مراكش – جوانب السياسة الخاصة بحل نظام اسم النطاق عبر بروتوكول نقل النص التشعبي الآمن (DoH)
و بروتوكول نظام اسم النطاق على أمن طبقة النقل (DoT) والقضايا ذات الصلة
الثلاثاء، 25 يونيو، 2019 – من الساعة 03:15 م إلى الساعة 04:45 م بتوقيت غرب أوروبا
اجتماع ICANN رقم 65 | مراكش، المغرب

أليجاندرا رينوسو: طاب مساءكم، جميعًا. أرجو التفضل بالجلوس؟ نحن على وشك البدء. شكرًا جزيلاً.

هل يمكنك تجهيز العرض التقديمي من فضلك؟ شكراً. بينما يتم التجهيز، شكرًا لكم جميعًا على الانضمام إلينا. نحن بصدد مناقشة موضوع ذي أهمية عالية حول حل نظام اسم النطاق عبر بروتوكول نقل النص التشعبي الآمن (DoH) و بروتوكول نظام اسم النطاق على أمن طبقة النقل (DoT). أولًا، جدول الأعمال سيتضمن تعريفي لأهداف الجلسة لكم وتقديم جميع أعضاء فريق المناقشة.

سيكون هناك استعراض فني للموضوع، ومن ثم سنتلقى الأسئلة والإجابات. بعد ذلك، سنناقش مخاوف التطوير المحتملة، وبعدها سنتلقى مجددًا الأسئلة والإجابات عليها، وفي النهاية سيكون هناك حلقة نقاش حول اعتبارات التطوير، ونتوقع منكم جميعًا المشاركة في هذا الموضوع المهم. لهذا السبب ستتجول الميكروفونات فيما بيننا. إذا كان بإمكانكم تعريف أنفسكم حيثما أنتم، سترونهم بالأرقام. يوجد أربعة وستة وثلاثة وأعتقد أن الرقم خمسة موجود هناك بالخلف. لا أستطيع رؤيته، لكن عليه أن يكون هناك. ها هي.

حسنًا، وقتما يكون لدى أحدكم سؤال، يرجى رفع يده قدر الإمكان، حتى يتمكنوا من الوصول إليكم وإعطائكم الميكروفون. سيكون رائعًا إذا كان العرض التقديمي جاهزًا.

سوف أبدأ بالتعريف بنفسي. أنا اليخندرا رينوسو من نطاق dot-GT. أنا نائب رئيس منظمة دعم اسماء النطاقات لرمز البلد (ccNSO). ومعي داني ماكفرسون. داني هو نائب الرئيس التنفيذي ومسؤول الأمن في شركة (Verisign) وهو أيضًا عضو في اللجنة الاستشارية للأمن والاستقرار (SSAC).

ومعي أيضًا بيتر كوش. يعمل بيتر لصالح شركة DENIC – مدير نطاقات نطاق المستوى الأعلى لرمز البلد (ccTLD) في DE – وحاليًا بصفته مستشار سياسات. ومعنا

باري ليبا. باري ليبا هو مدير المعايير الأول في شركة Futurewei Technologies. لقد عمل باري في تقنيات البريد الإلكتروني والتقنيات ذات الصلة منذ مطلع الثمانينيات من القرن العشرين ويركز حاليًا على إنترنت الأشياء والتراسل والتعاون في منصات الهواتف النقالة، وأمن وخصوصية تطبيقات الإنترنت، وتطوير ونشر معايير الإنترنت. باري أيضًا عضو في اللجنة الاستشارية للأمن والاستقرار (SSAC).

ومعنا اليسا مور هناك. أعتذر أني لا أشير على الأشخاص. اليسا هي المستشار الأول للسياسات والدفاع في (CIRA)، هيئة تسجيل الإنترنت الكندية، ومدير نطاقات نطاق المستوى الأعلى لرمز البلد (ccTLD) في كندا.

باري واليسا سيكونان المشرفين على الأسئلة والإجابات، وباقي أعضاء فريق النقاش هم تيم أبريل وهو مهندس الأمن الرئيسي في شركة Akamai Technologies التي تعمل في أمن الشبكات DNS والاستجابة للحدث. تيم عضو أيضًا في اللجنة الاستشارية للأمن والاستقرار (SSAC).

هل يمكننا الانتقال شريحتين من فضلك؟ سيكون معنا أيضًا فيتوريو بيرتولا. فيتوريو بيرتولا هو رئيس السياسة والابتكار في شركة Open-Xchange، الشركة الأم لشركة PowerDNS، وقد ناقش تبعات سياسة DNS المشفر في عدة أماكن خلال العام الماضي.

وأخيرًا معنا مايكل نيلون. مايكل نيلون هو المؤسس والمدير التنفيذي لشركة Blacknight Solutions، وهو أمين سجل معتمد لـ ICANN. مايكل عضو أيضًا في مجلس المنظمة الداعمة للاسماء العامة.

هل يمكننا الانتقال شريحتين للأمام من فضلك؟ أعتقد أن لدينا بعض المشكلات الفنية، كالعادة، لكنها ليست شيئًا صعبًا. لا أعلم إذا كان بإمكاننا البدء بالاستعراض الفني بشرائح أخرى. هل بإمكاننا؟ من أجل استغلال الوقت.

سيكون لدينا دقيقة واحدة أخرى لنرى إذا استطعنا الحصول على الشرائح. إذا لم نستطع فلن ننتظر، لكن دعونا نمهلها بعض الثواني. في هذه الأثناء، بإمكانكم تنزيل الشرائح من الجدول لمتابعة المحادثة. أعتقد أن علينا البدء. رجاءً يا داني إن كنت لا تمانع.

داني ماكفرسون: بالتأكيد. سأبدأ من دون الشرائح، وقد كان موضوعًا صعبًا بما يكفي مع الشرائح على الأرجح للعديد من الأشخاص.

أنا داني مكبيرسون، أنا عضو في اللجنة الاستشارية للأمن والاستقرار (SSAC)، وفي هذا السياق، أنا أعرض عليكم شرائح اللجنة الاستشارية للأمن والاستقرار (SSAC). لذا فالأخطاء تخص اللجنة الاستشارية للأمن والاستقرار (SSAC) وليس أنا. سنتعامل مع الأمر.

على أية حال، سنتحدث عن موضوع اليوم، سأغطي الجانب الفني، ومن ثم سيناقش بيتر والفريق بعض التأثيرات المحتملة للجانب الفني. لكن حظي الموضوع العام في الآونة الأخيرة بالكثير من الاهتمام.إنه يتعلق بما نسميه DoH وDoT، إنه حل نظام اسم النطاق عبر بروتوكول نقل النص التشعبي الآمن وبروتوكول نظام اسم النطاق على أمن طبقة النقل.

وباختصار، إن المقصود من هذه التقنيات هو منح السرية لمعاملات DNS. إن DNS لم تمتلك أي فكرة عن السرية المدمجة بها على نحو تقليدي. ولم يكن لديها أي فكرة عن النزاهة المدمجة بها أيضًا، لكن الامتدادات الأمنية لنظام اسم النطاق (DNSSEC) كانت مثبتة إلى حد ما لتوفر حماية النزاهة لـ DNS، لكن هذا الأمر ما زال يترك DNS معرضًا لأشياء مثل المراقبة، والتنصت، وربما معالجة الاستجابات لمختلف العملاء لمجموعة من الأسباب. قد يكون من أجل أشياء مثل المراقبة الأبوية أو الرقابة الحكومية أو منع الوصول إلى موقع ضار لحماية المستخدم.

على أية حال، يوجد مجموعة واسعة من الدوافع لماذا نريد هذا، وعندما تصلون إلى الشريحة السادسة في تلك المجموعة وتطلعون عليها، سترون بعض الأسباب. لذا مجددًا،

الجوهر هنا أن DNS التقليدي وبه فكرة السرية ونوع من الدمج في الحالة الجغرافية السياسية التي نعيش فيها والتبعات الاقتصادية المتعددة للأشياء، التي توفر السرية لمعاملات DNS لها العديد من الفوائد وكذلك بعض الفروع.

لذا سنتحدث عن نماذج التطوير، ليس بالضرورة الكثير عن أولئك. على أية حال، إذا كنتم تتابعون، الشريحة السادسة تتحدث عما شرحته بشكل أساسي.

لذا دون السرية لمعاملات DNS، فإنكم تتركون أنفسكم عرضة لتسرب المعلومات أو هجمات الكشف. لذلك يستطيع الأشخاص النظر لتلك المعلومات ومراقبتكم أو معرفة وجهتكم على الإنترنت وتنقيب تلك المعلومات.

لذلك، الفكرة من كل من DoH وDoT هي توفير تشفير على السلك لما يحدث، لذا إذا كان هناك هجوم على المسار أو كان هناك مراقب، فإنهم لن يتمكنوا من رؤية تلك المعلومات. لذلك، على المستوى الرئيسي، هذا ما تدور حوله DoH وDoT.

الشريحة السابعة في المجموعة توفر بشكل أساسي استعراضًا لـ DNS تقليدي، وفي تلك الشريحة، بشكل أساسي إذا كنتم تفكرون في DNS، فقد حصلتم على جهاز وعلى ذلك الجهاز لديكم برنامج، ويحتاج البرنامج إلى حل شيء في DNS ويطلب عملية محلية على الجهاز مثل متصفح الإنترنت قد يطلب من نظام تشغيل هاتفك الآيفون أو من الحاسوب المحمول، فيقول "مرحبًا، كيف أصل إلى www.example.com؟"

ولدى جهازك أداة حل لـ DNS بها من سيتعامل مع شيء إما على الشبكة المحلية أو بالخارج على شبكة ISP. لذا يمكننا الانتقال إلى الأمام شريحتين أكثر، أعتقد للانتقال إلى الصورة، توضيح الـ DNS التقليدي، الشريحة الثامنة، من فضلك.

هذا ما كنت أوضحه منذ دقيقة. لديكم أجهزة تحتاج في النهاية إلى حل شيء لمستخدم أو عملية على جهاز، ويتعامل التطبيق مع نظام التشغيل المحلي بشكل تقليدي – مجددًا، يمكن أن يكون التطبيق على هاتفك الآيفون أو يمكن أن يكون متصفح إنترنت على حاسوبك المحمول.

ذلك التطبيق أو ذلك المتصفح قد يطلب من نظام التشغيل المحلي مكان اسم الوجهة تلك على الإنترنت، ومن ثم قد ينتقل ذلك الجهاز وقد يتعامل إما مع شيء معلوم بصفته معيد توجيه محلي أو مع محلل راجع على الأرجح.

يشكل تقليدي، تلك المحللات الراجعة كانت في شبكة ISP أو في شبكة محلية وفرها مقدم الوصول إلى الشبكة، لكن يشيع بكثرة أنهم قد يكونوا بالخارج في بنية أساسية لسحابة، على سبيل المثال، DNS مفتوح أو خادم اسم غوغل الراجع الذين يوفران ذلك على الإنترنت في مكان ما في البنية الأساسية للسحابة. لذا فإن هذا يعتبر واحدًا من المتغيرات المعمارية [المعاملات.] قد لا تكون محلية على الشبكة حيث تحدث الحلول بشكل تقليدي.

خادم الاسم الراجع ذلك قد ينتقل إلى بنية أساسية موثوقة، لتكن البنية الأساسية الجذرية والبنية الأساسية لنطاق المستوى الأعلى والبنية الأساسية الموثوقة ويحل الاسم ومن ثم يمرر تلك المعلومات إلى التطبيق مرة أخرى أو إلى محلل كعب الروتين الذي سيعطيها إلى التطبيق، ومن ثم سيتمكن التطبيق من الاتصال بالوجهة المطلوبة على الإنترنت.

وكما ترون من هذا الرسم التوضيحي، جميع تلك المعاملات اليوم، لا توجد فكرة عن سرية تلك المعاملات، لذا إذا كان هناك مراقب على المسار في أي من تلك الأماكن حيث ترون سهمًا أخضرًا في هذا الرسم التوضيحي، من ثم يمكنهم على الأرجح رؤية ما يحاول أن يحله المستخدم، وقد تكون معلومات تجارية تنافسية وقد تكون معلومات تتعلق بالأمن وقد تكون محتوى حساس وقد تكون أي شيء من مجموعة واسعة من الأشياء. لذا فإن ما تدور حوله DoH وDoT هو بعض الوسائل لحماية تلك المعلومات. فلننتقل إلى الشريحة التالية.

لذلك يعرف أحد الحلول على أنه DoT. DoT هو بروتوكول نظام اسم النطاق على أمن طبقة النقل. TLS هو ما نسميه أمن طبقة النقل وهو كاف بشكل مثير للاهتمام المعاملات الأكثر أمنًا على الإنترنت، إذا رأيتم قفلًا تقليديًا أو إذا انتقلتم إلى موقع إلكتروني مالي أو بعض المواقع الإلكترونية الأخرى التي تحتوي على معلومات حساسة؛ أمن طبقة النقل TLS هو البروتوكول الذي يدعم ذلك على الأرجح، ويوفر التشفير في الشبكة وفي طبقة

النقل، ويوفر التشفير أو السرية للمعلومات، بحيث يمكن للمهاجم على المسار إما معالجة أو مراقبة المعلومات على الأقل.

