مونتريال - كيف تسير الأمور: عمليات خوادم الجذر
الأحد، الموافق 3 تشرين الثاني (نوفمبر) 2019 - من الساعة 03:15 م إلى الساعة 04:45 م بالتوقيت الصيفي الشرقي
ICANN66 | مونتريال، كندا

ستيف كونتي: سنبدأ في دقائق معدودة. نحن في قاعة أكبر مما نحتاج إليه. إذا كان بإمكانكم أن تقتربوا، فهذا رائع، يمكننا أن نراكم حينها فعلاً. الطريقة التي سنفعل بها ذلك، تقوم RSSAC بتقديم عرض تقديمي وبعد ذلك سيكون لدينا أوقات مخصصة للأسئلة وسنرجع إليكم من أجل الأسئلة. لقد اتخذت بالفعل خطواتي لهذا اليوم، لذلك كلما كنتم أقرب كلما كان ذلك أفضل بالنسبة لي أيضًا، والأمر كله يتعلق بي. سوف نبدأ في غضون بضعة دقائق.

أندرو ماكوناتشي: مرحبًا، اسمي أندرو ماكوناتشي، أعمل لدى ICANN لدعم اللجنة الاستشارية لنظام خادم الجذر وسأتحدث اليوم عن البرنامج التعليمي لنظام خادم الجذر، وأعتقد أنني أستطيع رؤيته هناك. أحب أن أتحرك، لذلك لن أجلس، أعتذر لأي شخص مشارك عن بعد، يجب أن تتبعني الكاميرا أو أي شيء آخر. أعدكم أن العرض التقديمي أكثر إثارة للاهتمام من أي صور لي، لذلك سنمضي قدمًا.

سأقوم بذلك بالتنسيق مع زميلي، أوزان ساهين، الذي سيسير الجزء الثاني. سأستعرض أولاً نظرة عامة على DNS، والتي من المحتمل أن تكون قليلاً من المراجعة لكثير من الأشخاص في هذه القاعة لأنني أفهم أن لديكم بالفعل DNS101 لكننا سنتابع ذلك. ثم سأذهب إلى شرح تعدد الاتجاهات وكيف يختلف تعدد الاتجاهات عن فردية الاتجاهات وسبب أهميته بالنسبة لنظام خادم الجذر. بعد ذلك، سوف أنتقل إلى نظام خادم الجذر اليوم، معدات توجيهه وقليلًا من تاريخه. بعد ذلك، سيتولى أوزان ويتحدث عن RSSAC وتجمع RSSAC والعمل المستمر مع تطور نظام خادم الجذر. لنبدأ.

نظرة عامة حول نظام أسماء النطاقات. أخمن أن معظم الأشخاص في هذه القاعة يعرفون بالفعل عن المعرّفات على الإنترنت وأنواع المعرّفات المختلفة. تتحدث هذه الشريحة عن عناوين بروتوكول الإنترنت ومدى أهميتها بالنسبة للإنترنت. يتطلب جميع المضيفين المتصلين بالإنترنت عنوان بروتوكول الإنترنت، وهناك نوعان مختلفان، IPv4 وIPv6. إنها تسمية رقمية، وليست اسمًا. فهي معرّف أساسي من أجل الإنترنت.

لماذا DNS؟ ما هي المشكلة مع مجرد استخدام عناوين بروتوكول الإنترنت؟ حسنًا، من الصعب تذكر عناوين IP، فهي تتغير كثيرًا. هناك مشكلات حديثة حدثت أيضًا بعد إدخال DNS، وهو أنه يمكن مشاركة عناوين IP. يمكن للعملاء الحصول على عناوين IP متعددة، ويمكن أن يكون للخوادم عناوين IP متعددة، ويمكن للمضيفين الحصول على أكثر من عنوان IP واحد، لذلك، أي واحد تستخدمه؟ يمكنك استخدام نظام التسمية للمساعدة في ذلك.

كما تعلمتم على الأرجح في مناقشة DNS101، العرض التقديمي، نظام DNS هرمي، له جذر في الأعلى وبعد ذلك، لديك ما يسمى نطاقات المستوى الأعلى، وهنا لدينا بعض الأمثلة من UK.، وORG.، وEDU. وفي الأسفل يكون لديكم المستوى الثاني ثم المستوى الثالث وبعد ذلك وهكذا دواليك. يمكننا عمومًا التفكير في وجود تقابل بين الأسماء إلى عناوين IP، والذي ربما يشار إليه باسم تخطيط A أو Quad A إذا كنت معتادًا على هذه المصطلحات. هناك أيضًا تخطيطات أخرى، وتخطيط الأسماء أيضًا لأسماء خوادم البريد، وهناك أيضًا عمليات البحث العكسي عن DNS.

لدينا هنا بعض التعاريف، ستكون هناك شريحتان مليئتان بالتعريفات، ومن الجيد أن نتجاوزها قبل أن نتعمق في الموضوع، فقط حتى يكون الناس على دراية بهذه المصطلحات. هذه بعض المصطلحات التي تستخدمها RSSAC بشكل تكراري، ليس فقط في مستنداتنا ولكن أيضًا في هذا العرض التقديمي. أول واحد استخدمته بالفعل من قبل هو نظام خادم الجذر وهذا هو مجموعة خدمات الجذر التي تنفذ مجتمعة خادم الجذر. سنقوم بالبحث في هذا لاحقًا.

ثم هناك منطقة الجذر، وهي البيانات بالفعل، مثلما حدث في الشريحة الأخيرة عندما تحدثت عن التسلسل الهرمي DNS، نحن نتحدث حقًا عن البيانات التي يساعد نظام خادم الجذر في توزيعها. منطقة الجذر هي البيانات التي يساعد نظام خادم الجذر في توزيعها. ليس له أصل ويحتوي على جميع المعلومات اللازمة للاتصال بنطاقات المستوى الأعلى تحته. أخيرًا، في هذه الشريحة، لدينا معدات التوجيه متعدد الإتجاهات لخادم الجذر، يستخدم كل مشغلي خوادم الجذر تعدد الاتجاهات، عندما نشير إلى خوادم فردية أو أجهزة مادية، نتحدث حقًا عن معدات التوجيه متعدد الإتجاهات.

هنا لدينا بعض الأدوار التنظيمية. لدينا مسؤول منطقة الجذر وهذه هي المؤسسة المسؤولة عن إدارة البيانات المضمنة في منطقة الجذر. هذه هي وظيفة IANA بشكل أساسي وهذا يتضمن تعيين المشغل إلى نطاقات المستوى الأعلى والحفاظ على التفاصيل الإدارية الفنية وما يعنيه

ذلك، والطرق التي يمكنك بها حل نطاق المستوى الأعلى، تتطلب وجود خادم لنطاق المستوى الأعلى هذا الذي يمكن أن يجيب على الاستفسارات والأشخاص الذين يشغلون نطاق المستوى الأعلى هذا، سيحتاجون في بعض الأحيان إلى تحديث الخادم الذي هو عليه ومن ثم عليهم التحدث إلى مسؤول منطقة الجذر.

يوجد أيضًا مشرف صيانة منطقة الجذر، وهو حاليًا Verisign وهذه هي المؤسسة المسؤولة عن قبول البيانات من مسؤول منطقة الجذر ثم تنسيقها في ملف منطقة ثم الأهم من ذلك، التوقيع بشكل مشفر ثم بعد ذلك، وتوزيعها على مشغلي خادم الجذر. مشغلي خادم الجذر، هناك 12 منهم وهذه هي المؤسسات المسؤولة عن إدارة خدمة الجذر على عناوين IP المحددة في منطقة الجذر وملفات الجذر. هذه هي المؤسسات الفردية التي تقوم بتشغيل خوادم الجذر الفعلية.

لقد تحدثت قليلاً عن هذا بالفعل، وهنا نتحدث عن الفرق بين البيانات وكيف يحصل الشخص على البيانات. هناك خوادم تخدم البيانات وهناك البيانات نفسها. تتحدث منطقة الجذر عن تلك البيانات، وهي ملف المنطقة، ثم يتكون نظام خادم الجذر من نظم خادم الجذر (RSO) التي لديها خوادم تقوم بعد ذلك بتقديم هذه البيانات. هذه الشريحة تقارن الاثنين. فيما يتعلق بمنطقة الجذر، فإنها حقًا نقطة الانطلاق. إنها قائمة بنطاقات TLD وأسماء الخادم الخاصة بها، فكيف ستحلونها. ستذهب إلى أسماء الخادم في TLDs من أجل حل الأسماء الموجودة أسفل نطاقات TLDs تلك. تتم إدارة منطقة الجذر بواسطة ICANN وفقًا لسياسة المجتمع.

كما هو موضح في الشريحة الأخيرة، يتم امتثالها وتوزيعها من قِبل جهة صيانة منطقة الجذر، على جميع وحدات خدمة تسجيل الدخول المختلفة وهي المعلومات التي يتم تقديمها بواسطة خوادم الجذر. نظام خادم الجذر هو النظام، الخوادم المكونة، التي تستجيب مع البيانات من منطقة الجذر إلى الاستعلامات. يوجد حاليًا 26 عنوان IP يتكون منها نظام خادم الجذر و13 عنوان IPv4 و13 IPv6 وهناك أكثر من 1000 معد توجيه فعلي. يختلف الرقم، فهو يرتفع ببطء مع مرور الوقت. الآن، نقول فقط أكثر من 1000. لقد اعتدنا على الحصول على شريحة توضح العدد بالضبط، ثم احتجنا باستمرار إلى تحديثه، لذلك قلنا، "حسنًا، يوجد الآن ما يزيد قليلاً عن 1000." إنه دور تقني محض لخدمة منطقة الجذر، ويقع على عاتق مشغلي خادم الجذر.

