим модели развертывания, но необязательно очень подробно. В любом случае, если вы

следите по презентации, на шестом слайде отражено то, о чем я сейчас рассказал.

Без конфиденциальности транзакций DNS вы уязвимы перед атаками, направленными на утечку и раскрытие информации, и кто-то сможет следить за вами или выяснить, что вы делаете в интернете, и изучить эту информацию.

Поэтому и DOH, и DOT призваны обеспечить шифрование «на лету», и при атаке на пути или наличии наблюдателя никто не увидит эту информацию. Если объяснять простыми словами, вот что собой представляют DOH и DOT.

На седьмом слайде презентации приводится обзор стандартной DNS, и по сути она представляет собой следующее: у вас есть устройство, на котором установлено приложение, и это приложение хочет разрешить что-то в DNS и запрашивает локальный процесс на устройстве, например, веб-браузер может спросить у операционной системы вашего iPhone или ноутбука: «Эй, как попасть на www.example.com?»

В ваше устройство встроен резолвер DNS, который ответит либо по локальной сети, либо по внешней сети интернет-провайдера (ISP). Перелистните еще два слайда, чтобы увидеть изображение стандартной DNS, слайд восемь, если можно.

Вот о чем я только что говорил. У вас есть приложения, задача которых – разрешить что-то для пользователя или процесса на устройстве, поэтому это приложение по сложившейся традиции обращается к локальной операционной системе – повторюсь, это приложение может быть установлено на iPhone или может представлять собой веб-браузер на ноутбуке.

Это приложение или веб-браузер запросит у локальной операционной системы местоположение имени адресата в интернете, а затем устройство выйдет в интернет и свяжется с тем, что известно ему как локальный сервер пересылки или, возможно, с рекурсивным резолвером.

Изначально эти рекурсивные резолверы находились в сети ISP или в локальной сети, предоставленной провайдером доступа к сети, однако теперь они все чаще могут располагаться в облачной инфраструктуре, например, OpenDNS или рекурсивном сервере имен Google, который предоставляет их в интернете, где-то в облачной инфраструктуре. Это один из меняющихся архитектурных [параметров.] Он может не быть локальным в сети, где традиционно давались разрешения.

Такой рекурсивный сервер имен может выходить за пределы доверенной инфраструктуры, будь то корневая инфраструктура, инфраструктура домена верхнего

уровня, доверенная инфраструктура, и разрешать имя, а затем передавать эту информацию обратно приложению или stub-резолверу, который передаст ее приложению, а затем это приложение сможет подключиться к необходимому адресу в интернете.

Как видно на этой диаграмме, все современные транзакции, конфиденциальность таких транзакций не обеспечивается, поэтому если в любом месте, отмеченном зеленой стрелкой на этой диаграмме, будет находиться наблюдатель, у него будет возможность увидеть, что именно пытается разрешить пользователь, а это может быть: информация, относящаяся к коммерческим секретам, конфиденциальный контент, практически что угодно. А DOH и DOT предполагают некоторые способы защиты такой информации. Давайте перейдем к следующему слайду.

Итак, одно из двух решений известно как DOT. DOT означает «DNS по TLS». TLS расшифровывается как «защита транспортного уровня», и, что примечательно, – это самые безопасные транзакции в интернете: если вы когда-либо видели стандартный замочек или заходили на финансовый или любой другой сайт, содержащий конфиденциальную информацию, то скорее всего его поддержку осуществлял протокол TLS, который обеспечивает шифрование в сети и на уровне передачи, он обеспечивает шифрование или конфиденциальность

такой информации, чтобы в результате атаки на путь злоумышленник не мог воспользоваться или, как минимум, наблюдать за информацией.

И в модели DOT – перейдем к следующему слайду – я хочу привести пример с слайда. В целом, в модели DOT традиционно осуществляется – повторюсь, можно развернуть и DOH, и DOT – целый спектр различных технологий. Они все еще на стадии разработки на уровне стандартов интернета и в оперативном сообществе. Но DNS по TLS традиционно предусматривает, что локальная система (например, ваш iPhone или ноутбук) может быть оснащена системной настройкой, которая сообщает о своем намерении использовать этот резолвер и эту инфраструктуру для разрешений DNS, и каждое приложение на таком устройстве будет использовать эту настройку, выходить за пределы инфраструктуры и делать это.

Здесь, например, вы видите, что веб-браузер делает то же, что и обычно. Он спросит у локального stub-резолвера: «Эй, мне нужно попасть на example.com в интернете. Решишь эту задачу?»

Однако теперь stub-резолвер вместо того, чтобы отправлять простой текст, фактически отправит его по зашифрованному каналу, чтобы выделить себе либо определенное место в облачной инфраструктуре, либо в

сети ISP для разрешения этой информации. По сути, именно это и отражают здесь красные стрелки.

Итак, информация будет зашифрована, и ни наблюдатель на пути, ни другой злоумышленник не сможет ей воспользоваться или, как минимум, наблюдать за происходящим. А затем и в самой доверенной инфраструктуре, сейчас не так много обсуждается вопрос о том, сможет ли решение DOH или DOT вписаться в корень, TLD или, возможно, в доверенную инфраструктуру домена второго уровня. Но часть этой информации еще дополняется.

Сейчас мы противопоставим это протоколу DOH, который отодвигает уровень шифрования немного назад. Перейдем к другому слайду и поговорим о DOH.

Я двигаюсь слишком быстро. Извините. Хорошо, знаете ли вы, что DOH использует вместо TLS для передачи DNS? На моем устройстве установлено много веб-приложений и через него проходит большой объем интернет-трафика, и в этой операционной системе или на этом устройстве много программного обеспечения, построенного на транзакциях HTTP, поэтому вместо того, чтобы использовать TLS по умолчанию в инфраструктуре, я буду зашифровывать ответы DNS в веб-запросах, HTTP запросах, и что примечательно, буду переправлять их по

TLS, по которой их пропускает HTTPS, а затем передавать их по сети.

Это снабжает приложение большим количеством фильтров, чтобы либо действовать с инфраструктурой разрешения напрямую и полностью обойти локальный stub-резолвер, либо использовать stub-резолвер, запущенный в операционной системе. Перейдем к следующему слайду и проиллюстрируем это для всех.

То, что вы видите, повторюсь, это всего лишь одна модель развертывания. Она может отличаться. Но может произойти следующее: мой браузер может использовать один рекурсивный сервер имен с DOH в инфраструктуре, а другое приложение может использовать локальный сервер или мой системный резолвер.

Итак, интересно становится, если кто-то вмешается в этот сценарий и разные приложения, используя другую DNS, поскольку сложно будет понять, что происходит.

Кроме того, традиционно ISP может использовать запросы DNS в качестве контрольной точки в инфраструктуре или предприятие может использовать запросы DNS в качестве контрольной точки, и они могут возражать против того, чтобы зашифрованные транзакции поступали непосредственно из приложения и проходили по определенному периметру или границе в инфраструктуре, поскольку они могут упустить из поля

зрения безопасность, родительский контроль и прочие элементы их инфраструктуры.

Здесь самое главное, что вместо использования stub-резолвера в случае с DoH, когда традиционно предусматривалось, что приложение будет отправлять запрос напрямую в инфраструктуру интернета, инфраструктура разрешения получит ответ DNS и обойдет все: и в операционной системе, и, возможно, в организации поставщика услуг локальной сети. Вот что мы здесь объясняем.

Хорошо, перейдем к следующему слайду. Что еще интересно отметить: если рассмотреть это с точки зрения контрольной точки, прослушивания или слежки, то DOH эффективно смешивает ваш трафик запросов DNS с остальным трафиком HTTP в сети. Поэтому потенциально намного сложнее вести слежку или прослушивать и даже фильтровать, поскольку придется взломать весь HTTP-трафик, чтобы вмешаться как-то технически с точки зрения контрольной точки в запросы DNS, относящиеся к DOH.

Повторюсь, DOT – это системная настройка, но, вероятно, вам придется ее настроить, и последнее, на что я укажу на этом слайде: модели развертывания, которые вы видите здесь для DOH и DOT, можно смешать между собой, а эти стрелки – поменять. Все зависит от того,

что именно хочет активировать приложение, что именно хочет активировать системный администратор и так далее.

Такая система, как stub-операционная система на устройстве может использовать DOH, а не DOT или может использовать традиционную DNS. Этот вопрос еще обсуждается.

Не так много внимания уделяется сейчас доверенной инфраструктуре, поэтому [неразборчиво] .net, .gov, .edu, .jobs, независимо от TLD и потенциально даже доменного имени второго уровня, и существуют некоторые другие технологии, например, анонимизация QNAME, которая обеспечивает определенную защиту конфиденциальности, хотя также существуют некоторые ответвления с различными аспектами.

Итак, я попытался ознакомить вас с этим вопросом, немного торопясь, поскольку Мишель напоминал мне о времени, но на этом мы ненадолго прервемся, вдруг у кого-то возникли вопросы, прежде чем перейти к части презентации, связанной с развертыванием – ее объяснит Питер. Поэтому если у вас есть какие-либо вопросы, связанные с тем, что мы сейчас рассказали участникам дискуссионной панели, можете задать их сейчас или подождать и дать Питеру возможность рассказать о

других последствиях внедрения DOH и DOT, а затем уже задать вопросы.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Дэнни, за это прекрасное и быстрое объяснение. У нас есть один вопрос. Большое спасибо.