لذلك في نموذج DoT – لننتقل فقط إلى الشريحة التالية، سأوضح هذا الامر من خلال هذه الشريحة. بشكل أساسي، في نموذج DoT، ما يحدث بشكل تقليدي – مجددًا، يمكن استعمال كل من DoH وDoT، تشكيلة من الأساليب المتنوعة. لا يزال هذا الأمر قيد التطوير في كل من المعايير والمجتمع التشغيلي. لكن بروتوكول نظام اسم النطاق على أمن طبقة النقل متوقع بشكل تقليدي في ذلك النظام المحلي، على سبيل المثال، هاتفك الآيفون أو الحاسوب المحمول الخاص بك، قد يحتوي على وضع يشمل النظام ككل ويقول إنني سأستخدم هذا المحلل والبنية الأساسية لحل الأشياء في DNS، وكل تطبيق على ذلك الجهاز سيستخدم ذلك الوضع وينتقل إلى البنية الأساسية ويفعل ذلك.

لذا ما ترونه هنا على سبيل المثال هو متصفح للإنترنت يفعل الشيء نفسه بالشكل التقليدي. سيطلب من وحدة الحل الجزئي المحلية، وسيقول "مرحبًا، أريد الانتقال إلى example.com على الإنترنت. هل ستحل ذلك؟"

وحدة الحل الجزئي الآن، بدلًا من إرسال نص واضح، سيرسلها عن طريق قناة مشفرة بشكل فعال من أجل إما تحمل أو الانتقال لمكان في البنية الأساسية للسحابة أو شبكة مزوّد خدمة الإنترنت ISP لحل المعلومات. وهذا ما ترونه بالأسهم الحمراء هنا بشكل أساسي.

لذا سيتم تشفيرها، لذلك لن يتمكن مراقب المسار أو المهاجم من التلاعب بتلك المعلومات أو على الأقل مراقبة ما يجري. ومن ثم هنا في البنية الأساسية الموثوقة، ليس هناك كثير من الاهتمام اليوم حول المكان الذي قد يتناسب فيه حل DOH أو DOT مع الجذر أو TLD، أو ربما البنية الأساسية لنطاق المستوى الثاني الموثوق. لكن بعض ذلك لا يزال يتم تجسيده.

سنقوم بمقارنة هذا الأمر في لحظة مع DoH، الذي يقوم في الأساس بنقل مستوى التشفير قليلًا. لذا لننتقل إلى الشريحة التالية ولنتحدث عن DoH للحظة.

أنا أنتقل بسرعة جدًا. عذراً. حسنًا، بالأساس، فضلًا عن استخدام TLS لنقل DNS، ما تقوم به DoH في الواقع هو، أتعلمون ما هو؟ لدي الكثير من التطبيقات الإلكترونية على جهازي أو الكثير من حركة زيارة الإنترنت والكثير من البرامج المبنية حول معاملات HTTP في نظام التشغيل هذا أو على هذا الجهاز، لذا بدلًا من استخدام TLS محليًا في البنية الأساسية، سأقوم بتشفير استجابات DNS في الاستعلامات على الإنترنت واستعلامات HTTP ومن ثم وضع ذلك على TLS بشكل كاف، وهو ما يعمل به HTTPS ومن ثم نقلها على الشبكة.

يوفر هذا الكثير من الخطافات لأحد التطبيقات إما للتعامل مباشرة مع البنية الأساسية للحل وتجاوز وحدة الحل الجزئي المحلية تمامًا، أو قد يستخدم وحدة الحل الجزئي التي تعمل على نظام التشغيل. لذا لننتقل إلى الشريحة التالية وسنوضح هذا الأمر للجميع.

بشكل أساسي، ما ترونه -- ومجددًا ما هو إلا نموذج نشر واحد. قد يختلف. لكن ما يمكن أن يحدث هو أن متصفحي قد يستخدم خادم أسماء راجع واحد مع DoH في البنية الأساسية، بينما قد يستخدم تطبيق أخر واحدًا محليًا أو قد يستخدم محلل النظام الخاص بي.

الآن، عندما يصبح هذا الأمر مشوقًا أنه إذا دخل شيء في هذا السيناريو واستخدمت تطبيقات مختلفة DNS مختلف، قد يصبح الأمر معقدًا لفهم ما يجري.

أما الشيء الأخر الذي يحدث أن ISPs قد تستخدم بشكل تقليدي استعلامات DNS كنقطة تحكم في البنية الأساسية، وقد يستخدم أحد المشاريع استعلامات DNS كنقطة تحكم وقد لا يحتاجون إلى معاملات مشفرة تنتقل مباشرة من البرنامج عبر بعض المحيطات أو الحدود في البنية الأساسية، لأنهم قد يفقدون الرؤية الأمنية أو الرقابة الأبوية أو أشياء أخرى لديهم في تلك البنية الأساسية.

لذا فإن صلب الموضوع هنا هو أن الأحرى استخدام وحدة الحل الجزئي في حالة DoH، الذي كان متوقعًا بشكل تقليدي أكثر أن تطبيقًا سيستعلم بشكل مباشر البنية الأساسية للإنترنت، البنية الأساسية للحل للحصول على استجابة DNS وتخطي كل شيء، في كل من نظام التشغيل وعلى الأرجح في مقدم خدمة الشبكة المحلية. هذا ما نعمل على توضيحه بشكل أساسي هنا.

حسناً، لننتقل إلى الشريحة التالية. الآن أحد الأشياء الأخرى المهمة للإشارة إليها هو أنه إذا كنتم تنظرون لهذا من نقطة تحكم أو من منظور تنصت أو مراقبة، فإن DoH تساهم بشكل فعال في حركة حل DNS الخاصة بكم مع حركة HTTP الأخرى على الشبكة. لذا هذا يجعل من الأمر أكثر صعوبة لاحتمالية المراقبة أو التنصت، أو حتى الترشيح، لذا سيكون عليكم فتح كافة حركات HTTP تلك لفعل شيء فني من منظور نقطة تحكم مع استفسارات حل DNS المتعلقة بـ DoH.

مجددًا، DoT هو وضع يشمل النظام ككل، لكن سيكون عليكم أيضًا فعل ذلك، ومن ثم الشيء الأخير أعتقد أني سأوضح على هذه الشريحة أن نماذج النشر التي ترونها لكل من DoH وDoT هنا قد تكون مختلطة وتلك الأسهم يمكن أن تكون مقلوبة. إنها مسألة ما يريده التطبيق ليتم تمكينه، وما يريد مدير النظام تمكينه وما إلى ذلك.

نظام مثل نظام تشغيل مكعب الروتين على جهاز قد يستخدم بالفعل DoH بدلًا من استخدام DoT أو قد يستخدم DNS التقليدي. لذلك أعتقد أن النقاش في هذا الأمر سيطول.

ليس هناك الكثير من الأفكار المقدمة اليوم حول البنية الأساسية الموثوقة، لذلك [غير مسموع] فإن نطاقات jobs، edu، gov، net، أو أيا كان نطاق المستوى الأعلى، أو حتى نطاق المستوى الثاني المحتمل، وهناك بعض التقنيات الأخرى مثل إخفاء الهوية QNAME التي توفر بعض حماية الخصوصية هناك، على الرغم من وجود بعض الفروع مع جوانب مختلفة من ذلك أيضا.

لذلك أعتقد أنني حاولت إخبارنا بالمستجدات بالتحدث سريعًا إلى حد ما لأن مايكل ظل يذكرني، لكننا سنتوقف هنا للحظة ونرى إذا كان لدى أحد أسئلة على هذا الأمر قبل الانتقال لجزء بيتر الخاص باعتبارات النشر. لذا إذا كان لديكم أسئلة، يمكنكم أن تطرحوها الآن فيما يتعلق بما قلناه آنفًا على الفريق، أو يمكنكم الانتظار وترك بيتر يتحدث عن بعض الآثار الأخرى الخاصة بـ DoH وDoT، ومن ثم اطرحوا أسئلتكم.

أليجاندرا رينوسو: شكرًا لك داني على هذا الشرح الرائع والسريع. لدينا سؤال هنا. شكرًا جزيلاً.

نايجل كاسيميري: نعم. طاب مساءكم. أنا اسمي نايجل كاسيميري من الاتحاد الكاريبي للاتصالات. هذا الأمر جديد علي، لذا أنا أحاول فهم المشكلة التي تحاولون حلها بهذا الأمر كله. لذلك، أهي محاولة لجعل DNS أكثر أمانًا؟ وكيف يقارن هذا الأسلوب مع DNSSEC على سبيل المثال؟

ميشيل نيلون: حسنًا، نحن الآن نتشاجر على من سيتحدث. لذا سآخذ الميكروفون. حسنًا، يتم التحدث عن DNSSEC كثيرًا في اجتماعات ICANN وكأنها رصاصة سحرية تحل جميع المشاكل المتعلقة بـ DNS. وهي ليست كذلك. DNSSEC هي وسيلة لقول متى تذهب إلى المصرف الخاص بك. مهما كان ذهابك فعليًا إلى المصرف الذي تتعامل معه وأن شخصًا لم يعترض طريقه وأدخل شيئًا في المنتصف.

لذا هذا النوع من الهجوم هو ما ستسميه تسمم الـ DNS، الذي كان مشكلة في بعض الأماكن في الماضي. لذا تعمل DNSSEC في إصلاح ذلك. بفضل DoT وDoH إنها تحاول أن تضيف مستوى من الخصوصية ومستوى من الأمان معًا، لكن هناك مشكلات مع الإثنين. من حيث الخصوصية، تفهم ذلك، وأعتقد أن بعضًا منا على الأرجح سيتحدث أكثر عن كيف يمكن أن يكون لها آثار سلبية على بعض الجوانب الأمنية للأشياء. لكن ما تقون به بشكل أساسي هو نقل استعلامات الـ DNS تلك، بالوسيلة التي تقوم من خلالها الأجهزة بالبحث – حاسوبك المحمول أو هاتفك أو الآيبود الخاص بك أو شيئًا أخر – بنقلها بعيدًا عن الـ DNS التقليدي إلى البروتوكولات الأخرى.

لذا في حالة DoH؟ إنها ترى فقط على أنها طلب عادي على الإنترنت. مع مراعاة أنني لست خبيرًا مثلها، لذا من المحتمل أن تصحح لي، لكن هذا نوع من الوسائل البسيطة للنظر على هذا الأمر.

أليجاندرا رينوسو: شكرًا لك، ميشيل. لدينا شخص يشارك عن بعد. رجاءً.

آرييل ليانج: يوجد سؤالين من اثنين من المشاركين عن بعد. السؤال الأول من محمد يوسف. هل الـ DNS عبر TLS يسبب تراجعًا في الأداء فيما يخص وقت حل الاستعلام؟ ومن ثم سنقرأ سؤالًا ثانيًا بعد ذلك.

ميشيل نيلون: هذا الأمر يعتمد على كيفية تنفيذ وحدة الحل الجزئي. يمكن أن تفرض عقوبة إضافية أو رحلة ذهابًا وإيابًا إلى المُحلل في وقت إعداد الاتصال الأولي، ولكن إذا تم تهيئة كعب الروتين للاستمرار في الاتصال بمرور الوقت، فيمكن أن تكون - التكلفة [مخففة] هي نفسها تكلفة الـ DNS العادي.

آرييل ليانج: هناك سؤال ثان من المشاركين عن بعد. إنه من يزيد أكانهو من بنين. الشريحة السادسة، التقنيات مثل تقليص تقنية QNAME قد تكون فعالة أيضًا في حفظ خصوصية المستخدم. كيف لكل المحللين تنفيذ هذا؟

داني ماكفرسون: لا نريد الحديث كثيرًا عن تقليص تقنية QNAME، لكنه أسلوب خفيف للغاية. كان DNS مطنبًا جدًا بشكل تقليدي، وإذا أردت حل شيئًا فيه، فسأقدم اسم نطاق مؤهل بالكامل، لذا internalsecretserver.foo.verisign.com، وأود أن أسأل كل خادم موثوق في المسار السؤال كاملًا، عندما يكون في الوقاع لا نحتاج إلا إلى الجذر ليخبرني كيف أنتقل إلى المستوى التالي في التسلسل الهرمي ومن ثم إلى dot-com.

لذا عندما أسأل الجذر سؤالًا، أنا لا أحتاج إلى أن أخبره كل شيء أحتاج إليه، أنا فقط أريد أن أسأله كيف أنتقل إلى dot-com ومن ثم dot.com ستخبرني كيف أنتقل إلى verisign.com، و verisign.com ستخبرني كيف أنتقل إلى الخادم السري الداخلي.

بشكل فعال جدًا لا تكشف عن الاسم الكامل لما تنوي حله، لذا فإنك تقلص هذا الامر. إنها وظيفة تحليل اسمية لحفظ الخصوصية، وهي خفيفة للغاية وهي منتشرة ومنفذة بالفعل

في تطبيقات خادم الاسم الراجع بوسائل متنوعة وهي توفر بعض التقليصات السطحية للهجوم القابل للقياس من منظور الخصوصية.

أليجاندرا رينوسو: شكرًا جزيلاً. سأطلب من الجميع الالتزام بالموضوع قدر الإمكان. نحن نعلم أن هناك مفاهيم ذات صلة جدًا حول الأمن والإنترنت، لكن الآن، علينا أن نحاول التركيز على DoT وDoH حتى يتمكن الفريق من المضي قدمًا. سأتلقى سؤالين آخرين. هناك أربعة، ورقم خمسة هناك، ومن ثم ننتقل للمحاضر التالي. شكراً.

فريد بيكر: لقد دُهشت قليلًا من اجابتك عن الاختلاف بين TLS والعمل مع DNSSEC، لأنهما تؤمنان أشياءً مختلفة. DNSSEC تؤمن المحتوى وسجل الموارد الفعلي، بينما تؤمن TLS القناة.