تستعرض هذه الشريحة كل تفاصيل استعلام DNS استجابةً لذلك. سأقضي بعض الوقت على هذه الشريحة وأتصفح ما يحدث مع جهاز الكمبيوتر عندما يريد حل اسم وهو يمر باسم خادم تكراري.

إذا بدأنا من جديد على اليمين، فإننا نرى لدينا المستخدم لدينا، لدينا مستخدم الانترنت يعرف أيضا باسم العميل وأنهم يستخدمون الكمبيوتر وسيرغبون حقًا في الوصول إلى www.example.com. الآن، بافتراض أن هذا الخادم التكراري قد تم تشغيله للتو وليس لديه أي شيء في ذاكرة التخزين المؤقت، لذلك فهو جاهل بشكل أساسي، فهو لا يعرف شيئًا سوى كيفية الوصول إلى خوادم اسم الجذر. ما الذي سيفعله المستخدمون في الكمبيوتر أولاً، سيقوم بالاتصال باسم الخادم التكراري هذا الموجود في منتصف الصورة، وسيرسل استعلامًا إلى اسم الخادم التكراري هذا يقول، "مهلا، ما هو عنوان IP الخاص بالموقع www.example.com؟"

واسم الخادم التكراري، لأنه فقط تم تشغيله وأنه ليس لديه أي شيء في ذاكرة التخزين المؤقت، فإنه سيقوم بالاتصال أولا بنظام خادم الجذر، وهو اسم خادم الجذر. ومن المرجح أن يرسل الاستعلام بالكامل إلى اسم خادم الجذر ذلك وسوف يطلب فقط، "مهلا، ما هو عنوان IP من أجل الموقع www.example.com؟" وسيقول اسم خادم الجذر، "لا أعرف العنوان للموقع www.example.com لكنني أعرف كيفية التواصل مع نطاق COM. وبالمناسبة، فهذا توقيع لهذه البيانات."

وسأرسله مجددًا إلى اسم الخادم التكراري. ثم يقول اسم الخادم التكراري، "حسنًا، هذا جيد. أعرف الآن كيفية الوصول إلى COM. وأوه، لدي هذا التوقيع أيضًا، سأقارن ذلك بشكل تشفيري بالجزء العمومي من مفتاح توقيع المفتاح شفرة الدخول الأساسية KSK، الموجود داخل اسم الخادم التكراري وأحدد أنه نعم، هذه الإجابة من اسم خادم الجذر لموقع COM. صحيحة، سأقوم الآن بالاتصال بنطاق COM."

بعد ذلك يتجه اسم الخادم التكراري إلى اسم خادم COM. ويقول: "أين www.example.com؟ "ويقول اسم خادم .COM Name Server، "لا أعلم أين يوجد لكن أعلم أين يوجد example.com وأوه بالمناسبة، إليك توقيع هذه البيانات." بعد ذلك سيقوم اسم الخادم التكراري بعمل نفس الشيء أساسًا، حيث يقول، "حسنًا، جيد.لدي example.com، ويمكنني التأكد منه بواسطة التوقيعات التشفيرية." ثم بأنتقل إلى اسم خادم example.com

لأحصل في النهاية على الإجابة للموقع www.example.com، بالإضافة إلى توقيع.سيعود إلى اسم الخادم التكراري، ويقول اسم الخادم التكراري، "حسنًا، لدي عنوان IP للمواقع www.example.com الآن ولدي توقيع، وسأقوم بالمقارنة التشفيرية.حسنًا، إنه يتحقق."

الآن فقط يعود اسم الخادم التكراري إلى المستخدم أو يعود إلى كمبيوتر المستخدم ويقول "إليك عنوان IP الخاص بك." ما هو موضح هنا هو أنه من خلال استعلام بسيط بدأه المستخدم، هناك تكرارية، هناك عملية معقدة وطويلة الأمد تستمر في اسم الخادم التكراري وإلى أن تنتهي من ذلك، فإنها لا تعود في الواقع إلى المستخدم.

هذا تعمق في مزيد من التفاصيل حول ما تحدثت عنه للتو. تعرف خوادم الجذر فقط ما تحتاج الخوادم أن تُسأل عنه لاحقًا. في المثال الأخير، كانوا يعرفون فقط كيفية الوصول إلى خوادم COM. إنهم لا يعرفون كيفية حل الاسم بالكامل. ومع ذلك، ضمن الخوادم التكرارية، سيتذكرون تلك الردود، وسيقومون بتخزين تلك الاستجابات مؤقتًا.

ليس عليهم فعلاً الذهاب إلى خوادم الجذر في كثير من الأحيان وفترة بقاء البيانات فعّالة، وغالبًا ما يطلق عليهم TTL لتلك المعلومات المخزنة مؤقتًا لمدة يومين. سيطلب خادم تكراري من خادم الجذر تحديد مكان خوادم اسم COM.، وسيتذكر تلك المعلومات لمدة يومين على الأرجح، ثم لن يضطر إلى السؤال مرة أخرى حتى تنتهي مهلة هذه المعلومات.

هناك بعض التحسينات الحديثة على DNS. تحدثنا عن توقيع التشفير على بيانات DNS. يتم تعريف كل ذلك داخل أمان DNS أو امتدادات الأمان لـ DNS. يتم استخدام أمان DNS فقط كمصطلح قصير للتحدث عن جميع عمليات التوقيع والتحقق التي تحتاج إلى المتابعة من أجل ضمان أن الخوادم التكرارية والعملاء يحصلون على المعلومات الصحيحة من الخوادم. كانت هناك بعض التحسينات الأخيرة للخصوصية وكذلك DNS لأن الاستفسارات يمكن أن تسرب المعلومات. سيقوم DNS الأصلي أو التقليدي بالإبلاغ عن 53 UDP أو كان TCP في نص واضح، وهناك معايير حول معالجة نقل تشفير DNS. لدينا أيضًا DNS عبر TLS، وهناك أيضًا DNS عبر HTTPS.

تعدد الاتجاهات هو تحسين حديث آخر. في هذه المرحلة، جميع مشغلي خادم الجذر الذين طبقوا تعدد الاتجاهات، لدينا قسم كامل يظهر بعد هذا حول تعدد الاتجاهات، يمكننا التحدث عن ذلك بعد ذلك. هذا يقودني مباشرة إلى شرح تعدد الاتجاهات. في البداية كان هناك فردية

الاتجاهات وفردية الاتجاهات تعني أن الحزم من المصادر تذهب جميعها إلى نفس الوجهة، وهناك وجهة واحدة والحزم من جميع المصادر تذهب إلى تلك الوجهة.

بشكل أساسي، يتوافق عنوان IP مع خادم واحد، ويتوافق مع نقطة نهاية واحدة. هذا جيد، إلا إذا كنت تريد توسيع نطاق الأشياء. يتيح تعدد الاتجاهات قابلية التوسع، فهو يجعل قابلية التوسع أسهل بكثير، وهذا مهم إذا كنت ترغب في زيادة الخدمة، إذا كنت تحصل على المزيد من الاستفسارات الصحيحة. من الجيد حقًا أيضًا إذا كان يقوم الأشخاص بشن هجمات الحجب المنتشر للخدمة على خدمتك وترغب في إلغاء تحميل بعض انتقال البيانات إلى العديد من الخوادم المختلفة، يصبح التعامل معها أسهل كثيرًا.

في تعدد الاتجاهات، يتغير التخطيط بين عنوان IP ونقطة النهاية والآن لديك تخطيط عنوان IP واحد إلى خوادم متعددة، إلى نقاط نهاية متعددة. ستصل مصادر مختلفة إلى وجهات مختلفة ولكنها لا تزال جميعها على اتصال أو لا تزال جميعها ترسل انتقال البيانات إلى عنوان IP نفسه، إنها تصل إلى وجهات مادية مختلفة. تحصل المصادر على البيانات بشكل أسرع، وهناك قفزات أقل وسيطة لأن المصادر يمكن أن تكون أقرب إلى وجهاتها. سيكون انتقال بيانات هجمات DDoS هي ما يطلق عليه ثقب الإخماد Sink Hole أو يتم إرسالها إلى أقرب معد توجيه لها ولن تؤدي إلى تعطيل معدات توجيه أخرى.

إليك مثال بسيط جدًا لتدفق انتقال البيانات فردي الاتجاه، وهناك أقصر طريق واحد إلى وجهة واحدة. لدينا مصدر واحد ولدينا وجهة واحدة. إذا قمت بإضافة مصدر آخر إلى ذلك، فسوف ينتقل إلى نفس الوجهة. إليك تعدد الاتجاهات، لديك وجهات متعددة، هذا الذي يبدو كقطرة باللون الأرجواني أو الأزرق، المسماة وجهة. لا يزال لدينا مصدر واحد فقط ولكن يمكنك أن تتخيل ما إذا كان مصدر آخر أقرب إلى وجهة مختلفة متجهة إلى تلك الوجهة الأخرى. يسمح - من الأسهل بكثير توزيع انتقال البيانات.