НАЙДЖЕЛ КАССИМИР (NIGEL CASSIMIRE): Да. Добрый день. Меня зовут Найджел Кассимир, я из Телекоммуникационного союза стран Карибского бассейна. Для меня все это в новинку, и я пытаюсь понять проблему, которую вы пытаетесь решить с помощью всего этого. Это попытка сделать DNS более надежной? И как эта технология сопоставима с DNSSEC, к примеру?

МИШЕЛЬ НЕЙЛОН: Так, теперь мы спорим, кто ответит. Поэтому я просто возьму микрофон. В кругах ICANN о DNSSEC часто говорят как о чудодейственном средстве, которое решит все проблемы, связанные с DNS. Это не так. DNSSEC защищает вас, например, когда вы идете в банк, буквально идете в свой банк, от того, чтобы вам никто не встретился по пути и вы ни на что не наткнулись.

Такая атака называется «DNS-отравление», что ранее являлось проблемой. DNSSEC решает ее. А DOT и DOH

пытаются одновременно добавить уровень конфиденциальности и уровень надежности, но оба вызывают сложности. Что касается конфиденциальности, вы понимаете, и думаю, что кто-то из нас подробнее расскажет о том, какие негативные последствия это может иметь для некоторых аспектов безопасности. Но фактически эта технология позволяет переносить запросы DNS таким образом, чтобы отправку запросов осуществляли устройства (ноутбук, телефон, iPad или что-то еще), таким образом они отходят от традиционной DNS для перехода к совмещению на других протоколах.

А в случае с DOH? Он выглядит как обычный запрос к приложению интернета. Имейте в виду, что я не так хорошо подкован, как он, так что он, вероятно, меня поправит, но это простой способ разобраться.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Мишель. У нас есть удаленный участник. Пожалуйста.

АРИЭЛЬ ЛИАНГ: Есть вопросы от двух удаленных участников. Первый – от Мухаммеда Юсифа (Mohammed Yousif). DNS по TLS каким-либо образом снижает производительность в том, что касается времени решения запроса? Затем мы зачитаем второй вопрос.

МИШЕЛЬ НЕЙЛОН: Все зависит от способа внедрения stub-резолвера. Он может вызвать дополнительное снижение производительности или круговое обращение резолвера в момент настройки первоначального подключения, но если stub-резолвер настроен на то, чтобы сохранять соединение с течением времени, то, возможно, – [амортизированная] стоимость останется примерно такой же, как и в случае с обычной DNS.

АРИЭЛЬ ЛИАНГ: Есть второй вопрос от удаленного участника. Его задает Язид Акано (Yazid Akanho) из Бенина. Слайд шесть: такие технологии как QNAME Minimization тоже могут быть эффективны в защите конфиденциальности данных пользователей. Как все резолверы могут это реализовать?

ДЭННИ МАКФЕРСОН: Мы не хотели много времени уделять QNAME Minimization, но это достаточно простая технология. Изначально DNS была очень подробной, и если я хотел отправить какие-то запросы в DNS, мне приходилось вводить полностью определенные имена доменов, например, internalsecretserver.foo.verisign.com, и я бы задавал каждому авторитативному серверу полный вопрос, хотя на самом деле мне нужен только корень,

который сообщит, как попасть на следующий уровень иерархии, то есть на .com.

И когда я задаю вопросу корню, мне не приходится говорить ему все, что мне нужно, мне просто необходимо спросить его, как добраться до .com, а затем .com расскажет мне, как попасть на verisign.com, а verisign.com расскажет, как попасть на внутренний секретный сервер.

Фактически, вы не раскрываете полное имя того, что вы намерены разрешить, то есть происходит минимизация. Это сохраняющая конфиденциальность функция разрешения имени, она очень простая, и она уже различными способами развернута и реализована в большинстве реализованных рекурсивных серверов имен и с точки зрения конфиденциальности данных, она обеспечивает определенную измеримую минимизацию поверхности атак.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо. Я попрошу всех как можно ближе придерживаться темы. Нам известно о существовании очень схожих концепций, связанных с безопасностью и интернетом, но прямо сейчас мы должны сосредоточиться на DOT и DOH, чтобы дискуссионная панель могла продвинуться дальше. У нас еще два вопроса. Номер четыре и номер пять, а затем мы перейдем к следующему докладчику. Спасибо.

ФРЕД БЕЙКЕР (FRED BAKER): Меня немного удивил ваш ответ касательно различий между TLS и применением DNSSEC, поскольку они защищают разное. DNSSEC защищает контент, фактическую ресурсную запись, а TLS защищает канал.

Для сравнения можете представить себе трубопровод и воду. Допустим, у нас есть прекрасный бронированный трубопровод и это самый лучший в мире трубопровод, он берет начало в озере, которое я наполнил ядом. И хотя это самый прекрасный трубопровод, он все равно подает яд.

Поэтому защита контента снимает проблему самого яда. Нет, я не буду высказываться против TLS. Наличие хорошего канала – это тоже неплохо. Но DNSSEC приобретает большое значение в плане обеспечения того, что имя действительно содержит адрес, до которого вы пытаетесь добраться.

ДЭННИ МАКФЕРСОН: Я просто отвечу. Думаю, это очень точно подмечено, Фред. На мой взгляд, даже если в полной мере развернуть DOH или DOT в экосистеме, все равно потребуется DNSSEC и анонимизация QNAME для обеспечения дополнительной защиты. Они решают совершенно разные задачи, так что это ценное замечание.

АЛЕХАНДРА РЕЙНОСО: Спасибо. Номер пять?

ДЖИМ ПРЕНДЕРГАСТ (JIM PRENDERGAST): Да. Здравствуйте. Признаюсь: я не из Инженерной проектной группы интернета (IETF). Знаю, что многие в этой комнате входят в ее состав. Дэнни, пока вы перечисляли преимущества, вы также упомянули о том, что может выйти из строя. Как эти протоколы могли получить утверждение в качестве стандартов, если они могут повлечь за собой такие непредвиденные последствия?

НЕИЗВЕСТНЫЙ МУЖЧИНА: [Стоит спросить IETF.]

НЕИЗВЕСТНЫЙ МУЖЧИНА: Это вопрос по существу, Джим.

ДЭННИ МАКФЕРСОН: Хорошо. Прошу прощения. Я думаю, что технология уже готова, а экосистема выявит подходящие модели развертывания. Не думаю, что кто-либо в этой экосистеме: от поставщиков браузеров до поставщиков операционных систем и от операторов рекурсивных серверов имен до операторов доверенных инфраструктур, хочет что-нибудь сломать.

Примечательно, что это вызывает определенные сложности, связанные с развертыванием, поскольку теперь если вы ISP и не видите DNS-трафик пользовательского браузера, а для разрешения имен с помощью DNS используется облачный сервис, то в случае если потребуется устранить проблему с помощью DNS, то вы, возможно, не сможете этого сделать. Или если с помощью DNS вы реализуете функцию родительского контроля, то, возможно, вы не сможете этого делать.

Итак, я думаю, что экосистеме придется приспособиться к этому, и именно поэтому я считаю важным понимать, что модели развертывания DOH и DOT будут различаться и адаптироваться в зависимости от того, что будет диктовать рынок и динамика: что оптимально, что работает и что не работает.

АЛЕХАНДРА РЕЙНОСО: Да. Большое спасибо. Итак, об опасениях, связанных с потенциальным развертыванием DOH и DOT, нам расскажет Питер.

ПИТЕР КОХ: Да. Спасибо, Алехандра. Меня зовут Питер Кох. Как меня уже представили, я работаю в DENIC старшим

советником по вопросам политики и являюсь одним из назначенных ccNSO членом этой рабочей группы.

Меня пригласили обсудить опасения, связанные с потенциальным развертыванием. И на самом деле, Джим, неофициальным подзаголовком было «протокол безвреден, но всякое бывает». Вероятно, это рассеет некоторые опасения.

Первая часть будет носить технический характер: итак, у нас есть два стандарта, которые более или менее решают одну – ах, да, нам нужно, простите –

АЛЕХАНДРА РЕЙНОСО: [неразборчиво] слайд, пожалуйста. Большое спасибо.

ПИТЕР КОХ: Да, вот этот. Хорошо, я начну отсюда. Итак, у нас есть два стандарта, которые слегка отличаются друг от друга технически, но оба решают проблему конфиденциальности циркулирующего DNS-трафика.

Просто напомню с чего все началось: пару лет назад был один парень по фамилии Сноуден и вот что он обнаружил, или, как минимум, чем поделился: DNS-трафик может быть источником разведывательной информации, его можно использовать для идентификации людей или

действий, которые эти люди совершали, например, посещали сайты.

Но не будем ограничивать свое внимание только сайтами. DNS используется и для любых других сервисов. И это один из факторов, подтолкнувших IETF – и я не говорю за них, члены группы опубликовали документы по этому вопросу, в которых объявили повсеместное наблюдение угрозой, риски которой будут снижены с помощью пары протоколов. И эти подходы действительно решают эту самую проблему, отвечая на повсеместное наблюдение повсеместным шифрованием.

Что касается шифрования DNS-трафика «на лету». Есть и другие технические аспекты, которые мы обсудим позже, но пока я просто добавлю: не только государственные субъекты это делают, есть и другие фрагменты головоломки, которые могут быть заинтересованы в изучении циркулирующего DNS-трафика, поскольку хотя информация в DNS, по большей части, носит общедоступный характер, тот факт, что кто-то запрашивает конкретное имя в конкретный момент времени, скорее всего, уже не позволяет относить эту информацию к общедоступной и делает ее ценной.