بالمقارنة، قد تفكرون في ذلك من حيث الأنابيب والماء. لنخيل أن أنني حصلت على أنبوب رائع ومطلي بدرع، سيكون الآن أفضل أنبوب في العالم بلا شك، وعند المنبع، لدي بحيرة ملأتها بالسم. عندما يتدفق من خلال الأنبوب المطلي بالدرع والرائع للغاية، يظل يتدفق بالسموم.

لذا فإن تأمين المحتوى يخلصنا من مشكلة السم. الآن، لن أتحدث عن TLS. امتلاك قناة جيدة أمر جيد أيضًا. لكن DNSSEC تصبح هامة للغاية من حيث ضمان أن الاسم يحمل بالفعل الشيء الذي تحاول الحصول عليه.

داني ماكفرسون: سأرد فقط على ذلك. وأعتقد أن هذه نقطة رائعة، يا فريد. أعتقد أنك حتى وإن امتلكت DoH أو DoT منتشرة بالكامل في النظام البيئي، ستظل تحتاج إلى كل من DNSSEC و QNAME لإخفاء الهوية لتوفير حماية مضافة. هم يعالجون أمر مختلف تمامًا، لذا هذه نقطة جيدة.

أليجاندرا رينوسو: شكراً. رقم خمسة؟

جيم برندرغاست: نعم. مرحباً. أعترف أني لست من فريق مهام هندسة الإنترنت. أعلم أن هناك العديد منكم هنا في الغرفة منهم. داني، كما كنت تستمع إلى الفوائد، تتحدث أيضًا عن بعض الأشياء التي قد يكسرها هذا. كيف تمت الموافقة على هذا كمعيار إذا كان هناك بعض هذه الأشياء التي تحدث كعواقب غير مقصودة؟

شخص غير محدد: [عليك أن تسأل فريق مهام هندسة الإنترنت.]

شخص غير محدد: هذا سؤال جيد يا جيم.

داني ماكفرسون: حسناً. عذرًا. أعتقد أن التقنية موجودة والنظام البيئي سيتكيف لمعرفة نماذج النشر الصحيحة. لا أعتقد أن أي أحد في النظام البيئي بداية من موردي المتصفحات إلى موردي أنظمة التشغيل ومشغلي خوادم الأسماء الراجعة أو مشغلي البنية الأساسية الموثوقة يريد أي شيء أن يُكسر.

من المثير للاهتمام بما فيه الكفاية أن هذا يسبب بعض تحديات النشر حيث الآن إذا كنت أحد مزودي خدمة الإنترنت، وليس لديك أي رؤية لحركة مرور DNS لمتصفح الإنترنت الخاص بالمستخدم، وتستخدم خدمة سحابة في مكان ما لحل DNS، واتصلوا بك لإصلاح مشكلة معهم في DNS، قد لا تتمكن من إصلاح المشكلة. أو إذا طبقت الرقابة الأبوية على DNS، قد لا تتمكن من فعل ذلك.

لذا أعتقد أن النظام البيئي سيكون عليه تعديل هذا ولهذا أعتقد أنه هام بالفعل لكل من DoH وDoT لمعرفة أن نماذج النشر ستختلف وتتكيف.وأعتقد انه بسبب أن السوق والديناميات تملي ما هو الأفضل، وما الذي يعمل وما الذي لا يعمل.

أليجاندرا رينوسو: نعم. شكرًا جزيلاً. بإيجاز، سيناقش بيتر معنا الآن مخاوف التنمية المحتملة فيما يتعلق بـ DoH وDoT.

بيتر كوتش: نعم. شكرًا لك، أليجاندرا. اسمي بيتر كوش. كما تم تقديمي، أنا أعمل لصالح شركة DENIC كمستشار أول لوضع السياسات، وأحد المشاركين المعينين من قبل ccNSO في مجموعة العمل هذه.

لذلك تم دعوتي للحديث عن مخاوف النشر المحتملة. والعنوان الفرعي غير الرسمي في الحقيقة، جيم، كان البروتوكول وهو بريء ومن ثم تحدث الأشياء. هذا من المحتمل أنه سيناقش بعض المخاوف.

الجزء الأول سيكون فنيًا بعض الشيء، لذا لدينا اثنين من المعايير التي تناقش ذات الشيء قليلًا أو كثيرًا – أجل، نحتاج، أعتذر –

أليجاندرا رينوسو: [غير مسموع] شريحة من فضلك. شكرًا جزيلاً.

بيتر كوتش: أجل، هذه هي المقصودة. حسنًا، سأقوم بهذا من هناك. لذا لدينا اثنين من المعايير التي تناقش بطريقة فنية مختلفة قليلًا المشكلة نفسها المتعلقة بسرية حركة DNS ذهابًا وإيابًا.

للتذكير فقط، الأشخاص الذين يسألون لماذا هذا، كان هناك شخص يدعى سنودن منذ عامين، وما اكتشفه، أو على الأقل شاركه، هو أن حركة DNS يمكنها أن تكون مصدرًا

للذكاء، يمكن استخدامها للتعرف على الأشخاص أو يمكن استخدامها لتحديد فعل يشترك فيه الأشخاص، مثل زيارة المواقع الإلكترونية.

لكن دعونا لا نركز فقط على المواقع الإلكترونية التي يستخدم من أجلها الـ DNS. كل خدمة أخرى كذلك. لذا فهي أحد العوامل المحفزة حيث IETF – لست أتحدث عنهم، لكنهم نشروا وثائق عن هذا الأمر – أعلنت مراقبة واسعة النطاق كتهديد سيتم تلافيه من خلال اثنين من البروتوكولات، وتعالج تلك المحاولات بالفعل تلك المشكلة من خلال الاستجابة إلى المراقبة واسعة النطاق بتشفير واسع الانتشار.

لذا فهذا يتعلق بتشفير حركة الـ DNS بشكل موجز. للأمر جوانب أخرى من الناحية الفنية وسنتطرق إليها لاحقًا، لكن للإضافة فقط، ليس فقط الجهات الفاعلة الحكومية التي تفعل ذلك، إنها أيضًا قطع أخرى من الأحجية التي قد يكون لها مصلحة في البحث في حركة الـ DNS ذهابًا وإيابًا، لأن بينما معلومات الـ DNS في الغالب تكون عامة، إلا أن حقيقة أن شخصًا ما يطلب اسمًا معينًا في وقت معين، من المرجح جدًا ألا تكون معلومات عامة وهي معلومات قيمة.

لدينا هؤلاء المعيارين المتنافسين وهذا سهل الوصف. إنها تصف فقط كيف يتواصل الجزء الأول، المحلل، مع الجزء الأخر، الذي هو في هذه الحالة ما يسمى محلل DoH. يبدو وكأنه خادم على الإنترنت من الخارج، لكن بدلًا من توصيل المواقع الإلكترونية، يقوم بتوصيل استجابات الـ DNS.

ما لا يتم حله إلى الآن هو كيف للمستخدم وكيف لمتصفح الإنترنت في تلك الحالة أن يحصل على المعلومات، وممن يطلبها؟ عادة، هذه معلومات يتم تقديمها من قبل نظام التشغيل في تلك الحالات حيث لدينا هذا الأمر، وهذا هو الحال بالنسبة لمعظم أجهزة الحاسوب المحمولة والهواتف الذكية التي تستخدمها. هناك عملية تشغيل هناك وتحليل الاسم كامن بعمق في نظام التشغيل، وعادة ما يتم ذلك اليوم بشكل متسق مع الصندوق بأكمله الذي في يدك أو أمامك على الطاولة.

وهذه الأشياء قد تكون على وشك التغير. لذا فإن فريق مهام هندسة الإنترنت أو المطورين لا يزالون يعملون على التكوين الآلي وكيفية إيجاد محلل DoH هذا وهناك مبادرات

جارية أيضًا لمنح المستخدمين خيارات أكثر ولتمكينهم من تكوين خدمة DNS يدويًا، لكن هذا لا يزال في طور التكوين.

لذا كان هناك بالفعل متصفح إنترنت ومزود لمتصفح الإنترنت الخاص بهم قام بتمكين DoH، وهو DNS عبر HTTP، ويعامل تحليل اسم DNS بطريقة مشابهة قليلًا بالشبكة الإلكترونية ويشمل هذا ترميزًا صعبًا لـ URL – هذا هو المُعرِف، العنوان الإلكتروني الذي نأمل أن تعرفه من متصفح الإنترنت الخاص بك عند زيارتك لصفحات الإنترنت – ولتصحيح تلك المعلومات لـ DoH. لذا، جميع متصفحات الإنترنت من ذلك المزود في تلك النقطة من الزمن ستستخدم محلل DoH مخصوص. مرة أخرى، لن يكون هناك مثيل واحد، سيكون هناك Anycast وكل شيء.

وهذا من شأنه أن يتجاوز المعلومات التي يقدمها نظام التشغيل. لذلك سيختار التطبيق الآن استخدام مسار تحليل DNS مختلف عما يفعله بقية نظام التشغيل. قد يواجه ذلك بعض التحديات، وكما هو مبين على الشرائح، يمكن أن يتداخل مع سياسات أمان بعض مديري الشبكات حيث يحاول الأشخاص تخفيف الوصول إلى معلومات معينة، معظمها من مواقع الإنترنت أو مواقع التصيد الاحتيالي، كما تسمونها، عن طريق اعتراض حركة DNS، وهذا لن، كما اقترح شخص ما بالفعل، يعد يعمل. الشريحة التالية من فضلك.

ومن ثم بالطبع، السؤال الشيق، لماذا هناك اثنين من المعايير؟ أحاول ألا أخوض في التفاصيل الفنية، لكن DNSO – DoT عبر TLS وعبر أمن النقل، هو نوع ربما مشابه أكثر بالهندسة حيث نعتقد أن الشبكة في طبقات وغير ذلك، لكن بها على الأقل مشكلة واحدة أنك تريد معلومات معينة، ثقب آخر في أسوار الحماية الخاص بك، للوصول إلى هذه المعلومات، في حين أن الجميع يسمح للجميع بالدخول لأي خادم على الإنترنت هذه الأيام.

لذا فإن حركة DoH تبدو أكثر أو أقل مثل الوصول للمواقع الإلكترونية ولا يمكن عزلها عن ذلك، كما هو مبين على شريحة قادمة. أو على هذه الشريحة في الواقع. عذراً.

لذلك، لا أحد يستطيع حجب الوصول لخدمة تحليل الأسماء المبنية على DoH هذه دون حجب الوصول إلى خوادم مهمة على الإنترنت في الوقت نفسه. هذه هي الحيلة وراءها، إذا جاز التعبير.

ولا يزال البحث جارٍ لإضافة هذه الميزة إلى DNS عبر TLS مثل نهج DoT. بالطبع، من الناحية الفنية، هناك بعض التفاصيل الرائعة، لكنها ليست جزءًا من الموضوع لهذا اليوم.

نتيجةً لذلك، لم يعد بمقدور مديري الشبكات حظر تحليل الأسماء، لأنهم في الوقت نفسه، من المحتمل أن يمنعوا الوصول إلى مواقع الإنترنت، أو إلى محركات البحث الشائعة في هذا الشأن. هذا يمكن – ربما وربما لا – أن يتداخل مع بعض المتطلبات التنظيمية في بعض الاختصاصات التي يطلب فيها من مزودي خدمة الإنترنت أن يحجبوا تحليل أسماء نطاقات معينة وعندما أقرأ ذلك، أنا لا أقول إن آليات الحجب هذه فعالة للغاية، لكنها قد تكون متطلبات تنظيمية مع ذلك. وكما قلت، لا يمكن لهذا الأمر أن يكون ممتازًا لأنه يمكن التحايل عليه بسهولة من خلال تكوين محلل خاص بك أو استخدام VPN أو تشغيل محلل خاص بك على نظامك الخاص.

[يتخفى] قد تساعد استعلامات DNS في دفق حركة الإنترنت قد يساعد المستخدمين على الالتفاف على التصفية المستندة إلى DNS، ويمكنك تسمية هذه بالرقابة، وذلك عندما يتم فرض التصفية على المستخدم من قبل جهة خارجية، أو قد يحظر البرامج الضارة، وهو عادة شيء يشترك فيه المستخدم أو يزعم أنه تم تنفيذه لصالح المستخدم. الشريحة التالية من فضلك.

إذاً قليلاً من الصورة الأكبر، لأنه مرة أخرى، البروتوكول [بريء]، ولكن بعد ذلك تحدث أشياء غريبة. لا يحدد DNS عبر HTTP نموذجًا محددًا للنشر. يمكن لأي مشروع أن يستخدم محلل DoH وتوجيه متصفحات الإنترنت الخاصة بهم على ذلك، ومن ثم التصرف كما سبق. ومع ذلك، في المناقشة التي تمت حتى الآن، يمكننا أن نلاحظ وجود نموذج تطوير معين يميل حقًا نحو التركيز والتوحيد، كما هو الحال في مزودي متصفحات الإنترنت الذين يتعاونون مع مزودي تحليل DNS - وسأشير إلى ذلك في

البند التالي - ثم أشير إلى جميع عملاء متصفحات الإنترنت الخاصة بهم، ومستخدمي الإنترنت إلى خدمات التحليل الخاصة بمزود معين والتي توفر للمزود الكثير من الرؤية التي تمنح المستخدمين أيضًا قدراً من الاستقرار، ولكنها تعزز التركيز.