إليك إحدى المزايا الحقيقية، إحدى المزايا الرائعة لتعدد الاتجاهات، وهي ما يحدث في ظل هجمات الحجب المنتشر للخدمة، وهي أن المصادر التي تستخدم وجهات بعيدة عن هجوم DDoS لا تتأثر بها. إذا كان الهجوم محليًا، بمعنى ما من هجوم محلي أو جغرافيًا محليًا، فسيتم إخماده في خادم واحد ولن يؤثر على العمليات وبقية العالم. هذا هو واحد من الفوائد المهمة لتعدد الاتجاهات.

الآن، سأتحدث قليلاً عن تاريخ نظام خادم الجذر ونظام خادم الجذر اليوم. في الفترة من 1983 إلى 1986، كان لنظام خادم الجذر أربعة عناوين ومن ذلك الحين ازداد بشكل مطرد حتى عام 1998، حيث لا يوجد 13 عنوانًا. ربما ليست العناوين هي المصطلح المناسب للاستخدام هناك ولكن يمكنك أن ترى هذه التغييرات تنمو بمرور الوقت وفي الوقت الحاضر لأنه تمت إضافة IPv6، نقول الآن أن نظام خادم الجذر يحتوي على 26 عنوانًا. 13 IPv4 و13 IPv6. بسبب تعدد الاتجاهات، يمكننا القول أن هناك 26 عنوان، 13 IPv4 و13 IPv6، هناك بالفعل أكثر من 1000 معد اتجاه مادي.

هذه قائمة بأسماء المضيفين وعناوين IPv4 وIPv6، وكذلك المدير، مشغل خادم الجذر لنظام خادم الجذر الحالي. جميع المشغلين، وجميع أسماء المضيفين لها عناوين IPv4 وIPv6 المرتبطة بها. يمكنك أن ترى أنها مرقمة من A إلى M.

هذه خريطة مأخوذة من موقع root-servers.org، وليس المقصود أن تكون دقيقة ودقيقة جغرافيا. ما يمكنك فعله هو، إذا ذهبت إلى موقع root-servers.org، فيمكنك سحب هذا الأمر، إنه على الصفحة الأولى، ثم يمكنك بالفعل تتبع المدن الفردية، ويمكنك النظر إلى قارة ثم بلد ثم المدينة ومن ثم معرفة المشغلين الذين يقومون بتشغيل الخوادم أو معدات توجيه التشغيل في تلك المدن. هذا على أعلى مستوى، حيث يتم تكبير كل شيء، يقوم برنامج التخطيط فقط بتجميع الأشياء.

هذا يدل بشكل أساسي على أن هناك حالات في جميع أنحاء العالم، في كل قارة، لا ينبغي أن أقول ذلك لأنني لا أعرف ما إذا كانت هناك حالة في أنتاركتيكا، ربما شخص ما يمكنه تصحيح ولكن على الأقل كل قارة أخرى غير القارة القطبية الجنوبية. إذا كنت مهتمًا بالتعمق أكثر في هذا الأمر، فمن الممتع الانتقال إلى موقع root-servers.org والتنقل إلى الخريطة ومعرفة المدينة القريبة التي توجد بها معدات توجيه خادم الجذر ومن الذي يقوم بتشغيلها وهذا النوع من الأشياء.

يوضح هذا عملية التغييرات في منطقة الجذر وكيف يتم توفيرها في خوادم الجذر الفعلية، ثم كيف تذهب وحدات الحل وتحصل عليها. على اليسار لدينا مشغلي TLD. لنفترض أن أحد مشغلي TLD يحتاج إلى تقديم طلب تغيير، وسوف يتصلون بـ IANA وسيقولون لـ IANA، "نطاق TLD لدينا، أسماء الخادم لدينا، نستخدم عنوان IP هذا، نود تغييرها إلى عنوان IP آخر."

وسيخبرون IANA بذلك وبعد ذلك يوجد لدى IANA مجموعة من إجراءات التحقق التي تمر بها للتأكد من أنها تتحدث بالفعل مع مشغل TLD، وهذا تغيير جيد، وهذا لن يكسر أي شيء. بمجرد موافقة IANA على هذا التغيير، فسوف نجتاز ذلك عندما تخبر IANA مشرف صيانة منطقة الجذر بأنه "هذا هو ملف منطقة الجذر". سيقوم فقط بتحديث هذه المعلومات وملف منطقة الجذر التالي الذي ينتقل إلى مشرف الصيانة على منطقة الجذر. يقوم مشرف الصيانة على منطقة الجذر بامتثال منطقة الجذر ويوقعها تشفيريًا ثم يوزعها على المشغلين.

ثم على اليمين، كل تلك الفقاعات الصغيرة مع RS، من المفترض أن تمثل الحالات الفردية، هناك الكثير منها، لكل مشغل هناك الكثير منها. ثم في أقصى اليمين يمكننا أن نرى وحدات الحل التكرارية ترسل الاستفسارات وتحصل على الردود. هذا هو تدفق المعلومات، والتدفق عالي المستوى لكيفية تغير المعلومات في منطقة الجذر وعملية ذلك.

مزيد من المعلومات حول مشغلي خادم الجذر، كما قلت، هناك 12 منهم وهم يركزون بشكل أساسي على الموثوقية والاستقرار وإمكانية الوصول لجميع مستخدمي الإنترنت. يتعاونون مع بعضهم البعض من خلال RSSAC وعمليات الجذر وأماكن أخرى. تركز على الاحترافية وهناك أنواع مختلفة من المنظمات، فهي ليست جميعها غير هادفة للربح، وليست جميعها حكومات، وأنواع مختلفة من المنظمات وهي متنوعة من الناحية التنظيمية، والجغرافية، ونماذج تمويلها.

هذه هي بعض الطرق التي ينسقون بها. لقد ذكرت بعض الاجتماعات والهيئات الصناعية المختلفة مثل اجتماعات ICANN وRSSAC، وITF، وRIR، ومجموعات مشغل الشبكة، DNSORC، كما أنها تستخدم أنواعًا مختلفة أخرى من الأدوات مثل أي منظمات تحتاج إلى التنسيق. إنهم يشاركون البيانات فيما بينهم ويؤدون أيضًا أنشطة دورية، مثل تمارين خلايا الأزمات وما يجب التخطيط له في حالات الطوارئ وما إلى ذلك.

تشارك منظمات الدعم الإقليمية في تشغيل وتطوير الخدمة. تقيم التعديلات التقنية المقترحة وتنشرها، ربما على بروتوكول، مثل بروتوكول DNS. يشاركون في IETF لذلك. للتأكد من الحفاظ على الاستقرار والمتانة والقدرة على الوصول. لا يشارك المشغلون في صنع السياسة وهم لا يشاركون بالتأكيد في تعديلات البيانات. تقوم وحدات تسجيل الدخول بنشر البيانات فقط، ولا تشارك في ماهية البيانات.

وبالنظر إلى ذلك، تعرض هذه الشريحة بعض الأساطير التي واجهتها RSSAC والتي واجهتها على مر السنين، وكذلك الواقع. الأسطورة الأولى هي أن خوادم الجذر تتحكم في أماكن انتقال البيانات على الإنترنت والواقع هو أن أجهزة توجيه حزم البيانات تتحكم في مكان انتقال بيانات الإنترنت. خوادم الجذر تجيب فقط عن الاستفسارات التي تقدم لهم من الخوادم التكرارية.

أسطورة أخرى هي أن خادم الجذر يقوم بمعالجة معظم استعلامات DNS ومعظم استعلامات DNS لا تتم معالجتها بواسطة خادم الجذر بسبب التخزين المؤقت، لأن الخوادم التكرارية تتذكر الإجابات فقط، فقد حصلوا عليها من خوادم الجذر حتى لا يضطروا إلى السؤال كل مرة عن السؤال نفسه. هناك أسطورة أخرى هي أن إدارة منطقة الجذر وتوفير الخدمات هما نفس الشيء. مرة أخرى، هذا يعود إلى ما هو الفرق بين البيانات وعرض البيانات؟ تختلف إدارة البيانات اختلافًا كبيرًا عن الإجابة على استفسارات حول البيانات.

أسطورة أخرى هي أن بعض هويات الخادم لها معنى خاص. لا أحد منهم لديه حقا أي معنى خاص. ليس الأمر كذلك. أسطورة أخرى هي أن هناك فقط 13 من خوادم الجذر. لا، بسبب تعدد الاتجاهات، يوجد أكثر من 1000 ولكن هناك 13 هوية تقنية فقط. مشغلي خادم الجذر لا يعملون فقط بشكل مستقل تمامًا، بل يتعاونون مع بعضهم البعض، تحدثنا عن الشريحة الأخيرة. هذه الأخيرة، مشغلي خادم الجذر لا يتلقون سوى جزء TLD من الاستعلام.

عندما كنت أستعرض كيفية استخدام DNS لحل المشكلة، كان لديّ سلسلة استعلام كاملة تصل إلى خادم الجذر وهذا هو تقليديًا كيف تسير الأمور، وربما هذه هي الطريقة التي تسير بها الأمور بنسبة 90 بالمائة من الوقت الآن. لهذا السبب عادةً ما نكون جريئين، فهناك تقنية جديدة تسمى تقنية تصغير اسم الاستعلام، وهي تقنية خصوصية جديدة، وأعتقد أننا يمكن أن نسميها، وهي تخرج من IETF التي تهدف إلى تغيير ذلك ولكن هذا لا يتم نشره على نطاق واسع. يتم نشره أكثر فأكثر ولكن في الوقت الحالي، فإن مشغلي خادم الجذر عادةً ما يتلقون الاستعلام بالكامل.