Таким образом, у нас есть два этих конкурирующих стандарта, которые достаточно просто описать. В них просто описывается способ обмена данными одной части

(резолвера) с другой, которой в данном случае является так называемый резолвер DOH. Снаружи он выглядит как веб-сервер, однако он передает не сайты, а ответы DNS.

До сих пор не решена следующая проблема: как пользователь, как веб-браузер в таком случае получит информацию о том, кто делает запрос? Как правило, эту информацию передает операционная система при ее наличии, что верно для большинства ноутбуков и смартфонов, которые вы используете. В них встроена операционная система, а разрешение имен лежит глубоко в этой операционной системе, и, как правило, на сегодняшний день оно выполняется одинаково для всего аппарата, который вы держите в руке или перед собой на столе.

И это, возможно, придется изменить. Поэтому IETF или разработчики продолжают работать над автоматической конфигурацией (как найти этот резолвер DOH), а также в процессе выполнения находятся инициативы, которые предоставят пользователю больше выбора и дадут ему возможность вручную настраивать службу DNS, однако пока что это все находится на стадии разработки.

Итак, имеется веб-браузер, и поставщик активировал для своего веб-браузера DOH (то есть DNS по HTTP), который обращается с разрешением имен DNS схоже с этим веб-браузером и который содержит жестко закодированный

URL – это идентификатор, сетевой адрес, который, будем надеяться, вы узнали из своего веб-браузера при посещении интернет-страниц – и который жестко закодирует эту информацию для DOH. На тот момент времени все веб-браузеры этого поставщика будут использовать конкретный резолвер DOH. Повторюсь, здесь не будет одиночных серверов, будет Anycast и все.

И он будет перезаписывать информацию, поступающую от операционной системы. И тогда приложение сможет выбирать другой путь резолвера DNS, отличный от выбора остальной операционной системы. Это может вызвать определенные сложности и, как сказано в презентации, может вступить в конфликт с политиками безопасности некоторых администраторов сети, которые пытаются минимизировать доступ к определенной информации, в основном, к сайтам или фишинговым сайтам (список можно продолжить) путем перехвата DNS-трафика, поскольку в этом случае, как кто-то уже предположил, этот метод не будет работать. Следующий слайд, пожалуйста.

И разумеется, интересный вопрос: почему стандартов два? Я пытаюсь не вдаваться в технические подробности, но DOT (DNS по TLS (по протоколу защиты транспортного уровня)) относится скорее к инженерии, то есть мы воспринимаем сеть уровнями и так далее, но с этим возникла, по меньшей мере, одна проблема: необходимо

обладать определенной информацией и, чтобы её получить, нужно пробить еще одно отверстие в брандмауэре, при этом каждый дает любому другому человеку доступ на любой сервер.

Таким образом, DOH-трафик выглядит примерно как доступ на сайт и его невозможно выделить, как сказано на следующем слайде. Или вообще-то на этом слайде. Извините.

Поэтому никто не может заблокировать доступ к такой службе разрешения имен на базе DOH, так чтобы одновременно не заблокировать доступ к важным сайтам. В этом-то и фокус, если можно так выразиться.

И все еще ведется исследование, которое позволит добавить эту функцию к DNS по TLS в виде варианта исполнения DOT. Разумеется, с технической стороны проявляются некоторые неприятные подробности, но к сегодняшней теме они не относятся.

В результате администраторы сети, возможно, утратят возможность блокировать разрешение имен, поскольку тогда они могут заблокировать заодно доступ к сайтам или популярным поисковым системам. Это может – возможно, а возможно и нет – вступить в конфликт с нормативно-правовыми требованиями некоторых юрисдикций, в которых ISP обязаны блокировать разрешение определенных доменных имен, и читая это,

я не утверждаю эффективность этих механизмов блокировки, однако они могут попадать под нормативно-правовые требования. Как я сказал, добиться идеала невозможно, поскольку это с легкостью можно обойти, настроив собственный резолвер при помощи VPN или запустив собственный резолвер на своей системе.

[Преобразование] запросов DNS в потоке интернет-трафика может помочь пользователям обойти фильтрацию на базе DNS, и вы можете называть это цензурой: фильтрация устанавливается для пользователя третьей стороной, или возможна блокировка вредоносного ПО, на что пользователь, как правило, подписывается и что якобы делается в интересах пользователя. Следующий слайд, пожалуйста.

Рассмотрим это комплексно, поскольку повторюсь, протокол [безвреден,] но всякое бывает. DNS по HTTP не предусматривает конкретной модели развертывания. Любое предприятие может запустить резолвер DOH и направить на него свои веб-браузеры, а затем работать как прежде. Однако на данный момент в наших обсуждениях фигурирует определенная модель развертывания, которая склоняется в сторону концентрации и консолидации: поставщики веб-браузеров сотрудничают с поставщиками разрешений DNS – и я объясню это в следующем пункте – и направляют всех своих покупателей этих веб-браузеров,

своих интернет-пользователей в службу разрешений конкретного поставщика, что позволяет этому поставщику получить глубокое представление, а пользователям дает определенную стабильность, но обеспечивает концентрацию.

В течение последних 30 с лишним лет разрешение имен DNS было крайне децентрализованным. То есть оно могло происходить в ISP или на вашем ноутбуке или, если говорить о событиях 30-летней давности, на центральной ЭВМ и где угодно. Однако со временем появилось разрешение имен DNS как служба, и это так называемые «четверки», например, 1.1.1.1, 8.8.8.8, вы могли их видеть на картинках, нарисованных на стенах в некоторых странах, где люди сталкиваются с блокировкой DNS и обходят ее путем перехода на один из этих поставщиков разрешений. Есть и другие, которые используют одну и ту же цифру в каждой позиции. Это лишь вопрос любопытства и простоты использования.

Но эти аспекты вдобавок к выбору пути разрешения для отдельного приложения, а не отдельной системы, отдельного предприятия или даже отдельного ISP, где ISP предоставляет своим клиентам возможность выбора разрешений, совершенно точно ведут к росту концентрации резолверов, которые становятся все больше. И под «больше» мы имеем в виду постоянно растущую численность пользователей этих резолверов,

что означает, что можно ожидать того, что вес– и это также может означать политический вес – этого конкретного оператора резолвера будет увеличиваться, а он сам становится все более важным. Следующий слайд, пожалуйста.

Хорошо. Как мы сказали, DOH и DOT – оба обеспечивают конфиденциальность «на [лету»], и мы обсудили причины этого. Однако резолверы – будь то резолвер на вашем ISP или резолверы, предоставленные этими крупными службами разрешений – видят запросы пользователей на совершенно другом уровне детализации.

По какой-то причине иногда к вопросу добавляется конкретная информация, чтобы пользователи могли получать индивидуализированные ответы, поскольку в последнем пункте – я перейду к нему через секунду – некоторые технические сценарии зависят от того, что не все получают одинаковые ответы, задавая одинаковый вопрос, так называемые сети передачи данных часто используют DNS для направления пользователей в ближайшую систему доставки контента, чтобы сократить время ожидания и быстрее ответить пользователям.

Поэтому вопрос конфиденциальности решается не только путем шифрования «на лету», но во многом политикой резолвера DNS, например, чтобы разрешающий оператор обещал вам быть подотчетным

или вроде того, что происходит с данными о запросах, которые [он видит.] Можно было обойти ISP или государственный субъект как кого-то заинтересованного в ваших данных, но, вероятно, это не сильно помогает, если в дело вступает оператор резолвера. Следующий слайд.

Это не сработало. Итак, что касается вопроса политики, относящейся к резолверам DOH, интересно обсудить следующее: как их отбирать? И эта информация была на предыдущем слайде: каковы технические средства, как мне в качестве пользователя решить использовать какой-либо резолвер и если я его выбрал, то как настроить его для моего приложения, системы или чего-то еще? И каким образом операторы этих резолверов DOH отчитываются за выполнение своих обещаний и свои действия? Поскольку, повторюсь, их могут потребовать раскрыть информацию по запросу какой-либо организации, будем надеяться, что в большинстве случаев – правоохранительных органов.

И кто определяет, какие политики применимы – и в ходе обсуждения этого вопроса один из поставщиков сказал: «Хорошо, мы понимаем, что у сообщества есть определенные опасения в отношении нашего сотрудничества только с одним поставщиком. Мы можем рассмотреть возможность сотрудничества с другими поставщиками, но мы хотим, чтобы они придерживались определенных политик в отношении резолверов, и это

означает: чтобы они совершали одни действия и не совершали других действий с пользовательскими данными.» Следующий слайд, пожалуйста.

Теперь еще более комплексно, поскольку один из вопросов, конечно, будет звучать так: почему мы говорим об этом в контексте ICANN? Теперь представьте группу сотрудничающих поставщиков резолверов DOH. Эта группа будет небольшой, не такой обширной как раньше. И представьте конкретное приложение, сервис, который используется в основном в интернете, например, обозреватель, мы все так делаем.

И иногда возникает заинтересованность в дополнительном пути разрешения имен. В IETF, а также в ICANN, обсуждался вопрос TLD точка-onion, который не совсем TLD, но сейчас он зарезервирован. Но это другой путь разрешения, необходимый для того, что каким-то образом вписывается в пространство имен.

С практической точки зрения при наличии этой группы сотрудничающих поставщиков разрешений – с большой численностью – кто именно будет решать, открывать ли новые сегменты пространства имен? Как это будет выглядеть и что будет означать для роли ICANN в отношении корневой зоны DNS, когда произойдет смена власти, изменится то, что люди просто будут бойкотировать или привлекать к этому свои веб-

браузеры. Следующий слайд, пожалуйста, и он, кажется, последний.