إن تحليل اسم DNS، على مدى السنوات الثلاثين الماضية، اعتاد بشكل تقليدي على أن يكون لامركزي للغاية. بمعنى آخر، في مزودي خدمة الإنترنت حتى على الحاسوب المحمول الخاص بك، أو تفكير ما قبل 30 عامًا على المركزية الخاصة بك، أو سمها ما شئت. ومع ذلك، فقد تطور تحليل اسم DNS كخدمة مع مرور الوقت، وهذا ما يسمى المعرّف الرباعي، مثل 1.1.1.1، و8.8.8.8، وربما رأيت ذلك على صورة مرسومة على حائط في بعض البلدان التي واجه الأشخاص فيها حظر DNS ثم تحايلوا على ذلك من خلال الانتقال إلى أحد مزودي التحليل هؤلاء. وهناك آخرون يستخدمون الشكل نفسه في كل موقف. إنها مجرد مسألة فضول وسهولة في الاستخدام.

لكن هذه الجوانب بالإضافة إلى اختيار مسار التحليل لكل تطبيق بدلاً من كل نظام، أو لكل مشروع، أو حتى لكل مزود لخدمة الإنترنت حيث يقوم مزود خدمة الإنترنت بتوفير اختيار التحليل لعملائهم، مما يؤدي بالتأكيد إلى زيادة تركيز المحللات التي يزداد حجمها. بمعنى كبير، فإننا نعني أن عدد السكان وراء هذا المحلل ينمو وينمو، مما يعني أنه من الواضح أن الوزن - وهذا قد يعني أيضًا وزن السياسة - لمشغل المحلل المحدد هذا يمكن توقع زيادته ويصبح أكثر أهمية. الشريحة التالية من فضلك.

حسناً. كما قلنا، توفر كل من DoH وDoT الخصوصية على [السلك] وتحدثنا عن الأسباب. ومع ذلك، فإن المُحلِلات - التي هي إما المُحلِّل لدى مزود خدمة الإنترنت أو المُحلِلات التي توفرها هذه خدمات التحليل الكبيرة - ترى طلبات المستخدمين على مستوى مختلف من التفاصيل.

لسبب ما، في بعض الأحيان يتم إضافة معلومات معينة إلى السؤال حتى يتمكن المستخدمون من الحصول على استجابات مخصصة، لأنه في البند الأخير - سأقوم بإعادة التوجيه هنا لثانية - تعتمد بعض السيناريوهات الفنية على حقيقة أن الجميع لا يحصلون على الاستجابة نفسها عند طرح السؤال نفسه، تستخدم شبكات توصيل المحتوى

المزعومة الـ DNS في كثير من الأحيان لتوجيه المستخدمين إلى أقرب نظام نقل محتوى لخفض زمن الوصول وإعطاء المستخدمين استجابات أسرع.

لذلك لا يتم التعامل مع الخصوصية فقط من خلال التشفير على السلك، ولكن أيضًا من خلال سياسة محلل DNS، كما هو الحال في مشغل التحليل الذي يخبرك أو يعدك بالمسؤولية أو أيًا كان، ماذا يحدث لبيانات الاستعلام التي [ترى ذلك.] ربما تكون قد تحايلت على مزود خدمة الإنترنت أو ممثل الدولة كشخص مهتم ببياناتك، ولكن على الأرجح لن يساعدك كثيرًا إذا كان مشغل الحلول قد دخل.الشريحة التالية.

لا تعمل. لذا فيما يتعلق بسؤال الخصوصية لمحللات DoH، يوجد أشياء شيقة لمناقشتها ومفتوحة للنقاش، كيف يجب اختيارها؟ شاهدنا ذلك على شريحة سابقة، ما هي الوسائل الفنية، كيف لي كمستخدم أن أقرر ما استخدمه وإذا حددت واحدًا، كيف لي أن أكونه إلى التطبيق الخاص بي أو نظامي أو ماذا؟ كيف يكون مشغلي محللات DoH تلك مسؤولين عما يعدون وما يفعلون؟ لأنه مجددًا، قد يلزم لهم كشف معلومات بموجب طلب أي جهة كانت، في معظم الحالات جهات تطبيق القانون.

ومن الذي يحدد السياسات المقبولة - وهي مناقشة أخرى يقول أحد المزودين "حسنا، نحن نفهم أن هناك مخاوف في المجتمع من وجود مزود واحد نتعاون معه. قد نكون منفتحين للتعاون مع المزودين الآخرين، لكننا نود منهم الالتزام بسياسات معينة للحل، وهذا يعني أنهم يفعلون ولا يفعلون أشياء معينة مع بيانات المستخدم." الشريحة التالية من فضلك.

إذًا، حتى الصورة الأكبر، لأن أحد الأسئلة بالطبع ستكون، لماذا نتحدث عن هذا في ICANN؟ الآن، افترض مجموعة من مقدمي حل DOH المتعاونين. ستكون المجموعة صغيرة، غير منتشرة كما كانت في الأيام الأولى. ونفترض كذلك أن هناك تطبيقًا معينًا، خدمة يتم استخدامها بشكل كبير على الإنترنت، مثل الشبكة الإلكترونية، كما نفعل جميعًا.

وهناك في بعض الأحيان مصلحة في مسار تحليل اسم إضافي. وكان هناك نقاش في فريق مهام هندسة الإنترنت، وكذلك ICANN، حول نطاق المستوى الأعلى dot-onion

التي ليست بالفعل TLD لكنها محفوظة الآن. لكنه مسار تحليل مختلف مطلوب لشيء يتناسب بطريقة أو بأخرى مع العالم المجرد.

من الناحية العملية، عندما يكون لدينا هذه المجموعة من مقدمي تحليل التعاون - ولديهم عدد كبير من الأشخاص خلفهم - من سيكون في وضع يسمح له حقًا بتحديد ما إذا كان سيتم فتح شرائح جديدة من العالم المجرد أم لا؟ كيف سيبدو ذلك، وما الذي يعنيه دور ICANN فيما يتعلق بمنطقة جذر DNS عندما يكون هناك تحول في الطاقة، أو تحول في - ما، ببساطة يصوت الأشخاص بأقدامهم أو متصفحات الإنترنت الخاصة بهم. الشريحة التالية رجاءً، وينبغي أن تكون هي.

حسنًا، الاستنتاجات. الاستنتاجات الأولية، على الأرجح. لقد تعلمنا أن بعض عمليات نشر DOH و DOT قد تؤثر على نقاط التحكم التقليدية في التحليل. ومزودي خدمة الإنترنت ويمكن للمشروع أن يعترض استعلامات DNS ويرسل استجابات مختلفة. لتقديم الإعلانات، ولكن أيضًا للتخفيف من البرامج الضارة وبرامج الروبوتات.

لا تزال عملية توحيد محللات DoH وDoT في التطبيق وكيفية اختيارهم جارية. لا يوجد استنتاج نهائي. بالنسبة لمشغلي السجل والمسجل، يبدو حاليًا أن هناك تأثير ضئيل. ومع ذلك، مرة أخرى، يمكن أن يكون هناك شخص يطرق باب المسجل أو السجل ويقول: "أنا واحد من مزودي التحليل هؤلاء. لمَ لا تعطيني نسخة من بيانات DNS الخاصة بك؟ سأكون سعيدًا بتوصيلها لمستخدميك بسرعة أكبر."

ومن المبكر للغاية بالطبع أن نحدد الأثر الذي سيكون على المستخدمين. وكما سمعنا بالفعل، هذا متعامد تمامًا مع DNSSEC وآليات الخصوصية الأخرى مثل تقليص تقنية QNAME. ولم تتغير الحاجة لهؤلاء. ينبغي أن تكون هي. الشريحة التالية من فضلك. حسناً.

أليجاندرا رينوسو: شكرًا جزيلاً لك، بيتر.

بيتر كوتش: شكراً.

أليجاندرا رينوسو: هل هناك أية أسئلة من الجمهور؟ لدينا وقت لأخذ سؤالين. معنا رقم خمسة.

وارن كوماري: مرحباً. وارين كوماري، أعمل لصالح شركة غوغل. لست ضمن فريق متصفح كروم، لكني أقوم بنقل بعض الأشياء منها. حسنًا، بيتر في عرضك التقديمي، قدمت نوعًا واحدًا من نماذج النشر من قبل واحد من المتصفحات. هذا ليس نموذج النشر الوحيد. ما يخطط له كروم لفعله هو أنه سيعرض DoH لمستخدميه بوسيلتين.

إذا كان محلل نظام المستخدم يدعم DoH بالفعل، سيتم ترقية كروم ليستخدم ذلك. إذا كنت تستخدم محللات مزود خدمة الإنترنت الخاص بك بالفعل، وتبين أنهم يدعمون DoH، فسيقوم بعمل DoH عبر أولئك.

إذا أراد المستخدمين، يمكنهم اختيار محلل آخر. هذا هو ذات الشيء الذي يحدث بالفعل حاليًا. إذا لم يكن المستخدمين راضون بمحللات مزود الإنترنت الخاص بهم، يمكنهم اختيار واحد مختلف.

مهما كانت الحالة، لن يقوم كروم بتغيير ما يختاره المستخدمون دون اختيارهم لذلك. ونحن أيضًا لا نطلب أن يقوم المستخدمين باختيار شيء مثل DNS العامة الخاصة بغوغل.

كل ما يعنيه هذا هو الحمايات الموجودة التي يمتلكها الأشخاص لأشياء مثل البرامج الخبيثة، إذا قاموا بـ DNS من نوع المشروع، جميع أنواع الأشياء تلك تستمر في العمل بالطريقة نفسها.

لذا، أعتقد أن النوع الذي يستحق الإدراك هو الطريقة التي ينتشر بها هذا الأمر وهو ما يهم، وليس ماهية النقل نفسها. لست متأكدًا إذا كان لديكم أي فكرة عن هذا الأمر.

بيتر كوتش: أجل. شكرًا لك، وارن. لم يكن لدينا عمدًا أسماء على الشرائح، وآمل أنني لم أذكر أيًا منها. لذا شكرا لك على القيام بذلك في هذه الحالة بالذات. ونعم، إنها إضافة قيمة إلى سيناريو نموذج عمليات النشر. لم نسعى جاهدين إلى أن نكون مستفيدين، وأعتقد أن الشريحة أوضحت أن نماذج متعددة تتم مناقشتها، والنموذج الذي أظهرته بوضوح هو جزء منهم.

بالنسبة للجزء الآخر، أود أن أرجع إلى الفريق في وقت لاحق لعدم استباق تلك المناقشة، وربما يمكننا التركيز على أسئلة فورية حول أشياء أوضحتها بطريقة غير مفهومة.

أليجاندرا رينوسو: شكرا لك، بيتر. لدينا مشارك واحد عن بعد، وبعد ذلك سننتقل لرقم ثلاثة وسأنتقل لرقم أربعة، وبهذا سنختم قائمة الانتظار لهذا الجزء.

آرييل ليانج: هناك سؤال من ديرك جامبيرتز. يتم بالفعل إساءة استخدام DoH باعتبارها متجهًا للهجوم لإدراج محتوى ضار في صفحات الإنترنت من خلال استخدام سجلات [TXT] معدّة. هل أنتم على علم بهذا؟ من الصعب للغاية حجب هذا الأمر لأنه يستخدم قناة موثوقة للهجوم [على THHP] كما هو مقترن مع DNS.

ألا يجعل هذا من DoH تهديدًا وليس نعمة؟

بيتر كوتش: هذه معلومات مثيرة للاهتمام يا ديرك. أنا شخصياً لم أكن أعرف ذلك. ربما باقي الفريق كذلك. أود أن أحيل هذا السؤال إلى جلسة المناقشة، وربما يمكننا وضع ذلك في الاعتبار.

أليجاندرا رينوسو: سنفعل، رقم ثلاثة؟

إدواردو دياز: لدي سؤال. هناك مشكلة محتملة للمستخدم أنه إذا قمت بتنزيل أحد التطبيقات، وكان هذا التطبيق من خلال [تنزيله] يستخدم أدوات حل خاصة به دون أن أعرف ذلك، لذلك فقد يؤثر بشكل كبير على المستخدم بسهولة دون معرفة ما يحدث في الخلفية. شكراً.

بيتر كوتش: نعم. شكرًا لك على هذه الملاحظة. أحد الجوانب التي لم يتم ذكرها هو أنه من الناحية النظرية - وكما تعلمنا، تصبح النظرية على الفور ممارسة - يمكن لتطبيقات مختلفة أن تقدم نتائج مختلفة، بحيث يبدو نظام اسم النطاق مختلفًا عن متصفح الإنترنت، أو لتطبيق البريد مثلاً أو لهاتف VOIP الخاص بك، لأنه بناءً على مسار التحليل الذي تختاره، قد يتم حظر بعض النطاقات وتوجيه الآخرين، أو حتى قد يتم إرسالك إلى النقطة أ هناك وإلى النقطة ب في مكان آخر. بحيث يمكن أن يكون حقا تجربة للمستخدم. ولكن هذه هي البداية لكيفية توقع المستخدم النهائي فعليًا. شكراً.

أليجاندرا رينوسو: شكراً. الرقم الرابع.

[ريمي نويكي:] شكراً. اسمي [نويك ريمي]. أنا من نيجيريا ممثلًا عن NCUC، دائرة المستخدمين غير التجاريين. إن اهتمامي يتركز على واحدة من النقاط على الشريحة، إنه من المبكر جدًا معرفة ما هي آثار DoH وDoT على المستخدم، لكن على الأقل يمكننا الاستمرار في المحاولة والنظر في التأثير المحتمل، التأثير السلبي الذي قد يصيب المستخدمين.