إذا كنت تدير شبكة، فهناك شيء يجب التفكير فيه فيما يتعلق بنظام DNS وتفاعلاتك مع خوادم الجذر. ربما تريد ثلاث أو أربع معدات توجيه قريبة. قريبة بمعنى، التقارب الطوبولوجي والشبكة، وليس بالضرورة التقارب الجغرافي. ربما يمكنك زيادة نظير في الاتصالات إذا كنت تعاني من الكمون. هناك العديد من الأشياء المختلفة التي يمكنك القيام بها.

شيء آخر هو تشغيل وحدة حل التحقق من صحة أمن DNS، وهذا يمكن أن يضمن أنه بالنسبة لتوقيع البيانات في منطقة الجذر، فإنك تحصل على البيانات الصحيحة، وتحصل على بيانات IANA غير المعدلة، بين خادمك المتكرر وخوادم الجذر وغيرها من الخوادم الرسمية، لا أحد يعبث بالبيانات المنقولة. التحقق من صحة أمن DNS لبيانات التسجيل، أنت تقوم بالتحقق من صحة تلك البيانات في وحدة الحل المحلية الخاصة بك، وهذا يساعد حقًا.

إذا كنت مهتمًا، يمكنك أيضًا المشاركة والمساهمة في تجمع RSSAC وسيتحدث زميلي أوزان قليلاً عن ماهية RSSAC وعن تجمع RSSAC.

ذا كنت مشغل شبكة وترغب في استضافة معد توجيه متعدد الإتجاهات، فيمكنك التحدث إلى عضو من RSSAC بعد هذا العرض التقديمي، يمكنك بالتأكيد طرح ذلك خلال فترة السؤال والجواب أو يمكنك إرسال بريد إلى هذا العنوان ASK-RSSAC@ICANN.ORG.

الآن، سأنتقل إلى العرض التقديمي وأعطي الكلمة لزميلي، أوزان ساهين، الذي سيتناول الجانب التنظيمي للأشياء.

أوزان ساهين: شكرًا لك، أندرو. مرحباً بالجميع، اسمي أوزان، أنا عضو في منظمة ICANN، وأدعم عمل اللجنة الاستشارية لنظام خادم الجذر أو RSSAC.

دعنا نبدأ بدور RSSAC، فهو دور ضيق. يتمثل دور اللجنة الاستشارية لنظام الخادم الجذر نظام أسماء النطاقات ("RSSAC") في تقديم المشورة لمجتمع ومجلس إدارة ICANN حول المسائل المتعلقة بتشغيل وإدارة وأمان وسلامة نظام الخادم الجذر في الإنترنت.

على هذه الشريحة توجد ملاحظتان حول ما تقوم به RSSAC وما لا تفعله. إنها لجنة تقدم المشورة بشكل أساسي إلى مجلس إدارة ICANN ولكن أيضًا إلى هيئات ICANN الأخرى والمنظمات الأخرى المشاركة في أعمال DNS الشاملة. يتم تمثيل مشغلي خادم الجذر داخل RSSAC لكن RSSAC لا تشارك في الأمور التشغيلية.

إذا نظرت إلى تنظيم RSSAC، فهي تتألف من أعضاء معينين وممثلين معينين لمشغلي خادم الجذر. هناك أيضًا بدلاء لهؤلاء الممثلين وهناك جهات اتصال. أيضًا، هناك هذه الهيئة الأخرى المسماة تجمع RSSAC، وهي مجموعة من خبراء المواضيع المتطوعين وخبراء في DNS.

يتم تأكيد أعضاء تجمع RSSAC من خلال RSSAC استنادًا إلى رسالة بيان الإهتمام. إذا كنت تريد أن تصبح عضوًا في مجموعة RSSAC، فأنت تقدم أساسًا كما ناقش زميلي أندرو للتو، رسالة بيان الإهتمام الخاصة بك وRSSAC تؤكد عضويتك.

لدينا رئيسان مشاركان، وهما في هذه القاعة، براد فيرد وفريد بيكر. أريد أيضًا أن أشير إلى أن RSSAC تنتقل إلى نموذج الرئيس / نائب الرئيس. بحلول نهاية العام، سيخوضون انتخابات نائب الرئيس. ستكون RSSAC - ستتألف القيادة من رئيس ونائب للرئيس.

كما قلت للتو، هناك جهات اتصال في RSSAC، أربعة منها هي جهات اتصال واردة وأربعة منهم صادرة، مما يعني وجود اتصال من مشغل وظائف IANA وواحد من مشرف الصيانة على منطقة الجذر وواحد من مجلس هيئة إنشاء وتطوير الإنترنت أو IAB وواحد من اللجنة الاستشارية للأمان والاستقرار التي تعد لجنة استشارية أخرى ضمن نظام ICANN. هناك أربع جهات اتصال صادرة، واحدة لمجلس إدارة ICANN، وواحدة للجنة ترشيح ICANN، وواحدة للجنة الدائمة للعملاء ومنسق واحد للجنة مراجعة تطوير منطقة الجذر أو RZERC.

تضم مجموعة RSSAC أكثر من 100 عضو من الخبراء التقنيين في DNS. كما قلت، يتقدم أي شخص مهتم ليصبح عضواً في تجمع RSSAC من خلال تقديم رسالة بيان الإهتمام ويحصل على ائتمان عام لمساهمة العمل في منشورات RSSAC. يضيف التجمع بالفعل إلى شفافية RSSAC، بحيث يمكنك المشاركة في عمل RSSAC من خلال أن تصبح جزءًا من تجمع RSSAC. كما ذكرت، هؤلاء هم خبراء DNS الذين يقدمون خبرتهم إلى المنشورات.

يوجد حاليًا مجموعات عمل ضمن RSSAC. واحدة هي دراسة سلوكيات وحدات الحل الحديثة. تدرس سلوك البرامج المنشورة الموجودة ووحدات الحل التكرارية من خلال كل من أساس الكود ومجموعات البيانات المتاحة. والأخرى هي توقعات نظام خادم الجذر والمقاييس ذات الصلة. تتمثل مهمتها في تحديد النظام على نطاق واسع في مقياس خارجي يمكن التحقق منه والذي يوضح أن RSS ككل متصل بالإنترنت ويقدم استجابات صحيحة وفي الوقت المناسب للمستخدمين النهائيين.

هناك بعض الأدوات والآليات التي تساهم في شفافية RSSAC ومشغلي خادم الجذر. على سبيل المثال لا الحصر، هناك صفحة ويب RSSAC.ICANN.ORG حيث يمكنك الذهاب والعثور على أسماء أعضاء RSSAC، وأعضاء تجمع RSSAC ، ويمكنك الوصول إلى

المنشورات. يمكنك أيضًا العثور على محاضر اجتماعات RSSAC لعقد المؤتمرات عن بُعد. أيضًا، لدى RSSAC اجتماعات عامة، إذا كنت مهتمًا، يمكنك المشاركة في الاجتماعات.

لدى RSSAC أيضًا اجتماعات مع مجموعات أخرى في ICANN خلال اجتماعات ICANN العامة، على سبيل المثال خلال هذا الاجتماع، والرؤساء المشاركون لـ RSSAC يقدمون موجزات للجنة الاستشارية الحكومية، كما سيجتمع مجلس ICANN مع RSSAC وستعقد RSSAC اجتماعًا مغلقًا مع اللجنة الاستشارية للأمن والاستقرار. إنها تتحدث مع المجموعات الأخرى. تتوفر RSSAC على منشور 000، والذي يحدد إجراءاتها التشغيلية، مما يضيف أيضًا إلى الشفافية.

لدى مشغلي خادم الجذر RSOs أيضًا بعض المنشورات، فلديهم صفحة على الويب root-servers.org. أعتقد أن الخريطة التي عرضها زميلي أندرو للتو مع معدات توجيه في جميع أنحاء العالم يمكن العثور عليها في هذه الصفحة. أيضًا، لدى مشغلي خادم الجذر RSO صفحاتهم الفردية وينشرون تقارير تعاونية حول الأحداث الكبرى وأيضًا مرة أخرى، تحدث أندرو للتو عن ذلك، إذا كانت لديك أسئلة يمكنك إرسال أسئلتك إلى ASK-RSSAC@ICANN.ORG وسنحصل على إجابات.

في المرحلة الثانية من العرض التقديمي سأتحدث عن العمل الجاري في تطور نظام خادم الجذر. لنبدأ بالنظر إلى الجدول الزمني لهذا العمل. منذ أكثر من عام تم نشر RSSAC037 و38. اقترحوا بشكل أساسي نموذجًا جديدًا في إدارة نظام خادم الجذر. بعد ذلك، أصدر مجلس ICANN توجيهًا إلى منظمة ICANN للنظر في هذه الوثائق والعمل عليها. في نيسان/أبريل 2019، نشرت منظمة ICANN أخيرًا ما يسمى الورقة المفاهيمية. في آب/أغسطس 2019، تم إغلاق فترة التعليق العام على الورقة المفاهيمية. تم تلقي التشاور من مجموعات مختلفة. من خلال النظر في جميع التعليقات، فإن الخطوات التالية المتوخاة هي بحلول كانون الثاني/يناير 2020، سيكون هناك مجموعة عمل للحوكمة، تعمل على تطوير النموذج في عامي 2020 و2021. بحلول عام 2022، من المتوقع أن يتم تنفيذ النموذج الجديد.