Итак, выводы. Вероятно, предварительные выводы. Мы узнали, что некоторые модели развертывания DOH и DOT могут повлиять на традиционные контрольные точки в разрешении. ISP, предприятие может перехватывать запросы DNS и отправлять другие ответы. Для передачи рекламы, но также для ограничения вредоносного ПО и сетей зараженных машин (ботнетов).

Стандартизация DOH и DOT, резолверов в приложении и принципы их отбора все еще находятся в разработке. Окончательного вывода нет. В настоящий момент складывается впечатление, что влияние на операторов регистратур и регистраторов будет минимальным. Однако, повторюсь, кто-то может постучать в дверь регистратуры или регистратора и заявить: «Я один из этих поставщиков разрешений. Почему бы вам не дать мне копию своих данных DNS? Я буду рад передать их вашим пользователям еще быстрее.»

И, конечно, еще слишком рано судить о том, как это отразится на пользователях. Как мы уже слышали, это никак не влияет на DNSSEC и другие механизмы защиты конфиденциальности, например, QNAME Minimization. Потребность в них никуда не делась. Пожалуй, это все. Следующий слайд, пожалуйста. Хорошо.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Питер.

ПИТЕР КОХ: Спасибо.

АЛЕХАНДРА РЕЙНОСО: У аудитории есть вопросы? У нас есть время на пару вопросов. У меня номер пять.

УОРРЕН КУМАРИ (WARREN KUMARI): Здравствуйте. Уоррен Кумари, я работаю на Google. Я не из команды Chrome, но я передаю информацию некоторых членов этой команды. Питер, в своей презентации вы представили вариант модели развертывания одним из браузеров. Но это не единственная модель развертывания. Chrome планирует обеспечивать пользователей DOH двумя способами.

Если резолвер пользовательской системы уже поддерживает DOH, браузер Chrome просто обновится для поддержки. Если вы уже используете резолверы своего ISP и они поддерживают DOH, он просто будет осуществлять DOH по ним.

По желанию пользователи могут выбрать другой резолвер. Это практически ничем не отличается от того, что происходит сейчас. Если пользователи недовольны резолвером своего ISP, они могут выбрать другой.

В любом случае Chrome не будет изменять выбор пользователей самостоятельно. И кроме того, мы не требуем от пользователей выбирать нечто вроде Google Public DNS.

Все это означает, что существующие защиты, которые направлены на вредоносное ПО, если используется корпоративная DNS, все эти элементы продолжат работать как прежде.

Поэтому, на мой взгляд, важно понять то, каким образом происходит развертывание, а не что собой представляет протокол передачи данных. Не знаю, есть ли у вас какие-то мысли по этому поводу.

ПИТЕР КОХ: Да. Спасибо, Уоррен. Мы намеренно не включили никаких названий в презентацию, и, я надеюсь, я не назвал ни одно из них. Поэтому спасибо, что сделали это в этом конкретном случае. И да, это ценное дополнение к сценарию модели развертывания. Мы не пытались предоставить исчерпывающую информацию, кажется, в слайде говорилось, что обсуждается несколько моделей, и, безусловно, описанная вами является одной из них.

Что касается другой части, я бы хотел отложить ее до дискуссионной панели и не забегать вперед этого

обсуждения и, возможно, мы сможем сосредоточиться на срочных вопросах о том, что я непонятно объяснил.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Питер. У нас один удаленный участник, и затем мы перейдем к номеру три и номеру четыре, и в этой части очередь закончится.

АРИЭЛЬ ЛИАНГ: Есть вопрос от Дирка Джамперца (Dirk Jumpertz). DOH уже используют во зло в качестве вектора атаки, чтобы вставлять вредоносный контент на интернет-страницы с помощью собственноручно сделанных записей [TXT]. Вам об этом известно? Это невероятно сложно блокировать, поскольку для атаки [на THHP] используется надежный канал в сочетании с DNS.

Разве это не делает DOH угрозой, а не спасением?

ПИТЕР КОХ: Любопытная информация, Дирк. Лично я не слышал об этом. Возможно, остальные участники дискуссионной панели в курсе. Я бы хотел отложить этот вопрос до дискуссионной панели, и, возможно, нам удастся иметь это в виду.

АЛЕХАНДРА РЕЙНОСО: Так и сделаем. Номер три?

ЭДУАРДО ДИАС: У меня вопрос. Потенциальная проблема пользователя состоит в следующем: если я скачиваю приложение, а это приложение посредством [загрузки] использует собственные резолверы, о чем я не имею представления, это очень – это может оказать существенное влияние на пользователя, а он будет не в курсе происходящего. Спасибо.

ПИТЕР КОХ: Да. Спасибо за это замечание. Один момент не был озвучен в этой теории – а как мы знаем, теория мгновенно становится практикой – другое приложение может продемонстрировать другие результаты, следовательно система доменных имен будет отличаться от веб-браузера и, скажем, для приложения электронной почты или телефона, поддерживающего VOIP, поскольку в зависимости от выбранного вами пути разрешения некоторые домены могут оказаться заблокированными, а другие пути открыты, или даже вас могут направить в точку А там и в точку В где угодно. Это действительно будет пользовательским опытом. Но это самое начало того, что может ожидать конечного пользователя. Спасибо.

АЛЕХАНДРА РЕЙНОСО: Спасибо. Номер 4.

[РЕММИ НУЭКЕ (REMMY NWEKE):] Спасибо. Меня зовут [Нуэке Ремми]. Я из Нигерии, представляю Группу интересов некоммерческих пользователей (NCUC). У меня вызывает опасения один из пунктов, указанных на слайде, еще слишком рано судить о том, какое влияние могут оказать DOH и DOT на пользователя, но мы можем хотя бы попытаться и рассмотреть потенциальное влияние, негативное влияние, которое может затронуть пользователей.

Еще я бы хотел уточнить: какие контрмеры мы можем использовать против этих негативных последствий, вызванных DOT или DOH, а также за что будет нести ответственность пользователь, как это повлияет на расходы, уже не с технической стороны, а со стороны пользователя. Спасибо.

ПИТЕР КОХ: Хорошо. Думаю, это скорее предложение чем срочный вопрос, который можно включить в обсуждение. У нас осталось еще два слайда, прежде чем мы откроем дискуссионную панель. Я не вижу больше вопросов.

АЛЕХАНДРА РЕЙНОСО: Нет, переходим к дискуссионной панели. Пролистайте вперед пару слайдов, пожалуйста. Большое спасибо. Сейчас участники дискуссионной панели ответят на вопросы, которые вы видите перед собой. Я зачитаю их вслух.

Вы предполагаете, что развертывание DOH и/или DOT как-либо отразится на вашей работе?

Есть ли какие-либо вопросы, связанные с DOH/DOT, которые попадают под миссию ICANN?

Как, на ваш взгляд, следует реализовать DOH в таких приложениях как веб-браузеры?

Какие опасения у вас вызывают DOH и/или DOT?

Начнем с Тима.

ТИМ ЭЙПРИЛ: Потребуется вечность, чтобы ответить на все эти вопросы, но, поскольку я из сферы безопасности, мне больше всего запомнился, тот, что касается опасений в отношении DOH и DOT с точки зрения конечных пользователей и того, как может измениться их восприятие пространства имен.

Фактически если на начальном отрезке между браузером или приложением и резолвером используется DOH или DOT, вы получаете защищенный канал, но это не

гарантирует того, что соединения между резолвером и организациями имеют хоть какую-то защиту

Поэтому если вы беспокоитесь об утечке данных по каналу коммуникации, это может случиться за пределами резолвера, и также иногда это может происходить из-за самих конечных пользователей.

Также возникает проблема отладки, если вы используете – в зависимости от реализации – особенно в DOH, если приложение использует резолвер DOH без вашего ведома, вы можете приписать некоторые проблемы, связанные с разрешениями, своему ISP и позвонить ему, а он не будет иметь ни малейшего представления о том, что происходит, и для конечного пользователя это будет затяжная проблема отладки, если только у него нет глубоких технических познаний и он не знает где искать.

Я передаю возможность продолжить остальным.

АЛЕХАНДРА РЕЙНОСО: Хорошо. Витторио? Если можно.

ВИТТОРИО БЕРТОЛА: Думаю, мне есть что сказать. Начну с самого первого вопроса. Как поставщик программного обеспечения и поставщик услуг DNS некоторых крупнейших ISP мы

оказываем воздействие в том, что касается реализации нового протокола и внедрения его в жизнь, на нескольких [платформах, которые обслуживают несколько] миллионов запросов DNS в секунду, но настоящая проблема не в этом.

Как компанию, занимающуюся разработкой ПО в том числе с открытым кодом, нас больше беспокоит проблема открытости интернета и того воздействия, которое это может оказать на формирование рынка разрешений DNS и услуги в целом.

Поэтому, на мой взгляд, реальная проблема здесь состоит не в шифровании и не в передаче данных по зашифрованному соединению, что хорошо для сохранения конфиденциальности. Дополнительное движение DNS и то, что из сетевой службы, из того, что предоставляется в рамках сетевой службы вашей операционной системы, например, стек протоколов TCP IP, она превращается в службу приложений, в то, чем непосредственно управляет каждое приложение.

Это может вызвать целый ряд проблем. Часть из них связана с возможной путаницей, как мы уже говорили, разные приложения ведут себя по-разному. Но больше всего беспокойства вызывает то, что рынок приложений, особенно, если взять веб-приложения, которые на данный момент являются самыми распространенными в

использовании видами приложений, является намного более концентрированным по сравнению с сетевым рынком.