وأمر آخر أود أن نوضحه وهو ما هي التدابير المضادة التي يمكن أن نستخدمها في مقابل هذه الآثار السلبية الخاصة بـ DoH وDoT وكذلك ما هي مسؤولية المستخدم وتأثير التكلفة ليس على الجانب الفني الآن لكن على المستخدم. شكراً.

بيتر كوتش: حسناً. أعتقد أن هذه مساهمة أكثر من كونها سؤالًا عاجلًا مما يمكن أن يساعد في المناقشة. لدينا اثنين من الشرائح أيضًا قبل أن تفتح اللجنة. إذن لا أرى أية أسئلة أخرى.

أليجاندرا رينوسو: الآن، سننتقل إلى اللجنة. حسنًا، من مرر اثنين من الشرائح. شكرًا جزيلاً. الآن سيرد الأعضاء على هذه الأسئلة التي ترونها أمامكم. سأقرأهم جميعًا.

هل تتوقعون أي تأثير من نشر DoH وDoT، أحدهما أو كلاهما، في عملياتكم؟

هل هناك مشكلات مع DoH/DoT تقع ضمن مهمة ICANN؟

كيف ينبغي تطبيق DoH في تطبيقات مثل متصفح الإنترنت من وجهة نظركم؟

ما المخاوف التي تساوركم حول DoH وDoT؟

حسنًا، سنبدأ مع تيم.

تيم أبريل: التطرق لكل تلك الأسئلة سيستغرق منا وقتًا طويلًا جدًا، لكن ما يعلق بذهني كثيرًا، من منطلق الخلفية الأمنية، هو ما هي المخاوف التي تساورني حول DoH وDoT وهذا في الأغلب ينطبق على المستخدم النهائي وكيف يمكن أن تتغير نظرتهم إلى العالم المجرد.

في الأساس إذا كان الميل الأول من المتصفح أو التطبيق من خلال محلل يستخدم DoH أوDoT، فإنك تحصل على خصوصية القناة هناك، ولكن ليس لديك بالضرورة ما يضمن أن الاتصالات التي تنتقل من هذا المحلل إلى السلطات لديها أي نوع من الحماية على الإطلاق.

لذا فإنك إذا كنت قلقًا بشأن تسرب البيانات من خلال قناة الاتصال، فهذا قد يحدث وراء المحلل وفي بعض الحالات قد يكون ذلك متعلق بالمستخدم النهائي أيضًا.

هناك أيضًا مشكلة التصحيح إذا كنت تستخدم – وهذا يعتمد على تنفيذ – بالتحديد في DoH، إذا كان التطبيق الخاص بك يستخدم محلل DoH دون معرفة، قد تسبب بعض مشكلات التحليل لمحلل مزود خدمة الإنترنت لديك وستتصل بمزود خدمة الإنترنت الخاص بك، ولن يكون لديهم فكرة عما يجري، وهذه ستكون مشكلة تصحيح طويلة وهي مبهمة للمستخدم النهائي إلا إذا كان لديهم خلفية فنية قوية ويعلمون ما ينبغي البحث عنه.

سأدع الأخرين يستمرون.

أليجاندرا رينوسو: حسناً. فيتوريو؟ لو أمكن.

فيتوريو بيرتولا: أظن أن لدي الكثير لأقوله. بداية من السؤال الأول، بصفتي مورد برامج ومزود لخدمة DNS لبعض أكبر مزودي خدمة الإنترنت بالطبع، لدينا تأثير يتعلق بتنفيذ البروتوكول الجديد وجعله يعمل في العالم الحقيقي، في [منصات تخدم العديد] من ملايين استعلامات DNS في كل ثانية، لكن هذه ليست المشكلة الحقيقية.

نحن بصفتنا شركات برامج وشركة مفتوحة المصدر نهتم بشكل أكبر بمشكلة انفتاح الإنترنت والتأثير الذي قد يحتوي عليه هذا في شكل سوق تحليل DNS والخدمة بوجه عام.

لذا أعتقد أن المشكلة الحقيقية هنا لا تتعلق بالتشفير، لذلك فهي لا تتعلق بالنقل من خلال اتصال مشفر، الأمر الذي يعتبر جيدًا بالنسبة للخصوصية. إن الحركة المضافة لـ DNS وتغييرها من خدمة شبكية، وهو شيء يتم تقديمه كجزء من الخدمة الشبكية من قبل نظام التشغيل الخاص بك، مثل حزمة بروتوكولات الإنترنت (TCP IP)، إلى خدمة تطبيق، وهو شيء يتم التحكم فيه مباشرة من قبل كل تطبيق.

هذا يفتح الطريق لعدد من المشكلات. جزء منهم يتعلق بالالتباس المحتمل كما كنا نقول، تطبيقات مختلفة تعمل بطرق مختلفة. لكن أكثر ما يهم هو ما يتعلق بحقيقة أن سوق

التطبيقات، بالأخص إذا تطرقنا للشبكة الإلكترونية، وهو التطبيق الأكثر استخدامًا على نطاق واسع، وهو أكثر تركيزًا من سوق الشبكات.

حاليًا، إذا كنت ترغب في تجميع 95% من استعلامات DNS في العالم، فيجب عليك تجميع أفضل 1000 محلل DNS. في الشبكة الإلكترونية، يتعلق هذا بالشركات فقط في الأساس. جميعهم، بالمناسبة، في الاختصاص ذاته في الدولة نفسها.

لذا من حيث التأثير المحتمل على الخصوصية، فيما يتعلق بالاختصاص على وجه الخصوص، السيادة وكل هذه القضايا، يتغير هذا كثيرًا، لأننا نعلم جميعًا أنه بالنسبة للحكومات، أعتقد أن العديد من الدوائر الانتخابية تتأثر. أحدها هو مزودي خدمة الإنترنت، لكن في هذا السياق، لعل هذا [يستحق] الحديث عن الحكومات والمستخدمين النهائيين.

بالنسبة للحكومات، التأثير، المشكلة في الواقع تتعلق بفقد السيطرة على محلل DNS، وبالأخص للدول التي قررت استخدام إما أن توفر خدمات إضافية مثل الرقابة الأبوية أو أيضًا أن تطبق أي نوع من رقابة المحتوى والتصفية تجاه ما يمكن لمواطنيهم رؤيته.

في النهاية، ما يحدث هو أن متصفحات الشبكة الإلكترونية يمكنها أن تبدأ فقط في استخدام تلك المنصات العالمية، وهذا كله سيذهب بعيدًا والتحكم بأكمله سيتغير لمكان ما آخر لن يكون ضمن نطاق البلد. لهذا على الأقل الحكومة البريطانية أولت بعض الاهتمام، وأتوقع أن العديد من الحكومات ستقوم بهذا أيضًا.

وبالنسبة للمستخدمين، هذه مشكلة محتملة تتعلق بالاختيار، لأنه إذا بدأ التطبيق في تقرير – إما أن يرسل استعلامات DNS فقط إلى أيًا كان الطرف الذي يريدونه، ولكن أيضًا حتى الحد من اختيار القول "نحن الآن [غير مسموع] الأشخاص الذين يقررون من يستطيع تشغيل محلل، ويوجد فقط قائمة تحتوي على 10 محللات اعتمدناها عالميًا، ولن نسمح بأي شيء آخر."

ثم يصبحون حراس بوابة ويقررون سياسات تحليل DNS. لذا في النهاية، يعتمد هذا على السياسة، لذا فإن الرسالة الأخيرة التي أرغب في تركها هي أن هذا حقًا يعتمد على

نموذج النشر، لكن لنتفق على نموذج نشر هناك حاجة إلى بعض السياسات المشتركة، إما تصاعدية أو أن أشخاص التطبيقات لن يذهبوا ويفعلوا ما يرغبون فيه، لكن هناك فهم مشترك لما سوف يحدث.

أليجاندرا رينوسو: شكرًا لك، فيتوريو. ميشيل؟

ميشيل نيلون: شكراً. أعتقد أن الأسئلة التي نبحث فيها هنا ليست بسيطة. إنهم من نوع الأسئلة التي يحبها الجميع، الأسئلة الصعبة. وأعتقد ان بعضًا من هذه الأشياء أكاديمي ونظري إلى حد ما، بينما في الوقت الراهن، إنها أيام مبكرة جدًا. DoH وDoT حتى الآن كانت افتراضية. وهم يصبحون واقعًا الآن.

وما هو ذلك الواقع؟ كيف سيؤثر هذا علينا؟ السؤال الثاني. يمكن أن تتأثر مهمة ICANN ببعض الطرق مع هذا الأمر إذا انتهى بكم الأمر في موضع لن تظل فيه المعرفات العامة عامة. أنتم الآن ينتهي بكم الامر باحتمالية في موضع فيه عدد أقل بكثير من مشغلي تحليل DNS تقرر الآن ما هو الموجود في DNS وما يستطيع الأشخاص الوصول إليه، وما الذي يمكنهم الوصول إليه. لذلك، أعتقد أن هذا له بعض التأثيرات المحتملة.

شركتي الخاصة من مزودي الاستضافة وشركة سجل ونقدم أيضًا خدمات الإنترنت. الناس لا تفهم ما هو اسم النطاق. لا يفهمون الاختلاف بين اسم النطاق والمتصفح، ولا يفهمون الاختلاف بين محرك البحث وشريط العنوان في المتصفح.

لذلك عندما يقول أحدهم "أجل، يمكن للمستخدم أن يختار أن يغير الخدمة التي يستخدمها لهذا الأمر" يمكن أن يكون هذا صحيح إذا كنت تتحدث إلى مجموعة من المهووسين المتشددين. كم عدد الأشخاص في هذه الغرفة يستخدمون خادم الاسم الخاص بهم؟ حسناً. وأنظر في أرجاء الغرفة وأعلم أن هؤلاء جميعهم من المهووسين المتشددين.

كم منكم يستخدم خادم البريد الخاص به؟ إنها المجموعة نفسها على الأغلب، بالمناسبة. الآن، هل سيقول أي منكم بصدق، يداً بيد، أنه مستخدم إنترنت تقليدي؟ حسناً.

هذا هو الأمر. من المحتمل أن تقول إن هناك اختيار ليس صحيحًا تمامًا. وفي نهاية المطاف، نوع السياسة والجوانب الفنية لذلك، يفتح صندوق البندورا في بعض النواحي. لكن لماذا وصلنا إلى هنا؟ إذا عدتم للخلف للعرض التقديمي الذي قدمه داني ونظرتم للمقارنات بين التقنيات المختلفة، فإن السؤال الذي ينبغي طرحه هو لماذا حدث هذا؟ كيف ومن أين أتى هذا؟

والواقع أن العالم الذي نعيش فيه الآن، السياسة والخصوصية تعتبر أشياءً يقلق بشأنها الناس. وإذا لم تكن قلقًا بشأن السياسة والأمن، فأين كنت في السنوات القليلة الماضية؟ لقد كان الـ DNS عامة للغاية في نواحي عديدة. إن به مجموعة من المشكلات المشوقة.

لذا الآن لدينا مسارًا محتملًا لإصلاح بعض تلك المشكلات، مما يفتح مجموعة من المشكلات التي ستبقي على البعض منا في وظائفهم بالطبع لبقية حياتنا.

من منظور تشغيلي، لست متأكدًا من كيف سأشرح لبعض عملائي لماذا لا تعمل أشياء معينة، لأنها سيئة بما فيه الكفاية عندما يحيطون بك ويخبرونك بأنهم يواجهون مشكلات مع Outlook عندما لا يستخدمون Outlook بالفعل لأنهم يعتقدون أن Outlook هو عميل البريد الإلكتروني الوحيد أو أن Firefox هو المتصفح الوحيد.

لذلك، أعتقد أن هناك بعض المشكلات التشغيلية المثيرة للاهتمام التي سيتعين علينا التعامل معها، وإذا نظرت إلى ما سيحدث خلال الأشهر القليلة المقبلة حيث أصبح هذا متاحًا في مجموعة صغيرة من المتصفحات والتطبيقات المحتملة الأخرى، فسيكون لديك هذه المخاوف الأمنية، سيكون لديك - الناس بالفعل يجدون طرق جديدة ومثيرة للاهتمام لاستغلال التكنولوجيا الجديدة. إنهم يستخدمون سجلات من نوع TXT في DNS لنشر البرامج الضارة. لقد رأيت عرضًا تقديميًا لهذا الأمر منذ أسبوعين وكنت " هذا أمر مخيف بشكل لا يصدق، ولكن لماذا لم أفكر في هذا؟" أعتذر، أنا فقط أمزح.

لكن أعتقد أن هذا أمر علينا النظر فيه عن كثب. أنا شخصيًا لدي العديد من المخاوف حول فكرة تسليم تلك السيطرة، ذلك القرار. أنظر إليها من حيث شبكة مكتبي الخاص، هل سنكون قادرين على حماية أشيائنا الخاصة من البرامج الضارة وأنواع الهجمات المتعددة الأخرى؟ هل لدينا التقنية التي تمكننا من فعل هذا؟

وأشتبه أن الإجابة هي لا، لكن هل هذا شيء سيء بشكل أساسي؟ أعتقد أن الإجابة هي لا، لكنه سيتطور.

أليجاندرا رينوسو: شكرًا جزيلا ميشيل. والآن مرة أخرى الساحة مفتوحة لطرح الأسئلة على الخبراء. معنا رقم ستة، ورقم خمسة من بعده. حسنًا، من فضلك رقم ستة.