دعونا ننظر إلى ما كان موضوع RSSAC037. حدد 11 مبدأ لتشغيل وتطوير نظام خادم الجذر. بشكل أساسي، يقترح نموذج إدارة أولي لنظام خادم الجذر ومشغليه. يوضح أيضًا كيف

يعمل نموذج RSSAC037 من خلال مجموعة من السيناريوهات على تعيين مشغلي خادم الجذر وإزالتهم.

في هذه الشريحة، ترى ثلاث توصيات تثني على RSSAC037. أول واحدة هي بدء عملية لإنتاج نسخة نهائية من النموذج على أساس 37. أيضًا، الثانية هي تقدير تكاليف نظام خادم الجذر لتطوير النموذج. يجب أن تركز الجهود الأولية أيضًا على وضع جدول زمني وأيضًا تنفيذ الصيغة النهائية للنموذج استنادًا إلى مبادئ المساءلة والشفافية والخدمة المستدامة والنزاهة.

في هذه الشريحة، سترون رسمًا بيانيًا يوضح ما كان عليه الاقتراح. تشاهدون ثلاثة مجالات مختلفة، أحدها هو الحوكمة، وعمليات جذر DNS الأخرى، ثم هناك تشغيل ووقف تشغيل مشغلي خادم الجذر. في مجال الحوكمة، ترى ثلاثة أصحاب مصلحة هناك، IFT ومجتمع ICANN، وهيئة إنشاء وتطوير الإنترنت ومشغلي خادم الجذر. توفر الشريحة أيضًا الوظائف الخمس التي اقترحها النموذج.

وهي، وظيفة مراقبة الأداء والقياسات، وظيفة التعيين والإزالة، الوظيفة المالية، وظيفة سياسة هندسة الاستراتيجيات وهناك وظيفة الأمانة. تم اقتراح خمس وظائف عن طريق النموذج. ثم تلاحظون في الجزء السفلي من الشريحة وجود بعض مقاييس الأداء، والتي سيتم استخدامها في المنطقة الداخلية والخارجية لمشغلي خادم الجذر. هذا يتعلق بتعيين مشغلي خادم الجذر وإزالة عوامل التشغيل.

تحدثنا للتو عن الوظائف والعودة إلى نموذج المفهوم، فإنه يتصور الهياكل التالية على أساس نموذج 37 الذي يتوافق مع الوظائف الخمس. أحدها هو مجلس إدارة نظام خادم الجذر، واللجنة الدائمة الأخرى لنظام خادم الجذر، ولجنة مراجعة مشغل خادم الجذر، آخر وظيفتين هما وظيفة التمويل ووظائف الأمانة، منظمة ICANN.

تحدد الورقة المفاهيمية العملية التي يحركها المجتمع، لوضع اللمسات الأخيرة على نموذج جديد للتعاون والحوكمة لـ RSS استنادًا إلى التوصية رقم واحد في RSSAC 38، وهو منشور آخر يتعلق بتطوير نظام خادم الجذر في المرحلة الأولى، تقوم ICANN بمراجعة وتقييم RSSAC037 في اتجاه مجلس إدارة ICANN، الأمر الذي تم بالفعل.

في المرحلة الثانية، مجموعة عمل حوكمة أوراق المفاهيم RSSAC037، الوثيقة متوفرة للتعليق العام وتحدثنا عنها. في المرحلة الثالثة، يتعلق الأمر بتطوير نموذج جديد للتعاون والحوكمة لـ RSS وله مساران، أحدهما المسار الهيكلي والآخر المسار الإداري. تقوم مجموعة عمل حوكمة المسار الهيكلي بتطوير نموذج، في المسار الإداري، وتخطط لتنفيذ نموذج مجموعة عمل الحوكمة الذي تقوده منظمة ICANN.

ما هي مجموعة عمل الحوكمة وتكوينها؟ إنها تتألف من ممثلين من RSSAC ومنظمة دعم أسماء ccTLD ومجموعة أصحاب المصلحة للسجلات واللجنة الاستشارية للأمن والاستقرار. سيكون هناك أيضًا منسقون من مجلس إدارة ICANN وIANA ومشرف الصيانة على منطقة الجذر.

فريق عمل الحوكمة مكلف بوضع تفاصيل النموذج. تحدد الورقة المفاهيمية أيضًا بعض الإرشادات الخاصة بمجموعة عمل الحوكمة، والتي تلتزم بجدول زمني ذي معالم واضحة، وفتح باب العمل والشفافية، وتسعى إلى الحصول على مساهمات مستنيرة عند الضرورة، وتتبنى أيضًا المبادئ الواردة في RSSAC037 وتشير بشكل أساسي إلى الورقة المفاهيمية لـ RSSAC037 والتعليقات العامة التي تم تلقيها.

نحن الآن في جزء الأسئلة والأجوبة من الجلسة. يوجد في القاعة ممثلو مشغل خادم الجذر الذين هم أعضاء في RSSAC. إذا جاز لي أن أقترح عليهم أن يأتوا على المنصة ويشغلوا مقاعدهم لأخذ أسئلة من الجمهور. سيكون هناك بعض الميكروفونات الجوالة، إذا رفعت يدك، فسنقدم لك الميكروفون بحيث يمكنك طرح سؤالك.

ستيف كونتي: أثناء إعدادهم، لدي سؤال هنا ولكننا سننتظر حتى يتم تثبيت جميع خوادم الجذر. كان السؤال الأول قد انتهى في هذا الجانب هنا.

متحدث لم يذكر أسمه: كنت أتساءل فقط، أنا قادم من خلفية غير تقنية، كنت أتساءل كيف يمكنك تحديد متى وأين تحتاج إلى معد توجيه آخر من خادم الجذر؟ كيف يختلف مع اسم الخادم وما هو اسم الخادم المتكرر، وما الفرق بين ذلك واسم الخادم العادي؟

فريد بيكر: حسنًا، نقرر وضع خادم جذر جديد عن طريق الصدفة. ليس الأمر كذلك. لدينا بالفعل عملية نمر بها والتي تبدأ بالحاجة. لماذا نحتاج إلى خادم جذر الجديد؟ لماذا نحتاج إلى RSO جديد؟ ثم في حالة وجود حاجة صالحة بالفعل، فهناك مجموعة من المبادئ التي يمكننا من خلالها تحديد شركة أو مؤسسة يمكنها القيام بذلك، وتريد القيام بذلك. أود أن أقترح بصراحة أن تقرأ RSSAC037 لتغطية ذلك لأنه - هناك معلومات كافية هناك.

ويس هارداكر: أعتقد في الواقع، فريد، أنه سأل عن معد توجيه خادم الجذر، وليس مشغل خادم الجذر.

فريد بيكر: حسنًا. معد توجيه خادم الجذر، ستأتي إلى أحدنا، أحد مشغلي خادم الجذر، وعلى سبيل المثال، شركتي ISC، إذا انتقلت إلى صفحة الويب في ISC.ORG، ستجد شيئًا صحيحًا على الصفحة التي تقول، "انقر هنا إذا كنت تريد خادم جذر جديد أو معد توجيه لخادم الجذر."

وأتصور أن هذا صحيح بالنسبة لنا جميعًا. ثم سنتحدث معك حول متطلباتك. لدينا بعض التوقعات حيث سنرغب في توصيل كل من IPv4 وIPv6 بالنظام. يجب أن يكون هناك عرض نطاق ترددي كاف. هناك حاجة إلى الكهرباء، هذا النوع من الأشياء. نتبادل مذكرة التفاهم في النهاية. ثم تبدأ التشغيل وسنعمل على تشغيل الخادم، وسيكون في مقرك لكننا سنشغله عن بعد. أساسًا، إذا كنت تريد واحدًا تسأل ونبدأ هذا الحوار.

ويس هارداكر: إن كنت أستطيع الإضافة إلى ذلك قليلا. أعتقد أن ما تسمعه هو أننا نحصل على متطلبات من أماكن متعددة. نحصل على متطلبات خارجية حيث يرسل الأشخاص نقاط تبادل إنترنت جديدة وأشياء من هذا القبيل، والتي كانت آخر نقطة قمنا بوضعها - نقطة تبادل إنترنت جديدة جاءوا إلينا وقالوا: "سنكون جدد ليس لدينا شيء هناك، هل أنتم على استعداد للمساعدة؟ كنا مستعدين للقيام بذلك وكنا أول من فتح الباب بسبب ذلك، لكن لدينا متطلبات داخلية لكيفية تحليلنا، وكيف يتم خدمة العالم في الوقت الحالي.

أنا الآن بصدد نشر المزيد وأحاول الوصول إلى المناطق المشتتة جغرافيا للحصول على تغطية جيدة قدر الإمكان. إنها مزيج من المقاييس الداخلية والخارجية على حد سواء، ونحن نقدر تعليق أي شخص يعتقد أنه ليس لديه خدمة كافية في منطقته.