В настоящий момент если вы хотите собрать 95 % мировых запросов DNS, вам нужно собрать вместе 1000 самых лучших резолверов DNS. В интернете, и это только для компаний. Все они, кстати, находятся в одной и той же юрисдикции в одной стране.

Поэтому в том, что касается потенциального политического воздействия, особенно в вопросе юрисдикции, суверенитета и всех этих вопросов, это многое меняет, поскольку всем нам известно, что для правительств, думаю, несколько групп интересов будет затронуто. Одна из таких групп представлена ISP, но, думаю, что в этом контексте, возможно, [стоит] поговорить о правительствах и конечных пользователях.

Для правительств это воздействие, эта проблема действительно связана с утратой контроля над разрешениями DNS, особенно это касается стран, которые решили использовать DNS для предоставления таких дополнительных услуг, как, например, родительский контроль, или задействовать любой вид контроля и фильтрации контента, который могут видеть их граждане.

В итоге происходит следующее: веб-браузеры могут просто начать пользоваться этими глобальными платформами, и все это утратится, а весь контроль окажется в другом месте, которое не попадает под юрисдикцию страны. Вот почему, по крайней мере, британское правительство уделяет этому внимание, и я надеюсь, что остальные правительства тоже это сделают.

Что касается пользователей, существует потенциальная проблема выбора, поскольку если приложение начнет выбирать – или просто отправлять запросы DNS любой стороне, какой хочет, а также просто ограничивать выбор, заявляя: «Мы теперь [неразборчиво] те, кто решает, кто может запускать резолвер, и вот он список аккредитованных нами всего 10 резолверов по всему миру, а все остальное мы запрещаем.»

То они превратятся в контроллеров и будут определять политики разрешения DNS. И в конечном итоге, это зависит от политики, поэтому напоследок я хочу сказать следующее: все действительно зависит от модели развертывания, но чтобы прийти к соглашению по модели развертывания, нужна совместная политика, либо по принципу «снизу-вверх», либо такая, чтобы создатели приложений не могли делать все что им заблагорассудится, а чтобы было общее понимание того, что произойдет.

АЛЕХАНДРА РЕЙНОСО: Спасибо, Витторио. Мишель?

МИШЕЛЬ НЕЙЛОН: Спасибо. Вопросы перед нами я совсем не считаю простыми. Такие вопросы всем нравятся: сложные вопросы. Думаю, некоторые из них носят теоретический и научный характер, по крайней мере на данный момент, на самом начальном этапе. До самого недавнего времени DOH и DOT носили гипотетический характер. Теперь они становятся реальностью.

А что такое реальность? Как это на нас повлияет? Второй вопрос. Миссия ICANN может быть затронута, если в итоге сложится ситуация, в которой общедоступные идентификаторы перестанут быть общедоступными. Потенциально вы можете оказаться в ситуации, в которой намного меньшее количество операторов резолверов DNS будет решать, что включать в состав DNS, куда люди могут выйти и до чего добраться. Я считаю, что это может оказать потенциальное воздействие.

Моя собственная компания является поставщиком услуг хостинга, регистратором, и мы также оказываем услуги ISP. Люди не понимают, что такое доменное имя. Они не видят разницы между доменным именем и браузером, или между поисковой системой и адресной строкой браузера.

И когда кто-то говорит: «Ох, пользователь может сам выбрать, какую службу для этого использовать», это справедливо только если иметь в виду кучку компьютерных фанатиков. У скольких присутствующих есть собственный сервер имен? Хорошо. Я осматриваюсь в зале и прекрасно знаю, что все это компьютерные фанатики.

У скольких из вас есть собственные почтовые серверы? Практически те же, кстати. А теперь начистоту: кто-нибудь из вас положа руку на сердце может назвать себя типичным интернет-пользователем? Хорошо.

В том то и дело. Поэтому говорить о наличии выбора не вполне справедливо. И наконец, что касается типа политики и технических аспектов этого, в некотором отношении это все равно что открывать ящик Пандоры. Но почему мы здесь оказались? Если вернуться к презентации Дэнни и рассмотреть сравнение разных технологий, то возникает вопрос: почему это произошло? Как это – что стало причиной?

А реальность такова, что в том мире. в котором мы сейчас живем, людей волнует конфиденциальность и безопасность. Если вас не заботит вопрос конфиденциальности и безопасности, то где вы были последние несколько лет? DNS была слишком открытой

во многих отношениях. У нее было полно интересных проблем.

И вот у нас есть потенциальное решение некоторых из этих проблем, которое создает новый набор проблем, что, разумеется, добавит некоторым из нас работы до конца наших дней.

С практической точки зрения, я вообще себе не представляю, как буду объяснять своим клиентам, почему что-то не работает, поскольку достаточно плохо уже то, что они звонят и говорят, что у них возникли проблемы с Outlook, хотя они не пользуются Outlook, а просто считают Outlook единственным почтовым клиентом, а Firefox – единственным существующим браузером.

Так что я считаю, что нам предстоит столкнуться с интересными операционными проблемами, и если вы посмотрите на то, что должно случиться в ближайшие несколько месяцев по мере того, как это будет становиться реальностью в небольшом комплекте браузеров и возможно других приложениях, вы будете ощущать беспокойство в отношении безопасности, вы будете – люди уже находят новые и любопытные способы злоупотребления этой новой технологией. Они используют записи TXT в DNS для распространения вредоносного ПО. Я видел презентацию по этому вопросу

пару недель назад и сказал: «Ого, это невероятно пугает, но почему я сам об этом не подумал?» Простите, я шучу, вроде того.

Но, на мой взгляд, нам нужно очень пристально на это посмотреть. Лично у меня много опасений связано с самой идей передачи контроля, с этим решением. Я рассматриваю этот вопрос с точки зрения собственной сети офиса, сможем ли мы защитить свой персонал от вредоносного ПО и многих других видов атак? У нас есть для этого подходящая технология?

И мне кажется, что ответ здесь – нет. Но разве это настолько плохо? Думаю, что нет, но может стать.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо, Мишель. А теперь я снова открываю обсуждение: можете задать вопросы участникам дискуссионной панели. Я вижу номер шесть, а за ним номер пять. Хорошо, прошу вас, номер шесть.

МИЛТОН МЮЛЛЕР (MILTON MUELLER): Здравствуйте. Во многих обсуждениях DOH всплывает термин «консолидация и концентрация». Но не в DOT, насколько я понимаю. Но для тех, кто имеет дело с экономическим анализом, эти термины несут в себе очень конкретное значение. Концентрация и консолидация – это плохо, поскольку они могут привести

к наличию монопольной власти, власти над ценами у поставщика.

Насколько я понимаю, большинство сервисов DNS, используемых сейчас людьми, не сконцентрированы, они распределены, никто за них не платит, это так? И опасения касаются того, что концентрация приведет к ситуации вроде установления монопольно высокой цены на сервис DNS, или это какое-то другое опасение? Вы можете уточнить, в чем это опасение заключается и как оно затронет общий рынок интернет-услуг?

АЛЕХАНДРА РЕЙНОСО: Кто-нибудь?

ВИТТОРИО БЕРТОЛА: Не думаю, что это опасение связано с ценообразованием, поскольку на сегодняшний день вы получаете DNS от своего ISP в рамках приобретаемой услуги доступа в интернет. Оно скорее касается концентрации информации и контроля.

К примеру, это протокол, путем [неразборчиво] продвижения конфиденциальности, но если в итоге около 60 % мирового населения будет использовать один и тот же резолвер, да, этот резолвер получит доступ к информации о [действиях] браузеров 60 % мирового

населения, что в итоге приведет к ощутимой утрате конфиденциальности.

АЛЕХАНДРА РЕЙНОСО: Мишель?

МИШЕЛЬ НЕЙЛОН: Спасибо. Я думаю, Милтон, как сказал Витторио, это связано не с ценой, а с тем как работает интернет, пока есть распределение. Это сеть сетей. Каждый ISP может настроить собственные резолверы, каждая сеть, мы все можем настроить собственные резолверы, если их сконцентрировать в одном месте, то утратится стабильность, то есть отказоустойчивость. Существует вероятность лишиться отказоустойчивости.

А кроме того, существует следующая проблема: в трафике DNS содержится огромный объем данных не только о том, что там есть, но и о том, чего там нет. И что люди пытаются найти то, чего не существует. Это стоит огромных денег.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо. Теперь пять.

НЕИЗВЕСТНЫЙ МУЖЧИНА: Необходимо прояснить один момент: когда вы говорите о DNS на уровне браузера, это пользовательский уровень и кто тогда применяет политики? Как нам внести ясность на уровне политики? Таков мой вопрос. Да.

ТИМ ЭЙПРИЛ: Кажется, ваш вопрос о том, кто будет устанавливать или определять политику, реализуемую в браузере. Вы об этом спрашиваете? Здесь все зависит от производителя браузера и любого пользователя, который даст им обратную связь в отношении того, что он выбирает реализовать. Нет такого политического механизма, который может их заставить что-то сделать. Это их ПО, по сути, они могут делать что захотят.

АЛЕХАНДРА РЕЙНОСО: Спасибо. Пункт номер три.

ЭДУАРДО ДИАС: Огромное спасибо. Возможно ли, что если я стану крупной компанией с крупным резолвером, то я смогу начать продавать или предлагать домены верхнего уровня без обращения в ICANN? И другие резолверы смогут связаться со мной, если не найдут свой корень, правильно? Это вообще возможно? Такое может произойти?