ميلتون مولر: مرحبًا. كلمتي "التوحيد والتركيز" تظهران في العديد من مناقشات DoH. ليست DoT حقًا بقدر ما أفهم. لكن شخصًا يتعامل مع التحليل الاقتصادي، هذه الكلمات لها معانٍ محددة جدًا. التركيز والتوحيد سيئين لأنهم قد ينقلون قوة الاحتكار وقوة التسعير للمورد.

وجهة نظري أن معظم خدمات DNS هذه التي يستخدمها الناس ليست مركزة بل موزعة وهم لا يدفعون لها على الإطلاق، أليس كذلك؟ وقلقي أن هذا التركيز سيؤدي إلى بعض أشكال احتكار التسعير لخدمات DNS أم هناك بعض المخاوف الأخرى؟ هل بإمكانكم التحديد بدقة أكبر ما هي المخاوف وكيف سيتأثر السوق العام لخدمات الإنترنت؟

أليجاندرا رينوسو: هل من أحد؟

فيتوريو بيرتولا: لا أعتقد أن أنها مخاوف تتعلق بالتسعير، لأن اليوم، تحصل على DNS الخاص بك من مزود خدمة الإنترنت الخاص بك وهو جزء من خدمة الوصول إلى الإنترنت. إن الأمر يتعلق أكثر بمعلومات التركيز والتحكم.

على سبيل المثال، هذا بروتوكول من قبل [غير مسموع] تعزيز الخصوصية، لكن إذا كان في النهاية 60% من العالم يستخدم المحلل نفسه، أجل، هذا المحلل سيحتاج إلى رؤية معلومات المتصفح [غير مسموع] من نسبة 60% من العالم، لذا من المحتمل أن تكون هناك خسارة كبيرة للخصوصية في النهاية.

أليجاندرا رينوسو: ميشيل؟

ميشيل نيلون: شكراً. أعتقد أن ميلتون، كما يقول فيتوريو، ليس له علاقة بالتسعير، إنه يتصل بنسبة كبيرة بأن الإنترنت يعمل لأنه مُقسَم. إنها شبكة تضم شبكات. يمكن لكل مزودي خدمة الإنترنت أن يقوموا بتنصيب المحللات الخاصة بهم، كل شبكة، يمكننا جميعًا أن نمتلك المحللات الخاصة بنا لهذا الأمر.إذا قمتم بتركيزه، فستفقدون ذلك الاستقرار وتلك المرونة. هناك احتمالية لتلك المرونة أن تُفقد.

وكذلك هناك مشكلة أن هناك كمية هائلة من البيانات في حركة الـ DNS، ليس ما هو موجود هناك بل وغير الموجود أيضًا. لذلك، فإن ما يحاول الناس الوصول إليه ليس موجودًا في الحقيقة. هذا يستحق الكثير من المال.

أليجاندرا رينوسو: شكرًا جزيلاً. الآن رقم خمسة.

شخص غير محدد: هناك لبس يحتاج إلى التوضيح، وهو أنه عندما تتحدث عن DNS في مستوى المتصفح، الذي هو مستوى المستخدم، ومن الذي يطبق السياسات إذًا؟ كيف نأتي بالوضوح في مستوى السياسة؟ هذا هو السؤال. أجل.

تيم أبريل: حسنًا، أعتقد أنك تسأل عمن يقوم بتفويض أو تحديد السياسة المستخدمة في المتصفح. هل هذا ما طرحتموه؟ هذا يرجع بشكل كامل إلى صانع المتصفح وأي من مستخدميه الذين يقدمون له التغذية الراجعة التي يختارون تنفيذها بالفعل. لا توجد آلية للسياسة لإجبارهم على فعل أي شيء. إنه البرنامج الخاص بهم، يمكنهم فعل ما يشاءون بشكل أساسي.

أليجاندرا رينوسو: شكراً. رقم ثلاثة.

إدواردو دياز: شكرًا جزيلاً. هل من الممكن أن أصبح شركة كبيرة بمحلل كبير، ومن ثم أستطيع البدء في البيع أو أعرض نطاقات المستوى الأعلى دون الرجوع إلى ICANN؟ ومن ثم يمكن للمحللات الأخرى أن تتواصل معي إذا لم يجدوا الجذر الخاص بهم، صحيح؟ هل يمكنكم القيام بذلك؟ هل من الممكن لهذا أن يحدث؟

تيم أبريل: إنه ممكن من الناحية الفنية. لا يوجد ما يمنع ذلك.

داني ماكفرسون: لا أعتقد أن DoH أو DoT تغير هذا على الإطلاق.

تيم أبريل: هذا مشابه جدًا لكيف قامت dot-onion.

أليجاندرا رينوسو: شكراً. الرقم الرابع.

فريد بيكر: الشيء الذي أجد نفسي قلقًا بشأنه هو توجيه الإنترنت. القضية التي أتحدث عنها على الأرجح مألوفة لديكم جدًا. إنها جهة قومية، لكنني سأحاول تجنب ذكر الاسم.

المشكلة هي أنه غالبًا ما تكون أيضًا مشكلة في المؤسسة. ستفرض الشركات نماذج أمن للمعلومات، وسيفعلون ذلك جزئيًا عن طريق منع الوصول إلى مجموعات معينة من الأسماء بطريقة أو بأخرى.

الآن، الجهة التي أفكر فيها، الناس في ذلك المكان اختاروا البدء في استخدام محلل غوغل، وتم التحايل في هذا الأمر، تم التحايل على هذه الخاصية من قبل الشركة المعنية باختطاف الوجهة إلى محلل غوغل.

وعندما يصبح الحل الأمني هو من يختطف الوجهات، فبصفتي شخصًا يستخدم الوجهات أقلق بشدة. سأكون مهتمًا بتعليقاتكم على هذا الأمر.

أليجاندرا رينوسو: داني؟

داني ماكفرسون: سأقول فقط، أجل، نظام التوجيه هو شبكة إلكترونية موثوقة، وطريقة عملها هو أنك تشير إليها على أنها توجيه عن طريق الشائعات، وتختار أن تصدق ما يخبرك به شخص ما وتروج له، أو لا، وليس هناك سلطة مركزية اليوم. هناك بعض الأساليب مثل البنية الأساسية لمورد المفتاح العام (RPKI) وأشياء أخرى، وعلى أي شخص يشغل أي خدمات حاسمة للبنية الأساسية أن يستخدم تلك الأساليب والأساليب الأخرى ليحمي نظام التوجيه

بشكل أفضل. لكنني أوافق، وأعتقد أن نظام التوجيه الأساسي ربما يعتبر واحد من المخاوف الأمنية الكبرى على الإنترنت اليوم بالتأكيد، وكل خدمة تكون مرتبطة بذلك حتى نزودها أكثر قليلًا.

تيم أبريل: وهناك أيضًا حالة - إنها فرصة عظيمة للقول إنه ينبغي على الأشخاص التفكير في استخدام DNSSEC و [دان] للقيام [غير مسموع] لأي من أدوات الحل التي يستخدمونها حتى عندما يكون الجهاز أو المحلل، أو أيًا كانت الأداة التي تقوم فعليًا بتقديم الطلب، بمحاولة الاتصال بالخادم، يمكنه التحقق من صحة شهادته من خلال DNS وباستخدام DNSSEC يتم التحقق فعليًا من أنه الخادم الذي يعتقد أنه يتصل به، حيث إذا كنت في منطقة لديها حق الوصول إلى مفتاح موثوق به من قبل [cert store]، ثم لا يمكنك الاعتماد على شهادة X.509 من خلال سلسلة الثقة، حيث إنه لا يمكنك الوثوق بها في تلك المرحلة.

أليجاندرا رينوسو: شكرًا جزيلاً. رقم ستة.

مارك سفانكاريك: فيما يتعلق بالأسئلة الموجهة إلى الجمهور، ما هي مخاوفكم، والقلق الذي يساور الكثير هو تركيز مزودي DNS. ولم لا يكون هذا هو السؤال هنا كمقابل لهذه البروتوكولات؟ في أكثر المتصفحات شعبية بشكل افتراضي – وهذا ما أفهمه أنه بشكل افتراضي – سينتقل إلى 8.8.8.8، فلديكم هذا التركيز الضخم بالفعل بغض النظر عن هذه البروتوكولات الجديدة. لم لا تكون هذه هي المشكلة التي تقلقنا كثيرًا؟ هذا ببساطة يسرع هذا الاتجاه.

لذلك سأفكر في أن يكون هذا أحد العناصر هنا بالإضافة إلى أسئلة البروتوكولات هذه. شكراً.

تيم أبريل: سوف أتغلب على وارن. وارن كان يقول إن متصفح كروم لن يختار 8.8.8.8 بشكل افتراضي. هذا هو الشيء الوحيد الذي يمكن اختياره. هناك متصفح آخر -

مارك سفانكاريك: [قال وارن أنه لـ DoH فقط.] [غير مسموع]

أليجاندرا رينوسو: من فضلك استخدم الميكروفون.

تيم أبريل: يمكن لوارن أن يصحح لي إذا -

مارك سفانكاريك: أعتذر إذا كنت أسأت تقديم وارن.

تيم أبريل: يمكن لوارن أن يصحح لي إذا كنت مخطئًا في هذا الأمر، لكنني أعتقد أن الطريقة التي يخطط بها كروم لتنفيذ هذا الأمر هي بشكل افتراضي إذا كان المحلل الخاص بك، كذلك محلل النظام الخاص بك، يقبل DoH، سوف يستخدم هذا كحزمة للتحليل. وإن لم يفعل، فسيعود إلى محلل النظام ومن ثم يستطيع المستخدم اختيار أن يستخدم DoH لأي محلل يختاره ويدعمه. لذا يمكنك اختيار 8.8.8.8. قد يكون خيارًا معدًا مسبقًا في القائمة المنسدلة ويمكنك اختياره، لكنه لن يكون مفعلًا بشكل افتراضي في متصفح كروم.

فيتوريو بيرتولا: إذا كان لي أن أضيف شيئًا عامًا أكثر، أجل، أنت على حق – العديد من المشكلات المتعلقة بالأمن والخصوصية والسيادة الذين [غير مسموع] كنا نتحدث عنهم موجودين

بالفعل اليوم عندما ينتقل مستخدم إلى هناك ويدخل أحد الخوادم، على سبيل المثال خوادم 8.8.8.8 بدلًا من الخادم الافتراضي الذي يحصلون عليه من شبكتهم.

الغرض هو أن هذا يجعل هذا فعلًا الاختيار الافتراضي، لذا فإن هذا يجعل الأمر أسهل بكثير للمتصفح أن يبدل الأشخاص بشكل أساسي من المحلل المحلي إلى المحلل الأكبر وفي الموضوعات – أتفق على أن أي نوع من التركيز يعتبر أحد المخاوف بالفعل. وأنا سعيد للغاية أن غوغل تقول إنهم لا يتبنون هذا النوع من نماذج النشر الآن، لكن بالطبع، ماذا يحدث في خمس أو عشر سنوات أو أيًا يكن؟

أليجاندرا رينوسو: شكرًا جزيلاً. رقم خمسة من فضلك.

روبرتو جيتانو. شكرًا جزيلاً. أنا كبير بما يكفي لأكون شهدت وقت ما كان برنامج الشبكة عبارة عن مجموعة من حلول الملكية التي كانت تفعل القليل من الأشياء بأجزاء مختلفة. وحينها عندما أنشأنا أسلوب البناء الذي كان في سبع طبقات، بطبقة نقل، وطبقة مادية وغيرهم، وجميع تلك الطبقات السبع.

وكانت النتيجة إمكانية وجود برنامج مفتوح والحصول على حلول يمكن أن تتنافس فيها كل طبقة مع بعضها البعض. والآن مع هذا النوع من نهج DoH وDoT، ألسنا نرجع للخلف لحل الملكية، ونحد من إمكانية الحصول على حلول تنافسية ونعود لذلك الشيء في الستينيات الذي كان يسمى بشكل غير صحيح – بالأخص بالنسبة لي بصفتي إيطالي – رمز الاسباغيتي. شكراً.

داني ماكفرسون: نعم، أعتقد أن الأمر عادل. أعتقد أن هذا لا يزال يستخدم حزمة بروتوكولات الإنترنت (TCP IP) ونموذج الطبقات، إنه يتجاوز تحليل الاسم الأعلى بدلاً من استخدام محلل كعب الروتين في النظام المحلي.

الآن، بالتأكيد، إذا رأيت نشرًا في مسارات التحليل على النظام المحلي أو يتحايلون على ذلك تمامًا، من ثم سيكون لذلك انعكاسات على المستخدم وعلى مشغل الشبكة وعلى البنية الأساسية، وهناك العديد من الأطراف التي قد تستفيد والأطراف المختلفة التي قد تخسر من ذلك بطرق معينة.

لذا فمن ناحية، أتفهم وجهة نظرك. من ناحية أخرى، لا أعتقد أنه يختلف عن ذلك، فأنا أعتقد أنه إذا كنت تمتلك تطبيقات المستخدم النهائي ولديك القدرة على الربط مباشرة بالبنية الأساسية لتحليل الأسماء التي تريدها، يمكنك حينئذٍ رؤية كلا الجانبين من تلك المعاملة، وقد تؤثر على مشغلي الشبكات، كما أوضح وارن ومندوبي غوغل، لترقية محللاتها لدعم هذه القدرات الجديدة، وفي أحيان أخرى، قد يكون المستخدم أكثر انجذابًا إلى البنية الأساسية لتحليل الأسماء ومزود الخدمة هذا أكثر من يدركون في الواقع، ويمكن أن يكون مشكلة.