براد فيرد: ما تسمعه هنا هو طرق مختلفة لأن كلًا من مشغلي خادم الجذر اختاروه بطريقتهم الخاصة. يمكن أن يستند إلى حاجة، وحاجة انتقال البيانات الفعلية. يمكن أن تستند إلى الحاجة الجيوسياسية. هناك أي عدد من الاحتياجات المختلفة التي تبرر معد توجيه.

أعتقد أن الجزء الثاني من سؤالك، ما هو الفرق بين وحدة حل تكرارية وخادم رسمي، نحن ندير خوادم رسمية، نحن رسميون من أجل الجذر. وحدة الحل المتكررة الخاص بك هو ما تتحدث إليه داخل مزود خدمة الإنترنت. وحدة الحل المتكررة الخاصة بك هي الوسيط الخاص بك جميع الخوادم الرسمية.

على سبيل المثال COM. هو خادم رسمي، والجذر هو خادم رسمي، وUS. وما إلى ذلك. على الأرجح، لا تتحدث إلينا مباشرة، تتحدث إلى خادمك المتكرر ثم تتحدث إلينا عندما تكون هناك حاجة إلى ذلك وإذا لم تكن الإجابة محفوظة في الذاكرة المؤقتة بالفعل. أرجو أن يكون هذا قد أجاب على سؤالك.

أوزان ساهين: لدينا سؤال آخر هنا.

متحدث لم يذكر أسمه: شكراً لكم. لا أدري ما إذا كان هذا الأمر مخصصًا للجنة أم الرجل قبل أو إذا كنت في قاعة خاطئة. إنه يقرأ DNS عبر HTTPS، لذلك أفهم أن فايرفوكس وكروم سوف يتحركان بهذه الطريقة في وقت قصير للغاية، مثل مسألة أسابيع أو أشهر، مما يعني أن 95 بالمائة من انتقال البيانات DNS يمكن تشفيرها، لا أعرف. أرى رأسًا يهتز هناك.

هذا هو بيت القصيد بالنسبة لي، هو أنني لا أعرف أي شيء، وكيف ستؤثر عليه، وكيف ستؤثر على العرض التقديمي بأكمله في بداية هذا الاجتماع حول كيفية عمل DNS،

أو إذا كان سيتغير أو إذا كان مجرد ستكون هي نفسها ولكن خفية؟ لم أشاهد أي لجان عليها في الجدول الكامل لـ ICANN ويبدو أنه شيء مهم حقًا. إذا لم تستطع معرفة ذلك هنا، فربما يمكنكم أن تعرفوا من أين يمكنني معرفة ذلك؟

ويس هارداكر: أنا أيضًا أعمل في هيئة إنشاء وتطوير الإنترنت، التي تشارك في IAFT حيث يتقدم هذا العمل من حيث عملية التقييس. بعض الحقائق عن النشر الذي يقوم به متصفحا فايرفوكس وكروم. إنهم يفعلون ذلك بطريقة مختلفة تمامًا، لذا لا تخطئ في كيفية حدوث ذلك. الشيء الآخر الذي يقومون به، هو فقط بين متصفح الويب ووحدة الحل.

في حالة فايرفوكس يقومون باختيار وحدة الحل، يتم تشغيل وحدة الحل الافتراضي على كلاودفلير، وسيكون لديهم قائمة منسدلة في التكوين الخاص بك عندما يمكنك اختيار وحدة حل التي تريد استخدامها ويقومون بتشغيلها بشكل افتراضي في الولايات المتحدة هذا الشهر، بقية العالم يبحثون عن شركاء آخرين للقيام بذلك. لا تقوم وحدة حل البيانات هذه بإجراء DNS مشفر لبقية النظام ويشمل خوادم الجذر، ويشمل خوادم TLD مثل COM. وخوادم ccTLD وexample.com وأشياء من هذا القبيل.

متصفح كروم من ناحية أخرى يقوم بشيء مختلف قليلاً. إنهم يحاولون معرفة ما إذا كانت وحدة حل مزود خدمة الإنترنت المحلي تدعم DoH وما إذا كان مدرجًا في القائمة المعتمدة، وسيتواصلون مع DoH إلى ISP. إنهم لا يفعلون ما يفعله فايرفوكس ويرسلونه إلى مكان واحد. هناك مشكلة مختلفة جدًا في النشر، وللأسف هناك الكثير من الارتباك لأن هذه المعلومات تتغير بسرعة كبيرة، وحتى رغبة فايرفوكس في القيام بالولايات المتحدة فقط مع كلاودفلير كان قرارًا حديثًا جدًا وما يحدث في الأسبوع المقبل يخضع للمناقشة.

في غضون أسبوعين، ستتم مناقشة ذلك بشكل أكثر تفصيلًا في IETF بين فريق عمل هندسة الإنترنت والذي سيكون في سنغافورة. هذا هو المكان الذي تجري فيه المحادثة التقنية. في غضون شهرين، سيكون الأمر مختلفًا، إنه يتغير بسرعة كبيرة الآن.

براد فيرد: هلا أضفت إلى ذلك. مرة أخرى، أكرر التأكيد على أن ذلك بين العميل ووحدة الحل حيث يحدث التشفير وليس بين وحدة الحل والخادم الرسمي الآن. سأقول، لقد تم الحديث عن هذا

الأمر في ICANN، وكان هناك موضوع اهتمام كبير في مراكش فيما يتعلق بهذا، لذلك سأعود إلى جدول أعمال مراكش.

لا أتذكر اليوم الذي كان فيه ذلك، لكن كان هناك عرض تقديمي كبير من قِبل SSAC وأعتقد أنه كان CCNSO، لقد كانت هناك مجموعة شرائح تتحدث عنه وما زالوا يتحدثون عنه. أعلم أن SSAC تعمل عليه وهناك أعمال أخرى يتم تنفيذها. هذا لديه الكثير من جهات الإشراف.

فريد بيكر: إذن، اسمح لي أن أطرح سؤالاً حول DNSSEC؛ بشكل عام، لا تقوم المتصفحات بتطبيق DNSSEC، فهي تعتمد على قيام شخص آخر بذلك، لذلك عندما يتم الانتقال إلى DoH، يتم التحقق من DNS؟

ويس هارداكر: هذا سؤال رئيسي ممتاز، فريد. سؤال جيد جدًا. هناك جانبان للأمن بشكل عام، يفكر فيهما معظم الناس. يوجد تشفير، بمعنى آخر، يتم حماية بياناتك، ثم هناك مسألة ما إذا كانت بياناتك أصلية، هل هي بالفعل البيانات الصحيحة؟ يمكن أن تكون مشفرة وما زالت خاطئة. قد تحصل على الملف المشفر الخاطئ على سبيل المثال.

في DNSSEC، فإنه يحمي من الأصل ومن المكان الذي تم إنشاء البيانات فيه، وفي هذه الحالة تكون IANA ومن خلال توقيع مشرفي منطقة الجذر على تلك البيانات، وبقية بيانات منطقة الجذر، وفي الواقع بالنسبة لمعظم TLDs وأي شيء يتعلق بهذا الأمر بخلاف ذلك الموقَّع أدناه، لا يهم، يمكنك فعلًا تسليم ذلك إليّ على ورقة، ويمكنني قراءتها ومسحها ضوئيًا، وأنا قادر على التحقق من التوقيع مقابل موقعه الأصلي من IANA وجميع الطريق إلى أسفل الشجرة.

كان السؤال الرئيسي لفريد هو: هل تقوم DoH أيضًا بالتحقق من النزاهة لكنها فقط بين نقطتين، لذلك إذا كان هذا الكيان أعلاه، وحدة الحل التي كنت تتحدث إليها بشكل غير آمن، فلن تعرفه وسوف تقدمه لك بطريقة لم يتم التحقق منها. ستقوم بعض أدوات حل DoH بالتحقق من DNSSEC. إذا كنت تعرف أنك تتحدث مع وحدة حل DoH عبر قناة محمية بنزاهة آمنة وتعلم أنك تقوم بالتحقق، فمن المحتمل أن تكون آمنًا من النهاية إلى النهاية. كلاودفلير هو أحد وحدات الحل التي أعتقد أنها تقوم بالتحقق من الصحة بشكل افتراضي، ولا أعرف عن الباقي.

براد فيرد: ولكن هذا شيء يستحق التحقق إذا كنت تبحث في ذلك.

ستيف كونتي: هل هذا متابعة سريعة لديك؟ حسنًا.

متحدث لم يذكر أسمه: البيانات غير مرئية لمزود خدمة الإنترنت في بيئة HTTPS، لم يعد بإمكانهم رؤية الأخطاء؟ كل ما يطير عبر شبكتهم ولكن يا رفاق لا يزال بإمكانك رؤيته؟ من سيظل قادرًا على الرؤية - من سيكون له رؤية في طلبات DNS ومن لن يكون في عالم DNS أو HTTPS؟

ويس هارداكر: من الصعب الإجابة اليوم لأنه كما قلت، سيكون الأمر مختلفًا في الشهر المقبل. هذا صحيح بالنسبة للأشخاص الذين يستخدمون فايرفوكس الذي يتصل بموفر DoH في مكان آخر ولكن موفر DoH، مثل كلاودفلير سيكون قادرًا على رؤيته. من هناك، يتم توزيعها على الكل - في مرحلة ما يجب عليك أن تطرح سؤالاً على شخص ما، في مرحلة ما يجب أن تذهب إلى شخص ما وتقول "يجب أن أطرح سؤالاً".