ТИМ ЭЙПРИЛ: Технически это возможно. Никакого запрета здесь нет.

ДЭННИ МАКФЕРСОН: Не думаю, что DOH или DOT хоть как-то это меняют.

ТИМ ЭЙПРИЛ: Это очень похоже на то, как был создан домен .onion.

АЛЕХАНДРА РЕЙНОСО: Спасибо. Номер 4.

ФРЕД БЕЙКЕР: Лично меня беспокоит маршрутизация в интернете. Вы, вероятно, в курсе того случая, о котором я сейчас расскажу. Это национальная организация, но я постараюсь ее не называть.

Здесь проблема часто также является корпоративной. Компании внедряют модели информационной безопасности и частично реализуют их посредством отказа в доступе определенным комплектам имен так или иначе.

Организация, о которой я говорю, люди в ней решили начать использовать резолвер Google, и обошли ее, компания, о которой я говорю, обошла эту характеристику путем захвата маршрута до резолвера Google.

И в тот момент, когда решением, обеспечивающим безопасность, становится захват маршрута, как человек, имеющий отношение к маршрутизации, я начинаю сильно волноваться. Будет интересно послушать ваши комментарии по этому вопросу.

АЛЕХАНДРА РЕЙНОСО: Дэнни?

ДЭННИ МАКФЕРСОН: Я просто скажу, да, система маршрутизации – это сеть доверия, которая работает следующим образом: вы где-то услышали, что это маршрут, и вы решаете поверить в то, что кто-то вам говорит, и вы распространяете это, или нет, на данный момент центр управления отсутствует. Существуют определенные средства, например, RPKI и другие, которые должен использовать каждый, кто управляет критически важной инфраструктурой, и другие средства для повышения безопасности системы маршрутизации. Но я согласен, на мой взгляд, действующая система маршрутизации, вероятно, является одной из тех, что вызывают самые большие опасения во всем интернете на сегодняшний день, и любой сервис находится под ее контролем, пока мы не приводим этот вопрос в порядок.

ТИМ ЭЙПРИЛ: А также это повод – это отличная возможность сказать о том, что люди должны принять к сведению использование DNSSEC и [DANE], чтобы [неразборчиво] для любых используемых ими резолверов, для того чтобы когда устройство или резолвер (или любой элемент, который делает запрос) пытается связаться с сервером, он мог подтвердить его сертификат в DNS, а использование DNSSEC подтверждает, что связь устанавливается именно с тем сервером, к которому обращен запрос, и если вы находитесь в области, у которой есть доступ к ключу, признанному надежным вашим [хранилищем сертификатов,] то вы не можете просто полагаться на сертификат X.509, проверяемый по вашей цепочке доверия, как и не можете ему доверять на этом этапе.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо. Номер шесть.

МАРК СВАНКАРЕК (MARK SVANCAREK): Что касается вопросов к аудитории: каковы ваши опасения, часто звучит опасение в отношении концентрации поставщиков услуг DNS. И почему этот вопрос не поднимается в отличие от этих протоколов? Если самый популярный браузер по умолчанию – насколько я понимаю, это происходит по умолчанию – перейдет на адрес 8.8.8.8, вы и так получит огромную концентрацию независимо от новых

протоколов. Почему этот вопрос не вызывает у нас самых больших опасений? Это просто усиливает тенденцию.

Я думаю, что этот пункт необходимо включить наряду с вопросами, касающимися этих протоколов. Спасибо.

ТИМ ЭЙПРИЛ: Я опережу Уоррена. Уоррен говорил, что Chrome не будет выбирать 8.8.8.8 по умолчанию. Этот адрес просто можно выбрать. Есть и другой браузер –

МАРК СВАНКАРЕК: [Уоррен сказал, что это справедливо только для DOH.] [Неразборчиво]

АЛЕХАНДРА РЕЙНОСО: Пожалуйста, говорите в микрофон.

ТИМ ЭЙПРИЛ: Уоррен может меня поправить, если –

МАРК СВАНКАРЕК: Прошу прощения, если я исказил слова Уоррена.

ТИМ ЭЙПРИЛ: Уоррен может меня поправить, если я ошибаюсь, но я так понимаю, что Chrome планирует внедрить это по

умолчанию, если ваш настроенный резолвер, чтобы резолвер вашей системы получал доступ к DOH, он будет использовать это в качестве комплекта разрешений. В противном случае он вернется к системному резолверу и тогда пользователь сможет по собственному выбору использовать DOH для любого резолвера по его выбору, который будет поддерживать этот протокол. Поэтому вы можете выбрать 8.8.8.8. Возможно, эту предконфигурированную настройку можно будет выбрать из списка раскрывающегося меню, но она не будет активна по умолчанию в Chrome.

ВИТТОРИО БЕРТОЛА: Если можно, я дополню в более общем плане, да, вы правы – многие проблемы в сфере безопасности, конфиденциальности, суверенитета [неразборчиво,] которые мы обсуждали, существуют уже сегодня, когда пользователь вводит один из адресов серверов, допустим, 8.8.8.8, а не использует предоставленный ему по умолчанию сетью.

Суть в том, что это уже делает этот выбор по умолчанию, поэтому браузеру намного проще переключать людей с локального резолвера на более крупный, и что касается проблематики – я согласен с тем, что любой вид концентрации уже вызывает опасения. И я крайне рад тому заявлению Google о том, что компания не применяет

сейчас такую модель развертывания, но что будет через пять, десять лет или дальше?

АЛЕХАНДРА РЕЙНОСО: Большое спасибо. Номер пять.

РОБЕРТО ГАЭТАНО (ROBERTO GAETANO): Большое спасибо. Я достаточно стар, чтобы помнить времена, когда сетевое программное обеспечение представляло собой набор собственных разработок, которые делали все понемногу в разных сферах. А затем мы произвели архитектуру с семью уровнями: с транспортным уровнем, физическим уровнем и т. д. – и всеми семью из них.

И в результате получили возможность создавать открытое ПО и решения для каждого уровня, которые могут между собой конкурировать. А теперь с моделями DOH и DOT, разве мы не возвращаемся назад к собственным разработкам, ограничивающим возможность наличия конкурирующих решений, и к тому, что в [60-х ] совершенно неуместно – особенно для меня, итальянца – называлось спагетти-кодом. Спасибо.

ДЭННИ МАКФЕРСОН: Да, думаю, это справедливое замечание. Думаю, что стек протоколов TCP IP и уровневая модель все еще будут

использоваться, просто обмен данными будет идти по первому разрешению имен, а не использовать stub-резолвер в локальной системе.

Разумеется, если вы увидите распределение в путях разрешений на локальной системе или они полностью обойдут его, то это повлияет на пользователя, на сетевого оператора и на инфраструктуру, и некоторые стороны могут выиграть, а другие – так или иначе проиграть от этого.

Поэтому с одной стороны, мне понятна ваша точка зрения. С другой стороны, не думаю, что это чем-то отличается, но, на мой взгляд, если вы являетесь владельцем приложений конечных пользователей и у вас есть возможность привязать их непосредственно к той инфраструктуре разрешения имен, к которой вы хотите, то вы сможете видеть обе стороны такой транзакции, а это может повлиять на сетевых операторов, как отметил Уоррен и ребята из Google, чтобы эти резолверы поддерживали эти новые возможности, и контроль такой инфраструктуры разрешения имен и такого поставщика услуг над пользователем может оказать сильнее, чем они осознают, и это может стать проблемой.

Поэтому с этой точки зрения, я считаю это справедливым замечанием.

ПИТЕР КОХ: Роберто, вы и предыдущий спикер не стали говорить о том, что это, по большому счету, напоминает формирование и отход от бункерного мышления, если смотреть более комплексно. Но эта тенденция необязательно связана со стандартизацией этих протоколов. Как я сказал, вероятно, они совсем безвредны. Но следуют общей тенденции.

На смартфонах большинства из вас установлено огромное количество приложений, и уже давно обсуждаются средства стандартизации и, разумеется, использование централизованной инфраструктуры, поскольку, когда я использую приложения, которые просто звонят домой, что я [неразборчиво] стандартов для уровня, отличного от HTTP, и все выполняется там, я могу сделать сам?

Это часть более важного вопроса. Разумеется, дело не только в этом, есть и другая тенденция: она касается самой инфраструктуры, с которой имеет дело ICANN, и это одна из основных причин, почему стоит затронуть этот вопрос перед этой аудиторией.

АЛЕХАНДРА РЕЙНОСО: Спасибо. Номер три.

ЙОРГ ШВАЙГЕРТ (JÖRG SCHWEIGER) Насколько я понимаю, вывод такой: DOH будет нести добро или зло в зависимости от модели развертывания, но я спрашиваю себя, правда ли это? И если решать будет только пользователь, то полезнее будет использовать DOH. Но примите во внимание, что пользователь загружает приложение, а затем путь разрешений будет лежать глубоко внутри этого приложения.

Таким образом в настоящее время выбора не существует, и раз этот магазин приложений будет принадлежать основному игроку, то, конечно, выбора нет. Так все ли зависит от модели развертывания?

ВИТТОРИО БЕРТОЛА: Это тоже бурно обсуждалось в IETF, поскольку, конечно, обсуждалось насколько эта проблема относится к протоколу и насколько к тому, как люди его используют.

Думаю, что в любом случае важнее всего, чтобы мы поняли, можно ли провести обсуждение среди всех заинтересованных сторон в отношении подходящей модели развертывания и каким образом. Поскольку в конечном итоге, если бы, к примеру, приложения должны были предоставлять пользователю выбор или даже по умолчанию использовать то, что пользователь настроил на устройстве, в операционной системе, в качестве настройки по умолчанию, и если бы эти приложения

использовали эту настройку в качестве правила, это начало бы сводить на нет большую часть проблем.