لذلك أعتقد أن هذه نقطة عادلة من هذا المنظور.

بيتر كوتش: روبرتو، أنت والمتحدث السابق تجنبتما قول إن هذا نوع من بناء الصومعة والعودة للخلف، بالطبع، في الصورة الأكبر. ولكن هذا اتجاه لا علاقة له على الفور بتوحيد هذه البروتوكولات. وكما قلت، إنهم على الأرجح أبرياء جدًا. لكن ذلك يتبع اتجاهًا عامًا.

لدى معظمكم الكثير من التطبيقات على هواتفهم الذكية، وكانت هناك مناقشات طويلة حول ما يعنيه ذلك للتوحيد القياسي، ثم بالطبع أيضًا لاستخدام البنية الأساسية المركزية، لأنه عندما أستخدم تطبيقات تتصل بالمنزل فقط، ما الذي [غير مسموع] معايير لغير مستوى HTTPs وكل شيء يتم هناك، يمكنني القيام به بنفسي؟

هذا جزء من صورة كبيرة. ليس هذا هو الشيء الوحيد، ولكنه بالطبع اتجاه آخر، وهو يتعلق بالبنية الأساسية ذاتها التي تتعامل معها ICANN، وهو أحد الأسباب الرئيسية لإيصال هذا إلى الجمهور هنا.

أليجاندرا رينوسو: شكراً. رقم ثلاثة.

يورغ شويغر: أعتبر أن الاستنتاج قد توصل إلى أن ما إذا كانت DoH جيدة أم لا، يعتمد على نموذج النشر، لكنني أتساءل عما إذا كان هذا صحيحًا حقًا. وإذا كان المستخدم فقط من لديه الاختيار، حينها سيكون من المفيد استخدام DoH. لكن مع الأخذ في الاعتبار أن المستخدم يقوم بتنزيل تطبيق ومن ثم سيدفن مسار التحليل في التطبيق بشكل عميق.

لذلك لا يوجد خيار حاليًا، وإذا كان ممكنًا أن ينتمي متجر التطبيقات هذا إلى لاعب رئيسي، حينها بالتأكيد لن يكون هناك خيار. حسنًا، إنه حقًا يتعلق بنموذج النشر بشكل تام؟

فيتوريو بيرتولا: لقد كان هذا الأمر محل نقاش مثير للاهتمام في فريق مهام هندسة الإنترنت، لأنه بالطبع، كان هناك بعض المناقشات حول إلى أي مدى تمثل هذه مشكلة في البروتوكول وإلى أي مدى هذه مسألة تتعلق بالطريقة التي يستخدمها الناس.

أعتقد أن الشيء الأهم على أية حال أننا نفهم إذا وكيف يمكن أن يكون هناك نقاش يشمل جميع أصحاب المصلحة على نموذج النشر السليم. لأنه في النهاية، على سبيل المثال، إذا كانت التطبيقات لازمة لجعل المستخدم يختار أو حتى يستخدم الافتراضي الذي أعده المستخدم في الجهاز، ونظام التشغيل، كإعداد افتراضي، وإذا قاموا بذلك كقاعدة، فإن معظم المشكلات ستبدأ في التبخر على الأقل.

لكن الهدف هو كيف يمكن لنا أن نحظى بهذه المناقشة؟ لأن هناك عدد قليل من الناس من صانعي المتصفحات هنا، وربما هي الشركات نفسها لكن ليسوا الأشخاص المعنيين بصنع المتصفحات. لذا كيف يمكننا إشراك هؤلاء الأشخاص في مناقشة السياسة؟

أليجاندرا رينوسو: شكراً. لدينا اثنين من الأسئلة من المشاركين عن بعد.

آرييل ليانج: السؤال الأول من كريستوفر ويلكنسون. كان التركيز مشكلة عالمية منذ 20 عامًا. خوادم الجذر، وخوادم الأسماء، ومزودي خدمة الإنترنت، DNS وغيرهم.

لماذا علينا الآن الذهاب في الاتجاه المعاكس؟ أين سيكون موقع هذه المحللات [يسبب انعدام الأمن؟]

فيتوريو بيرتولا: هناك نقطة واحدة أود أن أوضحها وهي أنه من الممكن توزيع منصات المحللات ويمكن أن يكون لديك خادم في كل بلد. ولكن إذا كانت الشركة لا تزال في مكان عمل معين في اختصاص محدد، فسوف تخضع دائمًا لذلك. لذلك أنا متفق مع كريستوفر في المخاوف التي قالها.

داني ماكفرسون: أرغب في إضافة أنني أعتقد أن نظام خادم الجذر وربما بعض السجلات على الأرجح هم المحللات الأكثر توزيعًا على نطاق واسع وأنظمة خدمات الإنترنت في العالم اليوم من كلا المنظورين الجغرافي والتحليلي. لذلك أعتقد أنه إذا – [تم] بعض العمل في الماضي على ما سميناه hypergiants حيث شكلت 20 أو أكثر من كيانات الإنترنت حوالي 80% من إجمالي حركة الإنترنت، وبالتأكيد، إذا كانت تلك الجهات هي التي تشغل هذا الأمر ولا يختار مزودو خدمة الإنترنت ولا الأشخاص الآخرين حماية سرية بيانات التحليل، فإن تلك الجهات قد ترى المزيد من الحركة وسيتسبب هذا بالتأكيد في مشكلات قضائية وغيرها. لكنني أعتقد أن الاقتصادات الطبيعية والرأسمالية سيساعدون في معالجة وتخفيف ذلك مع مرور الوقت. هذه تقنية حديثة للغاية نتحدث عنها. لذلك أعتقد أنها تحتاج إلى طرق للمضي قدمًا بعد.

أليجاندرا رينوسو: شكراً. هل لديك سؤال ثاني؟

آرييل ليانج: السؤال الثاني من مايك باغلي. ألا تسمح DoH بتخطٍ أفضل لأنظمة الحماية المبنية على DNS وتحجب برامج منع الإعلانات كذلك؟ ألا يزيد هذا من مخاطر الأمن؟

ميشيل نيلون: الإجابة المباشرة هي نعم.

داني ماكفرسون: سأتطرق لهذا الأمر. لقد أوضحت نقطة التقاء في الشرائح الخاصة بي، وما قصدته هو أنه إذا كان تحليل DNS الخاص بك يحدث في البروتوكول ذاته للوجهات ذاتها، وكان في طبقة التطبيق حيث تحدث حركة الشبكة الإلكترونية، فإن أي شخص يريد التلاعب في ذلك ببعض الطرق، سيتعين عليه بالتأكيد القيام بعمل أكثر قليلاً للتخلص منه والعثور على ما يريد التلاعب.

وبصراحة تامة، هذه واحدة من المشكلات هنا، هي أن بعض الأشخاص يتلاعبون باستجابات DNS اليوم، وإذا كنت مزودًا لمتصفح أو نظامًا داخليًا أو مشغل تطبيقات ويمكنك منع الأشخاص من التلاعب بالاستجابات، فيمكنك التأثير على اقتصاديات الأشياء تأثيرًا ملموسًا.

لذلك أعتقد أنه سيكون هناك فائزون وخاسرون في ذلك أيضًا، وأعتقد أن أنظمة الأمن سيتعين عليها أن ترتقي، وقد تقوم في الواقع إما بحظر هذه البروتوكولات بالجملة في المؤسسة، وربما هذا ما ستقوم به الكثير من الشركات، أو ستريد استخدام وكيل فيها. ربما لن تسمح لهذه الأشياء أن تتحلل أصلاً في الجزء العلوي في البيئات الخاضعة لسيطرة شديدة، أو حتى من منظور السيادة، وقد يكون ذلك مشكلة في النظام البيئي.

أليجاندرا رينوسو: الرقم الرابع.

كافوس أراستيه: شكرًا جزيلاً. يجب أن أبدي بعض التعليقات بدلاً من طرح الأسئلة. ميشيل، شكرا جزيلا لك. لقد قلت كم منا يفهم ما هو DNS وكيف يعمل. لا يمكنني الإجابة على ذلك، لأنه لم يكن بإمكاننا الحصول على إحصائية، لم أستطع التحدث نيابة عن أي شخص. لذلك فهذه هي كلمتكم.

ومن ثم قلت، هل نحن قلقون بشأن الأمن؟ الإجابة نعم.

هل نحن قلقون بشأن الخصوصية؟ الإجابة نعم.

هل نحن [غير مسموع] بشأن التقنية؟ الإجابة نعم.

لكن بالنسبة لبعض منا – ليس الكثير منا – هذه هي المشكلات الجديدة. علينا مناقشة ذلك. علينا فهم ذلك. قبل الإجابة على أي من تلك الأسئلة، نحتاج إلى رؤية كيف تعمل وما إذا كانت ترد وتستجيب لمشكلة الأمن والخصوصية. لذلك فهي أسئلة أو موضوعات حية، وعلينا اتباع ذلك، ومن الصعب الإجابة على أي من هذه الأسئلة، حتى السؤال الثاني الذي يرتبط مباشرة بمهمة ICANN. ربما لدينا المزيد من الأسئلة لإضافتها إلى هذا السؤال، أو ربما [فقط] هذا السؤال. على أية حال، نحتاج إلى الوقت. شكرًا جزيلاً.

ميشيل نيلون: شكرًا لك، كافوس. لأول مرة، نحن في الواقع متفقون. هذا لا يحدث كثيرًا. أعتقد أن الأمر مع شيء مثل هذا هو أنه جديد جدًا، وأعتقد أن العديد منا أشار إلى أنه تقنية جديدة وليدة.

أعتقد أن الشيء الذي حاول الكثير منا فعله هو محاولة تشجيع الناس في أجزاء مختلفة من النظام البيئي على البدء في طرح هذه الأسئلة وطرح الأسئلة البسيطة والأسئلة الأكثر تعقيدًا والأسئلة الصعبة حقًا فقط في نوع من المستوى النظري، ثم التحدث أيضًا إلى الشركات التي تقوم بالفعل بنشر هذه التقنيات.

وسيقولون "أجل، إنها جيدة، إنها رائعة. ما نقوم به هو من أجل المصلحة الكبرى." لكن ما لم تضعها فعليًا تحت المجهر، فأنت لا تعلم أنها ستكون هكذا إلى الأبد. الشيء الذي قد يبدأ بريئًا قد يصبح شيئًا آخر. أو ربما يظل بريئًا.

لذلك أعتقد أنه شيء سنحتاج إلى النظر فيه، والمشاركة هنا مع بعضكم في القاعة، وربما المشاركة خارج هذه القاعة، والبدء في مواصلة تلك المحادثة، لأن هذا شيء تمت مناقشته في فريق مهام هندسة الإنترنت وبعض الدوائر التقنية تعود إلى، ماذا، ثلاث، أربع سنوات؟ ربما أكثر. لقد بدأ كشيء بسيط، "كيف يمكننا جعل DNS خاصًا أكثر؟" ثم تحور وتحول. لكن الكثير من الأشخاص في هذه القاعة ممن ليسوا ضمن مساحة فريق مهام هندسة الإنترنت، بل من مساحة المهووسين المتشددين، لم يكونوا ينظرون إليها بالفعل، لكنها الآن أصبحت واقعًا، وأعتقد أن الوقت قد حان لبدء هذه المحادثات.

أليجاندرا رينوسو: شكرًا جزيلاً. رقم خمسة من فضلك.

آندي بيتس: مرحباً. شكراً. أنا آندي بيتس من Global Cyber Alliance. نحن من شركاء تأسيس 9.9.9.9 لذلك أجد أن هذا نقاش منعش حول التوحيد. أعتقد أن السؤال المطروح أمام الأعضاء هو أنني أعتقد أننا لا نريد أن يظل المستخدمون فقط مع DNS العادي، لذلك سواء كنت تستخدم أيًا من الثمانيات أو أيًا من الحلول، أعتقد أن الغرض هو أن هذا يعطي المستخدمين أصليًا الحماية من جرائم الإنترنت.

لذلك أعتقد أن طرح السؤال على هذا سيكون هل تريد الدمج أم الجرائم الإلكترونية؟ ليس هناك أي اختيارات حقيقية. لكنني أرحب برأيك من فضلك.

فيتوريو بيرتولا: تشفير المسار شيء إيجابي، أعتقد أن علينا فعله. النصيحة التي قد نعطيها للمشغلين [غير مسموع] هي نشر DoH. في الوقت نفسه، إذا قمت بحل بعض المشكلات المتعلقة

بالخصوصية والأمان، ولكن بعد ذلك قمت بإنشاء مشكلات أخرى تتعلق بالخصوصية والأمان قد تكون أكبر من ذلك، فأنت لم تتقدم حقًا.

لذلك أعتقد أن الطريقة الإيجابية للخروج من هذا هي الحصول على فهم مشترك لما يحدث وسياسة مشتركة حول كيفية القيام بذلك بحيث تزيد من الإيجابيات وتعالج السلبيات.

أليجاندرا رينوسو: شكرًا جزيلاً. رقم ثلاثة؟

وولفغانغ كلينفتشيتر: شكرًا جزيلاً. هذه هي قاعة اللجنة الاستشارية الحكومية هنا، وقد ذكرت ذلك بالفعل إحدى الشرائح، وسيكون لذلك بعض الآثار على الإطارات التنظيمية الوطنية. هل ترى دور للحكومات هنا، أم هل حصلت بالفعل على بعض التعليقات من وكالات إنفاذ القانون؟

ميشيل نيلون: ولفغانغ، لا أحد منا - لسنا مسؤولين عن هذا. نحن مجموعة من الأشخاص الذين طُلب منهم التحدث عن هذا لعدة أسباب مختلفة، ولكن إذا كنت تريد طرح هذا السؤال، فلا تسألنا وأعتقد أنه من الأفضل أن نقول ذلك.