هذا الشخص الذي يتعين عليك طرح سؤال عليه، مثل موقع الويب هذا، سيكون بإمكانه دائمًا رؤيته. هناك دائمًا شخص ما يجب أن يعرف سؤالك. بالنسبة إلى كروم من ناحية أخرى، نظرًا لأنهم سيصبحون DoH لدى ISP، أو لوحدة حلك لدى ISP، فإن ذلك لن يغير من رؤية ISP.

يعتمد هذا بشكل كبير على وضع النشر ويقوم كروم وفايرفوكس بعمل أشياء مختلفة. أنت قارئ البريد من ناحية أخرى، لا توجد خطط قارئ البريد من جهة DoH على سبيل المثال. إذا كنت تقوم بالبريد داخل متصفح الويب، فسيكون هناك. إنه سؤال - إنه ليس بنعم أو لا. هل يبدو ذلك منطقيًا؟

فريد بيكر: لذا، يبدو من الجيد الإشارة إلى تقنية تصغير اسم الاستعلام. هذا مشروع قيد التنفيذ في IETF وسيأتي إلى بعض البرامج بالقرب منك في وقت ما.الفكرة هي خيانة أقل قدر ممكن من المعلومات مع الحصول على الإجابة على السؤال. إذا كنت أبحث عن www.example.com، على سبيل المثال، قد أطلب من الخادم التكراري الخاص بي وسيقول الخادم التكراري: "لا أعرف أين يوجد COM.، لم أتصور ذلك بعد."

لذلك، فإنه الآن، بدلاً من إرسال الاسم بالكامل إلى خادم الجذر، وهو ما يفعله الآن، فإنه سيرسل COM إلى خادم الجذر، سيعلم خادم الجذر أنه طلب COM. وسيعطي ذلك الاسم ثم قد يطلب example.com. حقًا، فقط هذا الخادم التكراري يمكنه الوصول إلى تلك المعلومات. تريد أن تشاهد تقنية تصغير اسم الاستعلام.

متحدث لم يذكر أسمه: الجزء الآخر من هذا هو التجميع. إذا كان لديك الآلاف والآلاف من الأشخاص يذهبون إلى نفس حل وحدة الحل التكرارية، نعم أن وحدة الحل التكرارية تعلم أنك قدمت هذا الطلب ولكن الآن إذا كنت تتلقى آلاف الطلبات من نفس وحدة الحل التكرارية في كل مكان، فلن يكون بالضرورة ينسب إلى الفرد، مجرد شخص واحد من العديد من الأشخاص الذين يستخدمون وحدة الحل التكرارية تلك فعليًا.

سؤال ستيف: شكراً لكم. السؤال التالي في هذا الجانب.

متحدث لم يذكر أسمه: أريد أن أعرف ما إذا كانت DSOs تحتفظ بالسجلات وإذا كان الأمر كذلك، فهل هناك أي قواعد حول الخصوصية على سبيل المثال؟ بدافع الاهتمام، كيف يتم تمويل DSOs لعمليات خدمة النطاق؟

براد فيرد: هل تقصد RSO؟ نستمر في سماع DSOs، أردت فقط التأكد من أنك تعني RSO، صحيح؟

متحدث لم يذكر أسمه: نعم، عذرًا.

براد فيرد: حسنًا، سأعود إلى الخلف. لم أسمع الجزء الأول من السؤال ولكن الجزء الأخير بسيط للغاية حول كيفية تمويلها. في الوقت الحالي، إنه أمر غير ممول، كل هذا على أساس تطوعي. نظرًا لتطور الإنترنت بشكل عضوي، كان هناك متطوعون لتشغيل خوادم الجذر هذه وتمت إضافتهم بمرور الوقت، ما بين 1982 و1998 أساسًا ولم يكن هناك خادم جذر جديد منذ عام 1998. أعتقد أنه تم تقديم تعدد الاتجاهات عام 2001 وبدأ تشغيله بواسطة خوادم الجذر، لذلك انتقلنا من 13 معرِّفًا، و13 خادمًا إلى الآن، ونحن في آلاف الخوادم ولكننا نمتلك 13 هوية. باستخدام تعدد الاتجاهات، نحن قادرون على نشر ذلك بعيدًا وعريضًا ويتم كل ذلك، كل هذا يتم تمويله ذاتيًا من قبل كل مؤسسة. هل تتذكر الأجزاء الأخرى من الأسئلة، أو هل يمكنك تكرارها؟

متحدث لم يذكر أسمه: أنا مهتم إذا كنتم تحتفظون بسجلات للطلبات وإذا كان هناك أي قواعد حول خصوصية تلك السجلات؟

براد فيرد: الشيء الوحيد الذي يمكنني أن أشير إليه هو أن هناك سنويًا ما يشار إليه باسم مجموعة Diddle وهو يوم في الحياة ويشار إليه باسم Diddle وهو عبارة عن مجموعة من نافذة مدتها 48 ساعة تتيح للباحثين مجموعة كاملة من البيانات لمعرفة ما يفعله الإنترنت في يوم معين. يمكن لجميع مشغلي خادم الجذر المساهمة في ذلك، إلى جانب الكثير من TLDs وccTLDs الأخرى والمؤسسات الكبيرة ومشغلي DNS الكبار، إنه جهد مجتمعي والبيانات يتم تخزينها في قاعدة بيانات DNS ومن أجل الوصول إلى قاعدة البيانات، يجب أن تصبح عضو وتوقع وثائق بشأن السرية وما إلى ذلك.

ويس هارداكر: هناك نقطة أخرى، وهي أن الكثير من المشغلين يقومون بإخفاء هوية البيانات قبل إعطائها إلى OARC وما يعنيه هذا حقًا أنهم يقومون بإخفاء هوية IPS، وغالبًا ما يكون عنوان IP المطلوب هو وحدة حل في المقام الأول حتى لا يتم ربطه حقًا. إلى جهاز مستخدم نهائي واحد،

يتم ربطه بوحدة حل تقدم الكثير من الأشياء. أعتقد بشكل خاص مع الشركات الحديثة، خاصة ومنذ القانون العام لحماية البيانات أعتقد أن معظم المشغلين يقومون بإخفاء هويتهم ولكن عليك أن تتحدث مع كل منهم، ولا أتذكر الوضع الحالي لمن يحدد هويته وإلى أي مستوى.

أوزان ساهين: لدينا سؤال آخر.

متحدث لم يذكر أسمه: أولاً، يجب أن أعتذر لأنني أعتقد أن هذا السؤال سيكون من الصعب الإجابة عليه. في وقت سابق من الشرائح، لاحظت أن معظم المنظمات التي تملك عنوان IP الخاص بخوادم الجذر هي جميعها منظمات أمريكية وكنت أتساءل في عالم على سبيل المثال، الحكومة الأمريكية لن تلتزم حقًا بالحياد؛ ما الذي يمكن أن يضمن أو هل هناك أي آلية تضمن بقاء خوادم الجذر لشبكة الإنترنت الأساسية محايدة؟

فريد بيكر: للإجابة على ذلك، ومن المحتمل أن يكون هناك أكثر من إجابة واحدة ولكن أحد الأشياء التي تعمل عليها RSSAC الآن هو سؤال حول كيفية قياس النظام؟ أحد القياسات، أحد الأشياء التي نشعر بالقلق حولها هو ما إذا كان يتم قياس RSO الذي يتم قياسه ونقيسها جميعًا ولكنها تتحدث عن أحدها في أي وقت محدد، وهو يخدم بالفعل النظام الذي جاء من IANA.

إذا كانت منطقة الجذر التي تحصل عليها من خادم معين مختلفة، فهي تعد انتهاكًا لبعض الأشياء التي نعتبرها مهمة إلى حد ما. سيكون ذلك أمرًا سيئًا. ما نقوم به، هو تنزيل المعلومات حرفيًا، كل بضع دقائق شيء من هذا القبيل، تنزيل المعلومات من IANA، نحن نخدمها لفترة من الوقت وسنقوم بتنزيلها أكثر من ذلك. نمر دائمًا بما قدمته IANA.

الآن، ماذا أعطتنا IANA؟ تقوم TLDs وccTLDs وgTLDs بالتحول وإبلاغ IANA، وكان لدي هذه الأسماء ولديها هذه السجلات المرتبطة بها وIANA هي الطرف المحايد وتدير ذلك. أعتقد أن ما تعتمد عليه حقًا من حيث الحياد هو أخلاقيات IANA ونطاقات ccTLD، التي تقوم بذلك كعمل تجاري وRSOs. هل هذا هو الجواب الشافي لسؤالك؟

ويس هارداكر: اسمحوا لي أن أضيف أكثر قليلا، فريد، قبل أن تمضي قدمًا. أوصي بشدة بقراءة RSSAC023، وهو المستند من 0 إلى 23، إنه تاريخ كيفية إنشاء نظام خادم الجذر بالطريقة الحالية. في الواقع، كنا نتحدث عن ذلك في وقت سابق اليوم في اجتماع RSSAC، الذي نرحب بكم للمجيء إليه والاستماع إليه أيضًا.