Но вопрос в следующем: как нам провести такое обсуждение? Поскольку здесь очень мало представителей производителей веб-бразуеров и хотя это могут быть люди из тех же компаний, они не делают эти браузеры. Как нам привлечь таких людей к обсуждению политики?

АЛЕХАНДРА РЕЙНОСО: Спасибо. У нас есть два удаленных вопроса, прошу вас.

АРИЭЛЬ ЛИАНГ: Первый удаленный вопрос от Кристофера Уилкинсона (Christopher Wilkinson). Концентрация является глобальной проблемой на протяжении 20 лет. Корневые серверы, DNS-серверы, [ISP,] DNS и т. д.

Почему теперь мы двигаемся в противоположном направлении? Где будут расположены эти резолверы [вызывает отсутствие безопасности?]

ВИТТОРИО БЕРТОЛА: Я бы хотел сделать одно замечание: может, существует возможность распределить платформы резолверов и получить по серверу в каждой стране. Но если компания по-прежнему будет находиться в конкретном месте

ведения деятельности в конкретной юрисдикции, то она всегда будет сталкиваться с этим. Поэтому я поддерживаю опасения, о которых сказал Кристофер.

ДЭННИ МАКФЕРСОН: Я бы хотел добавить, что, на мой взгляд, система корневых серверов и, возможно, некоторые регистратуры, вероятно, являются самыми широко распределенными системами разрешений и интернет-служб в мире, с географической точки зрения и с точки зрения разрешений. Я действительно считаю, что если – [выполнялась] какая-то работа в прошлом по тому, что мы называем гипергигантами, где 20 интернет-организаций (или около того) составляли около 80 % всего сетевого трафика и адресатов, и, конечно, если эти организации управляют этим вопросом, а ISP и другие люди не делают выбор в пользу защиты конфиденциальности данных по разрешениям, то эти организации могут увидеть еще больше трафика, и это повлечет за собой юрисдикционные и прочие сложности. Но, я считаю, что естественная экономика и капитализм помогут решить и устранить эту проблему с течением времени. Мы говорим о только зарождающейся технологии. Поэтому, думаю, ей есть куда расти.

АЛЕХАНДРА РЕЙНОСО: Спасибо. Второй вопрос?

АРИЭЛЬ ЛИАНГ: Второй вопрос – от Майка Бэгли (Mike Bagley). Разве DOH не улучшает возможность обхода систем защиты на основе DNS и расширений для блокировки рекламы? Разве это не повышает риск для безопасности?

МИШЕЛЬ НЕЙЛОН: Кратко — да.

ДЭННИ МАКФЕРСОН: Я отвечу подробнее. В своей презентации я отметил смешение, и под ним я имел в виду следующее: если разрешение DNS происходит в одном и том же протоколе для одинаковых адресатов и это происходит на уровне приложений, где и интернет-трафик, то любой, кто захочет воспользоваться этим каким-либо образом, должен будет потрудиться, чтобы выделить этот трафик и найти то, чем он хочет воспользоваться.

И честно говоря, это одна из проблем: на сегодняшний день некоторые люди могут воспользоваться ответами DNS, и если вы производитель браузера или внутренняя система или оператор приложения и можете защитить людей от измененных ответов, то можете значительно повлиять на экономику вещей.

Поэтому, на мой взгляд, здесь тоже будут победители и проигравшие, поэтому я думаю, что системы защиты должны активизироваться, и вы можете либо массово

блокировать такие протоколы в организации, что, вероятно, организации и будут делать, или захотите использовать прокси. Вероятно, вы не позволите, чтобы эти вопросы решались за внутренними рамками в сильно контролируемой среде и тем более с точки зрения суверенитета, и это может создать проблемы для экосистемы.

АЛЕХАНДРА РЕЙНОСО: Номер 4.

КАВУСС АРАСТЕ (KAVOUSS ARASTEH): Большое спасибо. Я должен сделать пару комментариев вместо вопросов. Мишель, большое вам спасибо. Вы спросили: сколько из нас понимают, что такое DNS и как она работает? У меня нет на это ответа, поскольку у нас и не может быть никакой статистики, я не могу говорить за кого-то. Это ваши слова.

Затем вы спросили: нас беспокоит безопасность? Ответ — да.

Нас беспокоит конфиденциальность? Ответ — да.

Нас [неразборчиво] технология? Ответ — да.

Но для некоторых из нас – немногих – это новые вопросы. Нам нужно их переварить. Нам нужно их осознать. Прежде чем ответить на любой из этих вопросов,

нам нужно увидеть, как это работает и отвечает ли вопросу безопасности и конфиденциальности. Это животрепещущие вопросы или темы, нам нужно сосредоточиться на них, и сложно ответить на любой из этих вопросов, даже на второй вопрос, который непосредственно связан с миссией ICANN. Возможно, нам будет что добавить к этому вопросу, а может останется [только] этот. В любом случае, нам нужно время. Большое спасибо.

МИШЕЛЬ НЕЙЛОН: Спасибо, Кавусс. В кои-то веки мы действительно согласны друг с другом. Такое случается нечасто. Думаю, здесь все дело в том, что все это в новинку, и некоторые из нас упомянули о том, что это новая, зарождающаяся технология.

То, что, на мой взгляд, многие из нас пытались сделать – это попытаться побудить людей из различных частей экосистемы начать задавать эти вопросы, задавать простые вопросы, более сложные вопросы, действительно сложные вопросы на теоретическом уровне, а также поговорить с компаниями, которые занимаются развертыванием этих технологий.

И они скажут: «Ой, все в порядке, все отлично. То, чем мы занимаемся, послужит общему благу.» Но если не подвергнуть их тщательному исследованию, то можно и

не узнать, что так будет всегда. То, что изначально было безвредно, может стать чем-то другим. А может остаться безвредным.

Думаю, что нам нужно обратить на это внимание и задействовать некоторых из присутствующих, возможно, задействовать уже за пределами этого помещения, и продолжить вести этот разговор, поскольку этот вопрос обсуждался в IETF и некоторых технических кругах, когда, где-то три-четыре года назад? Возможно, больше. Все началось с простого вопроса: «Как нам повысить конфиденциальность DNS?» А затем все менялось и продолжало меняться. Многие из присутствующих, кто не входит в IETF, в число ярых фанатиков, не обращали на это внимания, а теперь это претворяется в жизнь, и я думаю, самое время начать это обсуждать.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо. Номер пять.

ЭНДИ БЕЙТС (ANDY BATES): Здравствуйте. Спасибо. Энди Бейтс из Global Cyber Alliance. Мы являемся одним из основателей 9.9.9.9, поэтому я считаю этот спор о консолидации очень своевременным. Думаю, мой вопрос участникам дискуссионной панели такой: мы не хотим, чтобы пользователи остались со стандартной DNS, поэтому

используете ли вы «четверки» или другие решения, на мой взгляд, самое важное – это предоставить пользователям подлинную защиту от киберпреступности.

Поэтому я думаю поставить вопрос так: что вы выберете – консолидацию или киберпреступность? Других вариантов нет. Но я с удовольствием выслушаю ваше мнение.

ВИТТОРИО БЕРТОЛА: Шифрование пути – хорошая вещь, которой, на мой взгляд, нам нужно заняться. Мы бы рекомендовали операторам [неразборчиво] – развернуть DOH. В то же время, если вы решите определенные проблемы в том, что касается конфиденциальности и безопасности, а затем создадите другие связанные с ними проблемы, которые могут оказаться еще серьезнее, значит продвинуться вперед не получилось.

Поэтому я считаю, что хороший способ избежать этого – это получить общее понимание о том, что происходит, и сформировать совместную политику в отношении того, как это сделать, чтобы максимизировать положительные стороны и решить вопрос с отрицательными сторонами.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо. Номер три?

ВОЛЬФГАНГ КЛЯЙНВАХТЕР (WOLFGANG KLEINWAECHTER): Большое спасибо. Это зал GAC, и вы уже упоминали один из слайдов, касающийся того, что это создаст определенные предпосылки для национальной нормативно-правовой базы. Вы видите здесь полномочия для правительств или вы уже получили какие-то комментарии от представителей правоохранительных органов?

МИШЕЛЬ НЕЙЛОН: Вольфганг, никто из нас – мы не отвечаем за это. Мы всего лишь группа людей, которую попросили рассказать об этом по ряду совершенно разных причин, но если вы хотите задать этот вопрос – не задавайте его нам, думаю, это лучшее, что можно ответить.

Витторио, конечно, сейчас поспорит со мной, но это его роль в этой дискуссионной панели. Питер со мной поспорит.

ПИТЕР КОХ: Впервые в истории, Мишель. Так что, да, отличный вопрос. Думаю, что существуют определенные аспекты всего этого спора о блокировке и существуют правительства, которые верят в блокировку DNS и в то, что она не позволит конкретному пользователю определенного контента получить к ней доступ.

Мы знаем, что эти средства легко обойти. Однако с другой стороны, там где разрешение доменных имен используется для предотвращения случайного доступа к контенту или чему угодно, если говорить о вредоносном ПО, фишинге и так далее, или [неразборчиво] для установления связи с системами управляющих серверов ботнета, это может сработать, но ничто не говорит о том, что поставщики разрешений – некоторые из них уже сегодня предлагают определенные услуги, например, защиту DNS или, не уверен, что это фирменное название, но есть брандмауэры DNS и так далее и тому подобное. На практике они существуют. Вы можете пойти туда.