سيعارضني فيتوريو بالطبع، لكن هذا هو دوره في هذه اللجنة. بيتر سيتعارض معي.

بيتر كوتش: للمرة الأولى على الإطلاق يا ميشيل. لذا أجل، سؤال ممتاز. أعتقد أن هناك بعض الجوانب لنقاش الحجب هذا بالكامل، وهناك حكومات تؤمن بحجب DNS وأنه سيمنع المستهلك المخصص لبعض المحتوى من الوصول إليه.

نحن نعلم أن هذه الطرق يسهل التحايل عليها. ومع ذلك، من ناحية أخرى، حيث يتم استخدام تحليل اسم النطاق لمنع الوصول غير المقصود إلى المحتوى أو أي شيء، والحديث عن البرامج الضارة والتصيّد وما إلى ذلك، أو [غير مسموع] الاتصال بأنظمة

التحكم والتحكم في شبكة الروبوت، والتي قد تعمل، ولكن لا يوجد شيء يقول أن موفري التحليل - بعضهم بالفعل يقدمون اليوم بعض الخدمات المعينة، كما هو الحال في حماية DNS، أو لست متأكدًا من أنها تحمل علامات تجارية، ولكنها جدران الحماية لـ DNS وما إلى ذلك. إنها منتشرة بحرية. يمكنكم حقًا الانتقال إلى هناك.

ثم للرجوع إلى سؤال ميلتون، نعم، وبعضهم يتقاضون أموالًا، والبعض الآخر يأخذ البيانات، وهو موضوع مختلف. لكن البعض منهم يفرض رسومًا مقابل الحصول على خدمة التحليل التي تمتلك بالفعل قوائم سوداء لمواقع البرامج الضارة والتصيد المعروفة. وليس هناك سبب لعدم نشر هذا من قبل بعض مقدمي الخدمات على الأقل الذين تحدثنا عنهم. وبهذا المعنى، لا ينبغي اعتبار جميع القصص المتعلقة بالتنظيم وأنه يمكن التحايل عليها بسهولة أمراً مسلمًا به. هناك بعض الصعوبات في الأمر وبعض التفاصيل.

وإذا كنت تؤمن بحجب DNS، فقد تؤمن بحجب DNS حتى مع DNS عبر HTTPS.

فيتوريو بيرتولا: أردت فقط أن أضيف شيئًا واحدًا. أنا شخصياً لا أحب حجب DNS بشكل خاص، لكنني أعتقد أنه من المهم حقًا أن يتم اتخاذ قرار بشأن حظر المحتوى من عدمه بشكل ديمقراطي من قبل كل بلد باستخدام مجتمع الإنترنت الخاص بها، ولا يتم اتخاذه من قبل شركات الإنترنت وصناع متصفحات الإنترنت معًا. لذلك أعتقد أنها مسألة سلطة حقًا بهذا المعنى. وهذا ما أغضبني، لأن بعض أنصار DoH خرجوا وأجروا مقابلات قائلين "نحن سوف ننقذ العالم من الرقابة وأي نوع من التحكم في المحتوى هو رقابة حتى في البلدان الديمقراطية."

هذا شيء حقًا، بصفتي مواطن أوروبي، أغضبني حقًا. وفيما يتعلق بالحكومات الأخرى - أعرف فقط الحكومات البريطانية، لكن إذا كانت هناك حكومات أخرى تتعامل مع هذا، فمرحبًا بها.

أليجاندرا رينوسو: شكرًا جزيلاً. ننتقل لرقم أربعة، ثم نغلق قائمة الانتظار مع المشاركين عن بُعد.

سيباستيان باتشوليه: شكراً. سأتحدث باللغة الفرنسية لأن لدينا أدوات الترجمة الشفوية ولدينا مترجمين فوريين مؤهلين في القاعة. لذلك أنا مستخدم نهائي فردي، وأنا عضو في ALAC، وهناك عدد معين من الأسئلة التي أردت طرحها. لكنني أملك الإجابة بالفعل.

لديّ سؤالان آخران: ما هو خيار المستخدم النهائي في كل هذا؟ ألا يوجد خطر في أننا نجد أنفسنا في الموقف الذي كنا فيه قبل بضع سنوات حيث كنا مع MSN، مع CompuServe وما إلى ذلك؟ الآن سيكون هناك آخرون. ولكن شخص ما سوف يختار لنا أين يحدث الحل.

يتعلق سؤالي الثاني بحقيقة أننا في ICANN. ما هي العواقب المحتملة للتسمية، ولخوادم الجذر، وعلى الطريقة التي سيتم بها إدارة كل ذلك في المستقبل؟ هل يمكننا تخيل أن ICANN لم يعد هناك حاجة إلى وجودها؟ نظرًا لأن هذه المحللات، قد تقرر الخوادم أن تضيف في ملفاتها امتدادات جديدة أو أسماء جديدة أو قد تزيلها؟ ومنها حجب أشياء أو إضافة أشياء. تلك الأسئلة مهمة في رأيي.

وأتفق مع ما قلته سابقًا. من المهم أن نواصل العمل على هذه الأسئلة. إنه لأمر سيء للغاية أن يتم التقييس قبل أن نتمكن من مناقشة هذه المواضيع مع جميع أصحاب المصلحة. شكرًا جزيلاً.

ميشيل نيلون: سيباستيان، شكرا على الأسئلة. أعتقد أن سؤالك الأول قمنا بتغطيته نوعًا ما بالفعل في بعض الأسئلة والأجوبة في وقت سابق من الجلسة. نعم، لديك القدرة على الانتهاء حيث يختار موردان ما يحدث. وبما أنني تطرقت إليه في وقت سابق، فلديك عكس الحجب حيث لديك إمكانية الإضافة. هذه مخاطرة.

لكن البروتوكولات والمعايير هي أشياء يتم تطويرها من قبل أشخاص داخل فريق مهام هندسة الإنترنت وهيئات المعايير الأخرى. لديهم مناقشات هناك. ويمكنك متابعة تلك المناقشات. إنها مفتوحة.

بالطبع الحاجز، هناك حاجز فني للدخول. إنها ليست مفتوحة للجميع. هناك معايير تؤثر على حياتنا اليومية، ولن يكون لدى الكثير منا أدنى فكرة عما يتحدثون عنه لأنه ليس مجال خبرتنا.

لقد أدرك الناس هذه الأشياء ويمكنهم إجراء تلك المناقشات. أعتقد أن هذا هو السبب وراء وجود هذه المناقشات الآن. لا أعرف، هل يريد أحد إضافة أي شيء آخر؟ تيم؟

تيم أبريل: كنت أود فقط أن أضيف أن تقنيات DoH وDoT لا تصنعان بطبيعتهما - ليست هي الجاني في هذه الحالة. الأمر متروك للتنفيذ الذي سيؤثر حقًا على كيفية اتخاذ هذه القرارات، حيث يمكن القيام بكل هذا دون اقتراح معايير DoH أوDoT في فريق مهام هندسة الإنترنت. قد يكون تم تنفيذه من قبل موردي المتصفح بشكل متعامد.

والسبب الرئيسي لوجود مثل هذا الموضوع الشسق الآن هو أنها المعايير المقترحة وهناك الكثير من النقاش حول تعزيز - أو إضافة آلية الخصوصية هذه إلى الميل الأول من طلبات DNS.

أنا متأكد من أنه إذا تم وضع حواجز الطرق في طريق هذا النوع من النشر، فسيستمر الأشخاص الأذكياء في فريق مهام هندسة الإنترنت في العثور على طرق أخرى حول حواجز الطرق هذه.

أليجاندرا رينوسو: أنا آسف للغاية لمقاطعتك، لكنني أعتقد أننا بحاجة إلى طرح السؤال الأخير عن بُعد لأن الوقت ينفد منا. آسف جدا للمقاطعة. يمكننا متابعة المحادثة في الردهة بعد ذلك. السؤال عن بعد من فضلك.

آرييل ليانج: السؤال عن بعد هو تعليق من بأول هوفمان. DoT و DoH بروتوكولان جديدان، لكن التطبيقات وأنظمة التشغيل تمكنت من القيام بشيء مماثل لهما لأكثر من 20 عامًا.

فيتوريو بيرتولا: إنه أحد واضعي معيار DoH. لكن الرأي عادل.

أليجاندرا رينوسو: حسنًا، شكرًا جزيلاً لك على تعليقاتك. الآن [أرغب في التقريب] وإنهاء هذا الموضوع ذي الاهتمام الكبير، سأطلب من كل واحد منك التفكير سريعًا في شيء ينبغي للجمهور أن يتذكره من هذه المحادثة. ويمكنكم البدء الآن. شكراً.

تيم أبريل: سأبدأ وأتخذ الأمر السهل. كما كنت أقول قبل ثانية، فإن DoH وDoT هما معياران مقترحان في فريق مهام هندسة الإنترنت لا يضيفان أي قدرات فنية إلى نظام الأسماء الذي لم يكن ممكنًا بالفعل من خلال طرق غير قياسية.

ومصدر القلق الكبير في ذهني على الأقل هو أن الكثير من المحادثات التي أجريناها هنا تعتمد كثيرًا على السياسات وتفاصيل التنفيذ لكل من هذين البروتوكولين في التطبيقات [غير مسموع] أو في المحللات والسلطات أثناء تقدمنا مع هذه التدابير.

فيتوريو بيرتولا: رسالتي هي فقط لمواصلة الفهم، خاصة إذا كانت هذه هي المرة الأولى التي تشارك فيها في هذه المناقشة، فهناك الكثير من الأشخاص الذين يسعدهم تقديم المساعدة، وهناك بالفعل عروض تقديمية مادية على الشبكة الإلكترونية. يمكنكم إيجاد أشياء. ولكن بعد ذلك فكر في الطريقة [المعتادة] التي يمكن بها لأصحاب المصلحة المشاركة مع بقية المجتمع والمساهمة في المناقشة سواء في فريق مهام هندسة الإنترنت أو في بعض أماكن السياسة التي لم يتم تحديدها بعد ولكن يمكن أن تتناول القضايا التقنية والموجهة نحو السياسة.

بيتر كوتش: نعم، أريد أن أقول إن المعايير الصادرة عن فريق مهام هندسة الإنترنت ربما تكون مفيدة للتطورات التي نراها، لكنها ليست السبب الجذري، وعلينا التركيز على السبب الجذري

وأيضًا الوصول إلى الصورة الأكبر، ماذا يفعل هذا يعني بالنسبة لبيئة ICANN و ICANN ومستقبل حوكمة العالم المجرد؟

داني ماكفرسون: أجل. من وجهة نظر تشغيلية، أعتقد أن هناك بعض النفقات العامة، ولكن هناك أيضًا فائدة من منظور الخصوصية والأمان، وفهم أين وكيف سيتم نشرها سيطبق على ذلك.

أعتقد أنه مع وجود تغطية SSAC لذلك، بدأت SSAC في التفكير في هذا الأمر، وإننا بالتأكيد نرحب بتعليقاتك. ما زلنا نناقش الأمر، وهو هدف متحرك. وهي تسير على مسار المعايير في فريق مهام هندسة الإنترنت. إنها ليست معايير كاملة بعد، لكنها بالتأكيد على مسار المعايير، [وأعتقد] أن تفهم الآثار المترتبة على ICANN وأنصار السياسة، والأشخاص الذين يشاركون في ICANN على وجه الخصوص، نأمل أن تساعد مشورة SSAC في معالجة أو تقديم بعض الرؤى الإضافية للأشخاص ليأخذوها بعين الاعتبار أثناء قيامهم بوظائفهم في ICANN. شكراً.

ميشيل نيلون: اليخندرا، لقد فعلتِ شيئًا خطيرًا للغاية. لقد أعطيتني الكلمة الأخيرة.

أليجاندرا رينوسو: تفضل.

ميشيل نيلون: شكراً. أعتقد أنه كانت هناك بعض الأسئلة والتعليقات المثيرة للاهتمام من كل الأشخاص هنا في القاعة وغيرهم. أعتقد بالنسبة لي شخصيًا، كان لدي بعض المشاعر حول التقنيات قبل مجيئي إلى هنا، والاستماع إلى بعض الأسئلة التي طرحناها وبعض التعليقات، ما زال تفكيري حول هذا الموضوع يتطور. وأعتقد أن هذا بالنسبة لي يعني أننا على الأرجح على المسار الصحيح فيما يتعلق بإجراء هذه المحادثة بالفعل.

لذا فإن الرسالة إلى بقيتكم هي إذا نظرت إلى الشريحة التي تظهر على الشاشة في الوقت الحالي، فهناك بضع نقاط هناك يمكنك من خلالها معرفة المزيد في اجتماع فريق مهام هندسة الإنترنت القادم. [أعتقد أنه كان] dnsprivacy.org، أعتقد أن لديه الكثير من المعلومات حول التقنيات الأساسية. هناك الكثير من منشورات المدونات من العديد من الشركات المختلفة، ومجموعات أخرى مثل CENTR أعتقد أنها نشرت بحثًا حولها مؤخرًا. خذوا وقتكم، وقوموا بقراءة المزيد حول هذا الموضوع، واطرحوا الأسئلة.

أليجاندرا رينوسو: شكرًا جزيلاً. انتهت هذه الجلسة. تصفيق كبير لأعضاء اللجنة.

[نهاية النص المدون]