يشرح كيف وصلنا إلى المؤسسات التي تخدمها حاليًا ويرجع ذلك تمامًا إلى التاريخ، ولم يتغير ذلك منذ 20 عامًا وأحد أهداف RSSAC037، وهو هيكل لكيفية إجراء تغييرات على هذه العملية في المستقبل منذ آخر شخص قام بتغييرات وافته المنية قبل 20 عامًا، قيد المناقشة.

والأهم من ذلك، أن نفس المحادثات التي كنت أتحدث عنها سابقًا فيما يتعلق بـ DNSSEC، إذا كنت تقوم بالتحقق من DNSSEC وكان النطاق الذي تعمل عليه قد تم التحقق منه من الأعلى إلى الأسفل، فأنت تعلم أنه لم يتم تعديله ولا يهم حقًا ما هي البلدان التي مر بها، فهو مستقل تمامًا من الناحية السياسية لأنه من المستحيل تقنيًا تزييف تلك البيانات من الناحية التقنية. هذا هو أكثر الأشياء أمانًا التي يمكنني أن أخبرك بها، وتأكد من أنك تستخدم وحدة حل تتحقق من صحة DNSSEC.

براد فيرد: سأضيف فقط أكثر قليلاً، وهو RSSAC037، الذي تم نشره وهو موجود للجميع ليقرأه وهناك ينص على المبادئ التوجيهية كما حددها مشغلي خادم الجذر. أحد هذه المبادئ الإرشادية هو الحفاظ على الحياد، إنها وجهة نظر غير سياسية، لا توجد سياسة معنية، نحن نخدم منطقة الجذر التي يتم تقديمها إلينا من IANA. فيما يتعلق بالتعليق حول الولايات المتحدة ومقرها، وهذا هو نتيجة بحتة للنمو العضوي. بدأت الإنترنت في الولايات المتحدة، ونمت في الولايات المتحدة، وكانت هناك حاجة لمشغلي خادم الجذر، وهذا ما حدث، ولم يكن هناك سبب آخر غير النمو العضوي.

فريد بيكر: ولدينا بالطبع مشغلي خادم الجذر خارج الولايات المتحدة، ولدينا مشغل في السويد وواحد في هولندا وواحد في اليابان.

ستيف كونتي: سوف آخذ المتحدث التالي هنا في الظل، إلى يمينك.

متحدث لم يذكر أسمه: أعلم أن الحرمان من الخدمة وهجمات الحجب المنتشر للخدمة، مثل العديد من الأشياء الأمنية، مثل القط والفأر، والمهاجمون يصبحون أكثر قوة، والأمن يزداد قوة والعكس صحيح ويستمر. ما الذي يتم فعله بالضبط للحفاظ على خوادم الجذر محمية بشكل مستمر؟ هل اجتمع RSSAC مع SSAC وعقدا اجتماعات بشأن الحفاظ على خوادم الجذر محمية أو كيف يعمل ذلك؟

براد فيرد: أول ما يمكنني قوله الآن هو مؤخرًا، قام مشغلو خادم الجذر بنشر مستند من هذا النوع يعالج سؤالك مباشرةً. إنها تهديدات لنظام خادم الجذر وماذا يفعلون وما فعلوه لتخفيف بعض تلك التهديدات الشاملة.

فيما يتعلق بـ RSSAC، فإن RSSAC تتواصل مع مجلس الإدارة، مع SSAC فيما يتعلق بأي نوع من التهديدات للنظام، ولهذا السبب - كان هناك سؤال مبكر حول DoH وDoT، تحدثنا عن ذلك والآثار المترتبة على البنية التحتية عندما يحدث شيء من هذا القبيل. هذه المحادثات تحدث في كل وقت. هذه ليست فعلية على الرغم من ذلك، فإن الأسئلة التشغيلية تحدث داخل RSO وبين RSO وفي حالة وجود DDoS أو أي شيء آخر، تتم مشاركة المعلومات وتحدث عمليات التخفيف.

ويس هارداكر: أين يمكن أن يجد تلك الوثيقة براد؟

براد فيرد: أعتذر. ليس وثيقة RSSAC، تقع تلك الوثيقة على صفحة ويب خادم الجذر، التي هي في www.root-servers.org؛ أعتقد أنها في الجزء العلوي من الصفحة.

متحدث لم يذكر أسمه: هذا أمر رائع، شكرًا جزيلاً لك. هل بإمكاني طرح سؤال أخير؟ أعرف أنه مع خوادم DNSSEC التي تم تكوينها بشكل خاطئ، فهناك أيضًا إمكانية لشن هجمات تضخيم وأعلم أن هناك الكثير من الضغط من أجل طرح DNSSEC، فأنا أشعر بالفضول إذا كان هناك أي طريقة ممكنة لدفع الخوادم التي تم تكوينها إلى DNSSEC؟ على سبيل المثال، إضافة حد لمعدل والأساليب الأخرى؟ أعلم أنه كانت هناك مناقشة كبيرة مرة أخرى في عام 2013 نيابة عن ICANN حول تشديد أمان DNS.

ويس هارداكر: هل يمكنك تنقيح سؤالك حول المكان الذي تسببت فيه خوادم DNSSEC التي تم تكوينها بشكل خاطئ في حدوث مشكلات نظرًا لأن هذا النطاق واسع جدًا أم أنك تشير إلى شيء محدد للغاية؟

متحدث لم يذكر أسمه: إذن، إذا قام شخص ما بإعداد خادم دعم DNSSEC تم تكوينه بشكل خاطئ وقام شخص ما بتشغيل هجوم يستند إلى UDP وقام بانتحال عنوان IP، فيمكنك ببساطة تجميع قائمة بخوادم DNSSEC التي تم تكوينها بشكل خاطئ، ثم يسمح فقط لهجوم التضخيم أن يكون أقوى من تضخيم DNS الطبيعي.

ويس هارداكر: أنت قلق بشأن هجوم الانعكاس. يضيف DNSSEC مجموعة كبيرة من البيانات إلى التواقيع تصبح كبيرة جدًا، والمفاتيح كبيرة جدًا وأنت على حق تمامًا، خاصةً في الماضي كان DNSSEC قد استُخدم بمثابة هجوم انعكاس لأنك ترسل حزمة بيانات صغيرة جدًا تقوم بتزويرها من العنوان الذي تريد الهجوم عليه وكمية كبيرة جدا من انتقال البيانات تذهب في هذا الاتجاه.

اليوم، معظم الخوادم ولا أتحدث عن خوادم الجذر فقط، لكن معظم الخوادم لديها تقنيات تستخدم شيئًا يُطلق عليه "تحديد معدل الاستجابة"، وما يفعله ذلك هو أنه لن يسمح لخادم واحد بطرح العديد من الأسئلة، بل يوقفها ويقول، "أنا لا أتحدث إليكم بعد الآن. لا يزال بإمكانك التحدث معي ولكن عليك العودة عبر TCP، وهو أمر يصعب تزويره."

ما تقوم به إعدادات كل خادم رسمي مختلف تمامًا. يمكنني أن أخبرك أنه قبل أن يتحول معظم الناس إلى ذلك، سترى مجرد طفرات يومية في انتقال البيانات لأن الجميع كانوا يستخدمونها وبعد ذلك بسنوات، أصبحت الرسوم البيانية لانتقال البيانات لمعظم الناس ثابتة إلى حد ما لأن الناس أدركوا أن هذه الطريقة لم تعد قابلة للتنفيذ. لم تشاهد هجمات الانعكاس في DNSSEC بعد الآن. أنا متأكد من أنها لا تزال موجودة في مكان ما.

ستيف كونتي: حسنًا، شكراً جزيلاً لك. هل هناك أي أسئلة أخرى في القاعة؟ لقد راجعت عبر الإنترنت، لا توجد أسئلة على الإنترنت. الفرصة الأخيرة للأسئلة في القاعة.

ويس هارداكر: هذه كلها أسئلة فنية رائعة، شكرا لكم.

ستيف كونتي: أود أن أشكر أندرو؛ أود أن أشكر أوزان على العرض التقديمي الرائع. أود أن أشكر مشغلي خادم الجذر الخاصين بنا للإجابة على هذه الأسئلة، وسوف أقوم بتوصيلات وقحة، أعرف أن اليوم انتهى تقريبًا ولكن بالنسبة لسلسلة كيف يعمل، لدينا جلسة جديدة تمامًا تبدأ من الساعة الخامسة في 512G. لدينا آرون قادمًا للحديث عن سجلات الإنترنت الإقليمية، وما الذي يقومون به والمعرفة الأساسية لذلك. أطلب منكم الانضمام إلينا لدورة واحدة أخرى، الساعة الخامسة، 512G لحضور جلسة حول سجلات الإنترنت الإقليمية. وبالوصول إلى هذه النقطة، أتقدم إليكم بالشكر. شكرا، أندرو، شكرا لك، أوزان، وشكرا لكم يا رفاق على وقتكم.

ويس هارداكر: هل يمكنني عمل توصيل إضافي واحد؟

ستيف كونتي: نعم، تفضل.

ويس هارداكر: مع صراع للأسف، ستيف، أعتذر. هناك أيضًا DNSSEC لحديث المبتدئين الذي يجري أيضًا في الساعة الخامسة.

ستيف كونتي: حسنًا، حسنًا عليك اختيار السم بعد ذلك. شكرًا لكم جميعًا.

[نهاية التدوين النصي]