А теперь, возвращаясь к вопросу Милтона, да, и некоторые из них берут плату, а другие – данные, что относится уже к совсем другой теме. Но некоторые из них берут плату за то, чтобы вы могли получить доступ к их службе разрешений, которая содержит черные списки для известных вредоносных и фишинговых сайтов. И хотя бы некоторым другим поставщикам, о которых мы говорили, ничто не мешает внедрить это. В этом смысле не все истории о правилах и о том, как легко их обходить, стоит принимать на веру. Там существует определенные сложности и определенные детали.

И если вы верите в блокировку DNS, то вы могли бы поверить в блокировку DNS даже с использованием DNS по HTTPS.

ВИТТОРИО БЕРТОЛА: Я только хотел добавить одну вещь. Лично мне не очень нравится блокировка DNS, но я считаю важным, чтобы решение о том, блокировать ли контент, принималось в духе демократии каждой страной и ее собственным интернет-сообществом, а не интернет-компаниями и производителями браузеров. Поэтому, на мой взгляд, в этом смысле это вопрос полномочий. И вот что меня раздражает: некоторые сторонники DOH выступили с интервью, в которых заявили: «Мы собираемся спасти мир от цензуры, а любой вид контроля над контентом – это цензура даже в демократических странах.»

И меня как европейца это действительно раздражало. А что касается других правительств – мне известно только о британском правительстве, но если есть другие правительства, которые разбираются с этим – добро пожаловать.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо. Мы переходим к номеру четыре, а затем закрываем очередь из удаленных участников.

СЕБАСТЬЕН БАШОЛЕ (SÉBASTIEN BACHOLLET): Спасибо. Я буду говорить по-французски, поскольку у нас в зале есть ресурсы для устного перевода и квалифицированные устные переводчики. Итак, я индивидуальный конечный

пользователь, я член комитета At-Large (ALAC) и я хотел задать несколько вопросов. Но у меня уже есть ответ.

У меня есть еще два вопроса: в чем заключается выбор конечного пользователя во всем этом? Разве не существует риска оказаться в ситуации, в которой мы были несколько лет назад вместе с MSN, CompuServe и так далее? Теперь это будут другие компании. Но кто-то будет выбирать место разрешений за нас.

Мой второй вопрос связан с тем, что мы входим в ICANN. Каковы возможные последствия для присвоения имен, для корневых серверов, и в перспективе как все это будет управляться в будущем? Можем ли мы себе представить, что в самом существовании ICANN больше не будет необходимости? Поскольку эти резолверы, серверы могут решить, что они добавят в свои файлы новые расширения, новые имена, или могут удалить их? То есть блокировать или добавлять. Как мне кажется, это важные вопросы.

И я согласен с тем, что вы сказали ранее. Важно, чтобы мы продолжили заниматься этими вопросами. Слишком плохо, что стандартизация была готова еще до того, как мы смогли обсудить эти темы со всеми заинтересованными сторонами. Большое спасибо.

МИШЕЛЬ НЕЙЛОН: Себастьен, спасибо за вопросы. Думаю, что мы уже отчасти ответили на ваш первый вопрос в сессии вопросов и ответов в начале этого заседания. Да, существует вероятность оказаться в итоге в ситуации, когда пара поставщиков выбирает, что будет дальше. И как я уже коснулся этой темы ранее, существует противоположность блокировки, когда есть возможность добавлять. Это риск.

Но протоколы и стандарты разрабатывают члены IETF и другие организации по стандартизации. Они устраивают обсуждения. И вы можете следить за этими обсуждениями. Они открыты.

Конечно, препятствие, существует техническое препятствие для входа. Это не для всех. Существуют стандарты, которые влияют на нашу повседневную жизнь, а многие из нас ничего бы не поняли из того, о чем они говорят поскольку это не наш профиль.

Чтобы люди были в курсе этого и могли это обсудить. Думаю, именно поэтому ведение этих обсуждений сейчас вполне обосновано. Не знаю, кто-нибудь хочет что-то добавить? Тим?

ТИМ ЭЙПРИЛ: Я просто хотел дополнить, что технологии DOH и DOT по своей природе не являются корнем зла в этом случае.

Все зависит от реализации, которая как раз повлияет на то, как будут приниматься эти решения, хотя все это можно было сделать без того, чтобы IETF предлагала DOH или DOT в качестве стандартов. Их реализацией могли бы заняться поставщики браузеров независимо друг от друга.

И основная причина того, что сейчас эта тема так бурно обсуждается, состоит в том, что они выступают в качестве предложенных стандартов, и еще активно обсуждается усовершенствование – или добавление этого механизма защиты конфиденциальности на начальном отрезке запросов DNS.

Уверен, если на пути у этого развертывания встретятся препятствия, умные люди в IETF продолжат искать способы их обойти.

АЛЕХАНДРА РЕЙНОСО: Простите, что перебиваю, но, думаю, нам нужно ответить на последний удаленный вопрос, поскольку мы уже выбиваемся из графика. Простите, что перебиваю. Мы сможем продолжить этот разговор уже потом в кулуарах. Пожалуйста, удаленный вопрос.

АРИЭЛЬ ЛИАНГ: На самом деле удаленный вопрос – это комментарий от Пола Хоффмана (Paul Hoffman). DOT и DOH – новые

протоколы, но у приложений и операционных систем была возможность сделать что-то аналогичное более 20 лет.

ВИТТОРИО БЕРТОЛА: Он один из авторов стандарта DOH. Но это справедливое замечание.

АЛЕХАНДРА РЕЙНОСО: Хорошо, большое спасибо за комментарий. Теперь [чтобы подвести итог] и завершить эту тему, представляющую особый интерес, я попрошу каждого из вас быстро подумать над тем, что эта аудитория должна вынести из этого разговора. Можете начать прямо сейчас. Спасибо.

ТИМ ЭЙПРИЛ: Я буду первым и начну с простого. Как я только что говорил, DOH и DOT – это два предложенных стандарта в IETF, которые не добавляют системе доменных имен никаких технических возможностей, которых невозможно было бы добиться посредством нестандартизированных методов.

И большое опасение, по крайней мере у меня, вызывает то, что многие из тех разговоров, которые мы здесь вели, во многом зависят от политик и подробностей реализации обоих этих протоколов в [неразборчиво] приложениях или

в резолверах и полномочиях по мере того, как мы реализуем эти меры.

ВИТТОРИО БЕРТОЛА: Мое напутствие: продолжайте осознавать, особенно, если вы впервые наткнулись на это обсуждение, многие будут рады помочь, и в интернете уже есть материалы презентаций. Можете найти персонал. Но затем подумайте о том, как [обычная] заинтересованная сторона может принять участие в остальном сообществе и внести свой вклад в это обсуждение в группе IETF или группах формирования политики, которые еще не определены, но могут обсуждать более технические и политические вопросы.

ПИТЕР КОХ: Да, я хочу сказать, что стандарты от IETF, вероятно, играют важную роль в разработках, которые мы видим, но они не являются первопричиной, и мы должны сосредоточиться на первопричине и получить более комплексное представление: что это значит для ICANN и среды ICANN, а также для будущего управления пространством имен?

ДЭННИ МАКФЕРСОН: Да. С практической точки зрения, думаю, что имеют место определенные накладные расходы, но есть и

преимущества с точки зрения конфиденциальности и безопасности, а понимание того, где и как эти протоколы будут развернуты, позволит ввести в курс дела по этому вопросу.

Как член SSAC я считаю, что SSAC только начинает рассматривать этот вопрос и мы, безусловно, будем рады получить от вас обратную связь. Мы все еще перевариваем, и это подвижная цель. И сейчас эти протоколы проходят стадию определения стандартов в IETF. Это еще не полноценные стандарты, но они определенно проходят стадию стандартизации, и [я думаю,] что понимание возможных последствий для ICANN и группы формирования политики, в частности тех, кто участвует в ICANN, это то, в чем рекомендации SSAC могут помочь разобраться или помогут раскрыть более подробную информацию для того, чтобы люди могли фактически выполнять свою работу в ICANN. Спасибо.

МИШЕЛЬ НЕЙЛОН: Алехандра, вы сделали кое-что рискованное. Предоставили мне последнее слово.

АЛЕХАНДРА РЕЙНОСО: Прошу вас.

МИШЕЛЬ НЕЙЛОН: Спасибо. На мой взгляд, здесь были подняты крайне интересные вопросы и комментарии как теми,

кто физически присутствует в этом зале, так и остальными. Что касается лично меня, прежде чем я пришел сюда, у меня были определенные чувства по отношению к этим технологиям, и послушав некоторые вопросы, которые мы задавали, а также комментарии, я продолжаю формировать свое отношение к ним. И я думаю, что для меня это означает, что провести этот разговор было правильным решением.

Мое напутствие вам: если вы посмотрите на слайд, который сейчас на экране, он содержит несколько пунктов о том, где можно найти более подробную информацию на предстоящем заседании IETF. [Кажется, сайт] dnsprivacy.org содержит много информации по этим основным технологиям. Кроме того, различные компании публикуют множество постов в блогах, как и другие группы, например, CENTR, кажется, опубликовал недавно документ по этой теме. Найдите время, прочитайте что-то еще по этому вопросу и задавайте вопросы.

АЛЕХАНДРА РЕЙНОСО: Большое спасибо. Объявляю заседание закрытым. Бурные аплодисменты для наших участников дискуссионной панели.

**[КОНЕЦ СТЕНОГРАММЫ]**